MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS
VERSLO IR EKONOMIKOS INSTITUTAS

IVONA ŠAKĖNIENĖ

ORGANIZACIJŲ VAIDMUO UŽTIKRINANT KIBERNETINĮ SAUGUMĄ: INDIVIDO IR INSTITUCIJOS SĄVEIKA

Magistro baigiamasis darbas

Vadovė:
Prof. dr. Asta Valackienė

VILNIUS, 2023

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

ĮVADAS

Temos aktualumas ir naujumas. Skaitmeninė era, Industrinės revoliucijos 4.0 sociumą keičiantys kokybiniai veiksniai taip pat Industrinės revoliucijos 5.0 kokybiniai ir kiekybiniai iššūkiai, įgalino keisti sociumo: ekonominę, politinę ir kultūrinę erdvę. Visuomenę 5.0 *galima apibrėžti kaip į žmogų orientuotą visuomenę, kurioje ekonominė pažanga derinama su socialinių problemų sprendimu, pasitelkiant sistemą, kuri glaudžiai integruoja kibernetinę (virtualią) ir fizinę (realią) erdvę. Visuomenės 5.0 tikslas - sukurti visuomenę, kurioje socialinės problemos būtų sprendžiamos į pramonę ir socialinį gyvenimą įtraukiant ketvirtosios pramonės revoliucijos inovacijas (pavyzdžiui, daiktų internetą, didžiuosius duomenis, dirbtinį intelektą ir dalijimosi ekonomiką)* (Piest, 2023). Šiuo požiūriu išsiplėtė visuomenės bendradarbiavimo laukas, naujos perspektyvos. Šiandien elektroninė erdvė apima didelę mūsų gyvenimo dalį, kiekviena valstybė suinteresuota aktyviai skatinti informacinių ir ryšių technologijų plėtrą (IRT), nes tai leidžia smarkiai padidinti asmenų ir įmonių tarpusavio ryšį visame pasaulyje. Vis daugiau kasdieninės veiklos ir sandorių atliekama naudojantis internetu, o siaučianti COVID-19 pandemija dar labiau paskatino mūsų priklausomybę nuo skaitmeninių sprendimų. Pandemijos metu tiek viešajam sektoriui, tiek privačiam buvo svarbu nenutraukti savo vykdomos veiklos ir toliau suteikti paslaugas, todėl institucijos ir įmonės buvo priverstos intensyviau diegti skaitmeninimo sprendimus, o vartotojus dar labiau paskatino naudotis el. prekyba ir el. paslaugomis. Žinoma kiekviena krizinė ar neeilinė situacija skatina vystymąsi, bet kartais neišvengiama ir neigiamų pasekmių. Piktavaliai irgi nesnaudžia ir ieško spragų, kurias išnaudotų savo piktiems tikslams pasiekti.

Kita vertus, sparčiai didėjant skaitmenizacijos tempui ir pažangių bei sudėtingų technologijų diegimui, organizacijos susiduria su didesne rizika kibernetinėje erdvėje nei anksčiau. Tam kad organizacija užtikrintų kibernetinį saugumą neužtenka naujausių ir pažangiausių technologijų, žmogus – organizacijos turtas, bet kartu ir silpnoji organizacijos vieta. Visos turimos technologijos, skirtos sistemoms apsaugoti, neužtikrins organizacijos saugumo, jei organizacijoje dirbantys žmonės neturės pakankamai kompetencijų ir priims blogus ar netikėtus sprendimus, kurie atveria sistemą įsilaužėliams. Todėl ypač aktualu investuoti į skaitmeninį raštingumą tarp visų skaitmeninės erdvės vartotojų amžiaus grupių. Kad organizacija būtų saugi ir gebėtų sumažinti riziką dėl kibernetinių atakų visi organizacijos darbuotojai turi suprasti, kad kibernetinis saugumas nėra vien tik techninis klausimas, kuris turėtų būti sprendžiamas „IT žmonių“. Pandemijos metų tai ypač išryškėjo - kol visi (organizacijos, įstaigos, žmonės) stengėsi prisitaikyti prie sumaišties ir susikoncentravo ties viruso (

COVID-19) plitimo mažinimo, piktavaliai taip pat susikoncentravo ir pasinaudojo kiekviena galimybe vykdyti nusikaltimus kibernetinėje erdvėje (ENISA, 2021). *70 proc. informacijos saugos vadovų išskiria kompetetingų darbuotojų trūkumą kaip didžiausią iššūkį siekiant užtikrinti įmonės kibernetinį saugumą* (Kibernetinis saugumas ir verslas, 2020, p. 19)

Visi organizacijos nariai turi imtis veiksmų rizikoms mažinti, organizacijos kaip socialinio instituto vaidmuo tas rizikas efektyviai valdyti. Visų pirma organizacijos vadovas turi formuoti visos organizacijos vertybes ir diegti požiūrį į bendrus saugumo tikslus, įtraukiant į šį procesą visus darbuotojus. Vadovas, investuodamas į saugumo technologijas, kartu turėtų skatinti, kurti ir plėtoti organizacijos kibernetinio saugumo kultūrą ir ieškoti sprendimų kaip spręsti žmogiškąją kibernetinio saugumo pusę.

Mokslinė problema ir ištirtumo lygis. Ankstesnėje literatūroje plačiai aptarta žmogiškųjų veiksnių ir kibernetinio saugumo elgsenos įtaka kibernetinio saugumo sąmoningumui arba kibernetinio saugumo sąmoningumo poveikis elgsenai (Alghamdi, 2021). Kibernetinio saugumo pasekmės vis didėja ir žmogus išlieka svarbiausiu šios ekosistemos elementu, darančiu įtaką visam saugumui (Gutzwiller 2019). Darbuotojų pagrindinis tikslas - atlikti užduotį, jei įdiegtos saugumo kontrolės priemonės trukdo arba lėtina šio tikslo įgyvendinimą, darbuotojas tai laikys kliūtimi ir apeis procesą. Šis reiškinys yra suvokiama kliūtis, kuri yra tai, ką darbuotojas laiko nepatogumu ir kaina, kurią jis patiria vykdydamas kibernetinio saugumo užduotis (Alghamdi, 2021). Tai atitinka Ertan (2018), kad daugiau nei pusė visų informacijos saugumo pažeidimų netiesiogiai arba tiesiogiai įvyksta dėl darbuotojų nesugebėjimo elgtis pagal informacijos saugumo procedūras, nes kai kuriais atvejais į saugumo politiką žiūrima tik kaip į gaires, o ne į privalomus nurodymus todėl darbuotojai dažnu atveju gali nuspręsti jos (saugumo politikos) nesilaikyti dėl patogumo atliekant kasdienes funkcijas darbo aplinkoje. Žmogiškasis veiksnys - tai žmogiškosios klaidos, dėl kurių kyla saugumo incidentų klaidos (Zwilling 2022). Nobles (2018) žmogiškuosius veiksnius apibūdina kaip žmonių sąveiką ir praktiką informacinės sistemos aplinkoje. Elgesys, susijęs su saugumo reikalavimų laikymusi, tebėra iššūkis, kaip pabrėžiama ENISA (2017), žmogaus piktavališki, aplaidūs ar netyčiniai veiksmai įvardijami kaip pagrindinė saugumo incidentų priežastis. Elgesio aiškinimas moksliniuose darbuose buvo grindžiamas planuojamo elgesio teorija (TPB) ir apsaugos motyvacijos teorija (PMT) (Ertan ir kt., 2018; Alghamdi, 2021; Nobles, 2018). Neatsargumas ar aplaidumas, o ne piktavališki ketinimai yra pagrindinė duomenų pažeidimų, kuriuos įgalina žmogus, priežastis (Nifakos ir kt., 2021). Darbuotojai priešinasi reikalavimų laikymuisi dėl žmogiškųjų veiksnių, tokių kaip laiko trūkumas, didelis darbo krūvis ir greitesnio būdo užduočiai atlikti suradimas (Ertan 2018; Nobles, 2018). A.A. Alghamdi

(2021) atvejo tyrime pažymėjo, kad 51 proc. respondentų grėsmę, susijusią su kibernetinio saugumo supratimu, laikė didele. Kai kurie ribojančią organizacijos politiką laikytų nereikalingu suvaržymu (Ertan ir kt. 2018), tam nepadeda ir esami kibernetinio saugumo sąmoningumo mokymai, kurių taikymo sritis yra ribojanti, nes jie nekeičia darbuotojų elgesio saugumo srityje (Nobles, 2018). Organizacijose, kuriose paprastai trūksta saugumo išteklių, įsitraukimas į išsamią kibernetinio saugumo sąmoningumo didinimo programą su darbuotojais gali pasirodyti kaip pageidavimų sąrašas, o galiausiai tai tampa tik atitikties pažymėjimo užduotimi, kai kompiuteriniai mokymai yra kasmetinė užduotis. Organizacijos turi atsisakyti tradicinių saugumo mokymų ir informuotumo didinimo iniciatyvų - kasmetinių kompiuterinių mokymų - ir pereiti prie labiau transformacinio pobūdžio mokymų (Alshaikh, 2020).

Remiantis darbe nagrinėjamos mokslinės literatūros bei atliktų taikomųjų tyrimų bei ataskaitų duomenimis galima teigti, kad yra nepakankama kibernetinio saugumo kultūra organizacijose, nepakankama sąveika tiek iš organizacijos kaip administracinio instituto, tiek iš darbuotojų, kaip pagrindinio įrankio, gebančio įsitraukti į kibernetinio saugumo užtikrinimą organizacijoje. Aptarta situacija magistriniame darbe leido konstatuoti, kad kibernetinis saugumas tai tik papildoma našta organizacijai, todėl darbe keliamas **mokslinės problemos klausimas:** ***kaip organizacija įgalina kibernetinio saugumo valdymo modelius, strategijas, taiko užkardymo instrumentus, įgalinančius užtikrinti kibernetinį saugumą?***

Magistro tezių mokslinis rezultatas – parengtos „Kibernetinės kultūros viešajame sektoriuje tobulinimas“ gairės.

Tyrimo objektas. Organizacijos ir individo sąveika užtikrinant kibernetinį saugumą.

Tyrimo dalykas. Viešojo sektoriaus darbuotojų tarpusavio sąveika užtikrinant kibernetinį saugumą.

Tyrimo tikslas. Išanalizuoti esamą kibernetinio saugumo situaciją viešajame sektoriuje bei įvertinti organizacijos ir individo sąveiką, užtikrinant kibernetinį saugumą.

Uždaviniai:

1. Pristatyti kibernetinio saugumo organizacijose teorinius aspektus, aptariant kibernetinio saugumo valdymo modelius bei strategijas.
2. Atskleisti, Baltijos šalių, kibernetinio saugumo organizacijose vystymo prioritetus nacionaliniuose dokumentuose.
3. Nustatyti veiksnius, turinčius įtakos organizacijos gebėjimui užkirsti kelią kibernetinio saugumo incidentams.

4. Pagrįsti organizacijos ir individo sąveiką viešajame sektoriuje, užtikrinant kibernetinį saugumą, parengiant Gaires „Kibernetinės kultūros viešajame sektoriuje tobulinimas“.

Darbe siekiama patvirtinti arba paneigti šiuos ginamuosius teiginius:

1. Kibernetinio saugumo kultūros neišmanymas organizacijoje kelia potencialią grėsmę organizacijai.
2. Nepakankamas individų bendradarbiavimas, užtikrinant kibernetinį saugumą organizacijoje yra kliūtis siekiant aukštą kibernetinio atsparumo lygį organizacijoje.

Darbe naudojami **duomenų rinkimo metodai**: mokslinės literatūros analizė, juridinių ir strateginių dokumentų analizė, antrinių statistinių duomenų analizė, taikomųjų tyrimų ir ataskaitų, aptariant skaitmeninį raštingumą ir kibernetinį saugumą viešajame sektoriuje analizė, ekspertinis interviu, viešojo sektoriaus darbuotojų anketinė apklausa. Ši analizė leidžia bendrai įvertinti esminius kibernetinio saugumo ir kibernetinės kultūros principus ir prioritetus bei iliustruoja kaip atskiruose dokumentuose ir studijose tai identifikuojama. **Duomenų analizei** taikomi **metodai:** anketinės apklausos kokybinė turinio (angl. *Content*) analizė, ekspertinio interviu kokybinė turinio (angl. *Cintent*) analizė ir interpretavimas bei aprašomoji antrinių statisnių duomenų analizė.

Darbo struktūra. Darbą sudaro penkios dalys: įvadas, teorinė dalis, tyrimas, empirinės dalis, išvados ir rekomendacijos kibernetinio saugumo gerinimui viešajame sektoriuje. Įvadinėje darbo dalyje apžvelgiamas temos aktualumas, iškeliamas darbo tikslas ir uždaviniai, aptariama darbo problema bei ištirtumo laipsnis, pristatomi ginamieji teiginiai ir darbo metodai. Teorinėje darbo dalyje analizuojami kibernetinės saugumo sampratos ir kibernetinės kultūros organizacijoje teoriniai aspektai ir problematika. Trečiame skyriuje pateikiama tyrimo metodologija. Ketvirtas skyrius – empirinė dalis, kurioje nagrinėjami tyrimo metu surinkti duomenys siekiant išanalizuoti esamą kibernetinio saugumo situaciją viešajame sektoriuje bei įvertinti organizacijos ir individo sąveiką, užtikrinant kibernetinį saugumą. Darbo pabaigoje pateikiamos tyrimo rezultatus apibendrinančios išvados ir parengtos Gairės „Kibernetinės kultūros viešajame sektoriuje tobulinimas“, literatūros sąrašas bei priedai.

Praktinis taikomumas. Spartėjant paslaugų ir procesų skaitmenizavimui, esant geopolitiniams iššūkiams ir įtampai auga kibernetinių ir hibridinių atakų grėsmės bei didėja jų socialinis ir ekonominis poveikis. Todėl Lietuvos Respublikai labai svarbu apsaugoti nuo kibernetinių grėsmių ir pažeidžiamumų, galinčių turėti įtakos, ypatingos svarbos informacinėms infrastruktūroms, valstybės informacinių išteklių elektroninei informacijai ir jų pagrindu veikiančioms sistemoms ir paslaugoms bei užtikrinti efektyvų kibernetinį saugumą (Valstybės kontrolė 2022). Kadangi šio tyrimo išvados

gautos Lietuvos kontekste, rezultatai greičiausiai bus pritaikomi tik Lietuvoje, tačiau išvados gali būti naudingas šaltinis kitose valstybėse.

1. ORGANIZACIJŲ KIBERNETINIO SAUGUMO KONCEPTO TEORINIS PAGRINDIMAS

Kibernetinis saugumas ir toliau išlieka vienu iš pagrindinių organizacijų rūpesčiu, nes kibernetiniai nusikaltimai kelia didelę riziką ir kainuoja didžiules pinigų sumas. Tačiau tai nieko nuostabaus, atsižvelgiant į daugybę su saugumu susijusių grėsmių, kurios yra organizacijos kasdienybė. Teorinė ši darbo dalis yra paremta kibernetinio saugumo supratimo ir kibernetinės saugumo kultūros organizacijoje teoriniais aspektais.

1.1. Kibernetinio saugumo samprata

Šiuolaikinio tarpusavyje susieto pasaulio galimybės yra neišmatuojamos. Šiandien žmonės, el. erdvėje, keičiasi bet kokios formos duomenimis: el. laiškai, balso žinutės, vaizdo įrašai ir pan. Informacija perduodama kibernetinėje erdvėje gali būti pažeista be siuntėjo žinios, tačiau retas kuris eilinis vartotojas pagalvoja kaip saugiai jo duomenys yra perduodami kitam be jokio informacijos nutekėjimo ir už to slypi kibernetinis saugumas. Šiandien internetas bei su juo susijusi veikla sparčiai plečiasi ir daugybe naujausių technologijų keičia bei formuoja žmonių kasdieninio gyvenimo infrastruktūrą. COVID-19 pandemijos metu interneto naudojimas padidėjo, visi pradėjome daug dažniau naudotis internetu savo kasdieniams darbams atlikti. Kibernetinė erdvė, kupina technologijų ir informacijos, yra neatsiejama šių dienų visuomenės dalis. Deja , kadangi technologijų nauda auga, plečiasi ir tobulėja, kartu tobulėja ir kibernetiniai nusikaltėliai bei didėja grėsmės e. erdvėje. Taigi kibernetinis saugumas, galima sakyti, yra naujas iššūkis mums visiems vartotojams.

Kas yra ir kam reikalingas kibernetinis saugumas? <...*kibernetinė erdvė yra nauja, sudėtinga, daugialypė ir ne iki galo ištirta sritis..*><... *Europos Sąjunga neturi bendros "kibernetinio saugumo" apibrėžties, vieningo supratimo ir (arba) bendros vizijos. Daugelis ES valstybių narių turi savo kibernetinio saugumo strategijas ir savą kibernetinio saugumo sampratą...*> (Giantas, 2019, p.7). Lietuvos Respublikos kibernetinio saugumo įstatyme kibernetinis saugumas tai – *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* (LRV Nutarimas dėl Lietuvos Respublikos Kibernetinio saugumo įstatymo įgyvendinimo, 2018 .).

Kibernetinis saugumas susijęs tiek su žmonėmis, tiek su sistemomis, nes žmonių kibernetinio saugumo supratimas – tai jų žinios, įsitikinimai, požiūris, normos ir vertybės, geriausios praktikos ir rizikos, susijusios su jų skaitmeninio turto, privatumo internete ir informacijos saugumo apsauga, suvokimas ir kaip tai pasireiškia žmonių elgesyje su informacinėmis technologijomis (ENISA, 2017). Kibernetinio saugumo supratimo lygis gali skirtis tarp atskirų asmenų ir gali priklausyti nuo tokių veiksmų kaip išsilavinimas, patirtis ir susidūrimas su technologijomis. Apskritai žmonių kibernetinio saugumo supratimas gali būti nuo minimalaus iki pažangaus. Kai kurie asmenys gali turėti pagrindinį supratimą apie įprastas kibernetinio saugumo sąvokas, pvz.: naudoti stiprius slaptažodžius, būti atsargiems ir nespausti įtartinų nuorodų ar neatsisiųsti jiems nežinimų priedų ir nuolat atnaujinti savo įrenginius bei įrangą. Taip pat jie gali suvokti kaip svarbu apsaugoti savo asmeninę informaciją ir atidžiai stebėti savo veiklą internete. Labiau kibernetinį saugumą išmanantys asmenys gali turėti daugiau žinių apie įvairias kibernetines grėsmes, pvz.: kenkėjiškas programas, sukčiavimo atakas ir socialinės inžinerijos taktikas. Atitinkamai tokie žmonės gali būti susipažinę ir su daugiau techninių sąvokų , pvz.: šifravimas, daugiafaktoriniu autentiškumo patvirtinimu, tinklo saugumu ir pan. Taip pat, galima numanyti, kad jie galimai geriau supranta teisinius ir etinius kibernetinio saugumo aspektus, o taip pat kibernetinio saugumo pasekmes įmonėms ir organizacijoms, vyriausybei ir visai visuomenei (Zwilling, 2022).

Klaidinga manyti, kad kibernetiniams piktavaliams jus neįdomus. Šiandien kibernetinio saugumo reikia visiems, kurie yra prisijungę prie interneto. Taip yra todėl, kad dauguma kibernetinių atakų yra automatizuotos ir jomis siekiama pasinaudoti bendromis pažeidžiamomis vietomis, o ne konkrečiomis interneto svetainėmis ar organizacijomis. Kibernetinis saugumas atlieka svarbų vaidmenį IT srityje. Kibernetinis saugumas tapo pasauliniu iššūkiu ir šiuos iššūkius dar labiau sustiprina besivystantis dirbtinis intelektas, kuris kibernetinio saugumo specialistams kelia vis naujų užduočių (ENISA, 2022).

1.2. Kibernetiniai iššūkiai

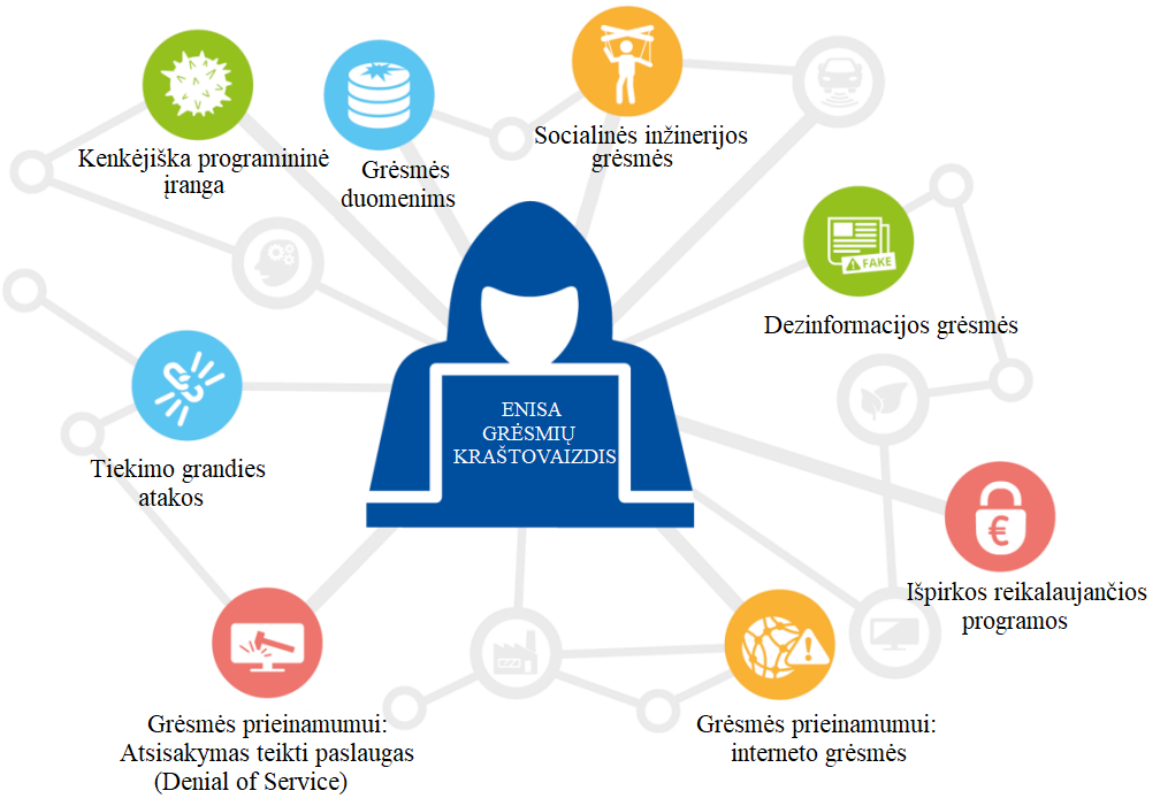
Dauguma pažeidimų įvyksta dėl to, kad darbuotojai nesilaiko organizacijos saugumo politikos (Ertan ir kt., 2018). Yra dviejų tipų organizacijos – tos į kurias jau buvo įsilaužta ir tos į kurias dar bus. Todėl šiuolaikinėje skaitmeninėje aplinkoje, kai visas pasaulio ritmas priklauso nuo interneto ir technologijos sparčiai tobulėja, organizacijoms tapo labai svarbu suprasti ir valdyti rizikas. Naujos technologijos kelia pavojų saugumui, kibernetinio saugumo incidentų vis daugėja. Dirbtinis

intelektas, daiktų internetas, robotai, savaeigiai automobiliai ir kt. tai jau nebėra ištraukos iš fantastinio filmo tai vis sparčiau tampa mūsų kasdienybė ir tokie įvykiai kaip COVID-19 pandemija bei didėjantys socialiniai ir politiniai neramumai priverčia vis dažniau kalbėti apie kibernetinį saugumą. 2022 metų I ketvirtį, Rusijos išpuolio prieš Ukraina kontekste, stebimas kibernetinių incidentų padidėjimas. Siekiant išvengti kibernetinio saugumo atakų, svarbiausia yra aktyvi apsauga (ENISA, 2022). Kompiuteriuose gali būti įdiegta pažangiausia ir geriausia saugumo programinė įranga, bet jei naudotojas nėra tinkamai apmokytas ir neišmano kertinių kibernetinio saugumo principų tai iš esmės galima teigti, kad nėra jokio saugumo. Kad dauguma kibernetinių atakų prasideda nuo žmogiškojo veiksnio, nesunku paaiškinti – išpuoliams neturi įtakos organizacijos infrastruktūros sudėtingumas, nes incidentai įvyksta bet kurioje organizacijoje ir visada panašiai. Darbuotojai yra universalūs įrankiai, kuriais piktavaliai gali prisijungti prie vidaus sistemų, nes jais galima emociškai manipuliuoti (Zwilling, 20220. Viešajame sektoriuje kibernetiniai incidentai laikomi vienu sudėtingesnių reiškinių su kuriais šiandien susiduriama. 2022 m. spalio mėn., vyko kibernetinio saugumo pratybos „Kibernetinis skydas 2022“, pratybų rezultatai – sukčiais patikėtų kas aštuntas darbuotojas (KAM, 2022). Taip pat 2022 m. spalio mėn. Valstybės kontrolės ataskaitoje pateikti rezultatai : *Tobulintina kibernetinio saugumo užtikrinimo sistema, nes: nacionaliniu lygiu neužtikrinamas tinkamas kibernetinio saugumo rizikos ir incidentų valdymas, nesudarytos tinkamos sąlygos vykdyti atitikties saugumo reikalavimams stebėseną, vis dar nekonsoliduotas kibernetinio saugumo ir elektroninės informacijos saugos teisinis reguliavimas, neužtikrinamas nuoseklus kibernetinio saugumo planavimo įgyvendinimas*<...> (Valstybės kontrolė, 2022).

Duomenys rodo, kad informacijos saugumo incidentai vis dažniau kyla dėl vidaus darbuotojų veiksmų. Saugumo paslaugų teikėjo „1 Password“ JAV ir Kanadoje atliktas tyrimas rodo, kad patys darbuotojai tapo labiau pažeidžiami (Sosafe, 2022). Taip pat išvarginti pandemijos ir paveikti nuotolinio darbo, žmonės mažiau rūpinasi kibernetine higiena, todėl yra labiau linkę daryti klaidas (RISC, 2021). Tai ypač aktualu organizacijų saugumo specialistams, kurie dėl šių pokyčių patiria didesnį spaudimą nei anksčiau (ISACA, 2022).

Taigi apžvelkime su kokiomis, ekspertų teigimų, kibernetinėmis grėsmėmis susiduriame. Remiantis ES Tarybos ir Europos Vadovų tarybos duomenimis kibernetinių išpuolių ir kibernetinių nusikaltimų skaičius Europoje auga ir jie tampa vis sudėtingesni. Ten pat pateiktas infografikas su glaustai aprašomomis pagrindinėmis kibernetinės grėsmės (consilium.europa.eu).

Plačiau apie kibernetines grėsmes ES yra pateikta kasmetinėje ENISA Grėsmių kraštovaizdžio 2022 ataskaitoje (Enisa Threat Landscape 2022). Pateiktoje ataskaitoje – ataskaitiniu laikotarpiu 2021 liepa – 2022 liepa, nustatytos pagrindinės kibernetinės grėsmės (1 pav.).



Šaltinis: išversta pagal „Enisa Threat Landscape 2022“, psl. 10

1 pav. **ENISA grėsmių kraštovaizdis 2022 - pagrindinės grėsmės**

Išpirkos reikalaujančios programos – ataskaitiniu laikotarpiu išpirkos reikalaujančios programos užėmė 1 vietą. Išradingi grėsmių sukėlėjai pasinaudojo nulinės dienų išnaudojimo atvejais. Geopolitika ir toliau daro didelį poveikį kibernetiniam saugumui. Per Rusijos ir Ukrainos konfliktą pastebėta, kad kibernetiniai veikėjai vykdė operacijas kartu su kinetiniais kariniais veiksmais. Nauja haktivizmo banga ypač pastebima nuo Rusijos ir Ukrainos krizės pradžios. Mašininio mokymosi (ML) modeliai yra šiuolaikinių paskirstytų sistemų pagrindas ir vis dažniau tapti atakų taikiniu. Labai padaugėjo atakų prieš prieinamumą, o ypač **atkirtimo nuo paslaugos tipo atakų** (angl. distrib-uted denial of service, DDoS), atakos darosi vis didesnės ir sudėtingesnės, persikelia į mobiliuosius tinklus ir daiktų internetą ir yra naudojami kibernetinio karo tikslais, o pagrindinė tokių atakų priežastis – vykstantis karas. Dažniausiai pasitaikantis pirminės prieigos vektorius vėlgi yra sukčiavimas. Šį augimą lėmė sukčiavimo rafinuotumas, naudotojų nuovargis ir tikslinis, kontekstu pagrįstas

sukčiavimas. **Kenkėjiškų programų** vėl daugėja po to, kai buvo pastebėtas ir su COVID-19 susietas sumažėjimas. Naudodami sutikimo apgaulę užpuolikai siunčia naudotojams nuorodas, kurias spustelėjus, užpuolikui suteikiama prieiga prie programų ir paslaugų. Vis dažniau įvyksta **duomenų pažeidžiamai** – nuolatinis ir nesustabdomas duomenų kompromitavimo didėjimas. Todėl dėl pagrindinio duomenų vaidmens mūsų visuomenėje smarkiai išaugo renkamų duomenų kiekis ir tinkamos duomenų analizės svarba. Valstybei priklausančios sertifikatų institucijos (CA) leidžia lengvai perimti HTTPS duomenų srautą ir vykdyti "man-in-the-middle" atakas prieš savo piliečius, todėl kyla **pavojus interneto saugumui ir privatumui**. **Dezinformacija** yra kibernetinio karo priemonė. Ji buvo naudojama dar prieš prasidedant "fiziniam" karui kaip parengiamoji veikla Rusijos invazijai į Ukrainą. **Dezinformacija** ir giluminės klastotės, kurias įgalina dirbtinis intelektas. Daugėjant botų, modeliuojančių asmenybes, galima lengvai sutrikdyti taisyklių priėmimo procesą ir bendruomenės sąveiką, užtvindant vyriausybines agentūras suklastotais komentarais. • Grėsmių grupuotės vis labiau domisi **tiekimo grandinės atakomis** ir atakomis prieš valdomų paslaugų teikėjus (angl. Managed Services Providers, MSP) ir didina jų pajėgumus (ENISA, 2022).

Remiantis 2021 m. ENISA ataskaita Informuotumo apie kibernetinį saugumą didinimas (angl. Raising awareness of cybersecurity, 2021 m., ENISA) kibernetinis saugumas išlieka vienas svarbiausių iššūkių valstybėse. Visuomenės informuotumas vis dar yra ribotas, beveik visi yra girdėję apie kibernetinį saugumą ir jo svarbą, tačiau piliečių elgesys ne visada atspindi aukštą informuotumo lygį. Kibernetinis saugumas yra labai svarbus asmenims ir viešosioms bei neviešosioms organizacijoms, tačiau laikytis saugumo praktikos dažnai būna sudėtinga (ENISA, 2021).

1.3. Kibernetinio saugumo kultūra organizacijose

Už tvarios kibernetinio saugumo kultūros kūrimą yra atsakinga ne tik organizacijos saugumo komanda, bet ir visų darbuotojų bendros pastangos. Kiekvienas darbuotojas atlieka svarbų vaidmenį užtikrinant organizacijos informacijos, sistemų ir turto apsaugą. Organizacijos kultūra – tai elgesys ir procesai, kurių darbuotojai turi laikytis. Kadangi darbuotojų elgesys, tyčinis ar netyčinis, yra vienas iš pagrindinių saugumo problemų šaltinių, svarbu, kad saugumo kultūra nuo pat pradžių būtų giliai integruota į organizacijos kultūrą. Tvarią saugumo kultūrą galima sukurti tik tada, kuomet visi darbuotojai žino apie riziką ir aktyviai dalyvauja ją mažinant. Norint to pasiekti organizacijos turėtų teikti pirmenybę visų darbuotojų kibernetinio saugumo supratimo mokymams (Nobels, 2018). Kibernetinė saugumo kultūra reiškianti bendras vertybes, įsitikinimus, elgseną ir praktiką,

atsirandančią žmonėms bendraujant per skaitmenines technologijas, tapo neatsiejama šiuolaikinės darbo vietos dalimi (Reegard, 2019).

Šiandien, turime daug puikių technologijų, kurios užtikrina sistemų ir duomenų apsaugą. Tačiau štai bėda – vis susiduriama su pažeidimų problema ir apsaugoti organizacijos jaurią skaitmeninę informaciją nuo kibernetinių atakų vis dar yra labai didelis iššūkis. Viešasis sektorius ir ne tik dažnai nesugeba apsaugoti savo informacinio turto, nes visų pirma yra priklausomas nuo technologinių sprendimų. Dabar valstybės tarnautojai, norėdami atlikti savo darbą, turi naudotis įvairiomis skaitmeninio bendravimo formomis, įskaitant elektroninį paštą, trumpąsias žinutes ir vaizdo konferencijas. Dėl šių technologijų bendravimas tapo greitesnis ir efektyvesnis, tačiau atsirado ir naujų iššūkių, pavyzdžiui, privatumo ir duomenų saugumo išlaikymas. Kibernetinė kultūra taip pat turėjo įtakos valstybės tarnautojų bendradarbiavimo ir dalijimosi žiniomis būdui (RISC, 2021). Todėl kibernetinio saugumo sąmoningumo didinimo visuomenėje yra itin aktuali kibernetinio saugumo tema. Organizacijoms reikia gilintis ir suprasti, kodėl darbuotojai ignoruoja organizacijos saugumo politiką, o ypač tokiose organizacijose, kur jau yra įdiegta informuotumo apie kibernetinį saugumą programa. Didėjant saugumo pažeidimo skaičiui, kuriuos sukelia darbuotojų saugumo politikos nesilaikymas, organizacijai tai tampa dideliu rūpesčiu. Kibernetinio saugumo supratimo ir įgūdžių poreikis tampa vis aktualesnis dėl mūsų priklausomybės nuo informacinių ir ryšių technologijų (IRT) visose mūsų visuomenės gyvenimo srityse (ENISA, 2021). Žmonės yra pagrindiniai kibernetinio saugumo dalyviai, o siekiant sumažinti riziką kibernetinėje erdvėje reikia didinti žmonių sąmoningumą šioje srityje. Remiantis informacija iš kibernetinio saugumo ataskaitų, galime matyti, kad kibernetinio saugumo incidentai pastaraisiais metais daugeliu atveju tapo brangesni, labiau trikdantys ir neretai politiniai. Kibernetinis saugumas daro gana reikšmingą poveikį viso pasaulio socialiniam vystymuisi (ENISA, 2022).

Remiantis ENISA kibernetinio saugumo kultūros organizacijose (angl. Cyber Security Culture in organisations, 2017) didelė dalis duomenų pažeidimų, įvyksta dėl žmonių kaltės ir neretai technologiniai saugumo sprendimai negali pilnai apsaugoti organizacijos, o ypač jei tokie sprendimai dėl kompetencijų trūkumo yra netinkamai įdiegti ar netinkamai naudojami, o neretai ir nenaudojami. Pateikiama nemažai pavyzdžių kai dėl darbuotojo netinkamo elgesio organizacijai gali kilti kibernetinių grėsmių. Nors organizacijose ir taikoma kibernetinio saugumo politika, tačiau darbuotojai tai labiau linkę laikyti saugumo gairėmis, bet ne taisyklėmis ir todėl bendravimas kibernetinio saugumo klausimais yra sudėtingas uždavinys (Ertan ir kt., 2018). Nesilaikant organizacijos saugumo politikos savaime yra ugdomi netinkami įpročiai, kurie didina duomenų

praradimo ar atskleidimo riziką. Kitas iššūkis nuolat besikeičianti technologijų, o kartu ir naujų grėsmių aplinka, todėl saugumo kultūros vystymas ir pritaikomumas organizacijose neturėtų būti paskutinėje vietoje. ENISA (2017) Kibernetinio saugumo kultūra organizacijose (angl. Cyber Security Culture in organisations), pažymima, kad sėkminga organizacijos kibernetinio saugumo kultūra formuoja visų darbuotojų (įskaitant saugumo komandą) mąstymą apie saugumą, didina atsparumą visoms kibernetinėms grėsmėms, o ypač toms, kurios inicijuojamos socialinės inžinerijos būdu. Kibernetinio saugumo kultūra padeda išvengti apsunkinančių saugumo priemonių, kurios trukdo darbuotojams veiksmingai vykdyti pagrindines verslo funkcijas. Ten pat pateiktas ir organizacijų kibernetinio saugumo apibrėžimas - tai žmonių žinios, įsitikinimai, suvokimas, nuostatos, prielaidos, normos ir vertybės, susijusios su kibernetiniu saugumu, ir tai, kaip jos pasireiškia žmonių elgesyje su informacinėmis technologijomis (ENISA, 2017).

Sėkmingos kibernetinio saugumo kultūros programos kūrimas ir įgyvendinimas organizacijose - tai užduotis, kuriai reikia įvairiapusio ir diferencijuoto požiūrio, įtraukiant vyresniąją vadovybę ir kitus darbuotojus. Kultūra apima ne tik sąmoningumą, bet ir įsitikinimų, normų, vertybių formavimą. Reikia, kad vyresnioji vadovybė, kibernetinio saugumo įgyvendintojai ir darbuotojai abipusiai suprastų, kokias funkcijas, atsakomybę ir praktiką jie turi atlikti siekdami apsisaugoti nuo kibernetinių nusikaltimų (ENISA, 2017). Ataskaitoje yra sudaryta rekomendacija kaip žingsnis po žingsnio organizacijose galima būtų ugdyti kibernetinio saugumo kultūrą. Kibernetinės saugumo kultūros procesas nėra griežtai linijinis, o pasikartojantis arba kitaip – žiedinis. Grįžti prie ankstesnių procesų reikia sugrįžti kuomet tobulinama kibernetinio saugumo kultūros veikla. Tobulinant kibernetinio saugumo kultūrą pasirenkama nauja veikla ir tobulinti organizacijos elementai į kuriuos būtina susikoncentruoti bei parenkant tikslinius darbuotojus į kuriuos orientuota kibernetinio saugumo kultūros veikla, poreikiui esant keičiami tikslai.

Žingsnis po žingsnio kibernetinės saugumo kultūros programos įgyvendinimo planas (2 pav.).

Pirmas žingsnis – sukurti pagrindinę kibernetinio saugumo kultūros grupę.

Antras žingsnis – organizacijos veiklos supratimas ir rizikos vertinimas.

Trečias žingsnis – apibrėžti pagrindinius tikslus, sėkmės kriterijus ir tikslines auditorijas.

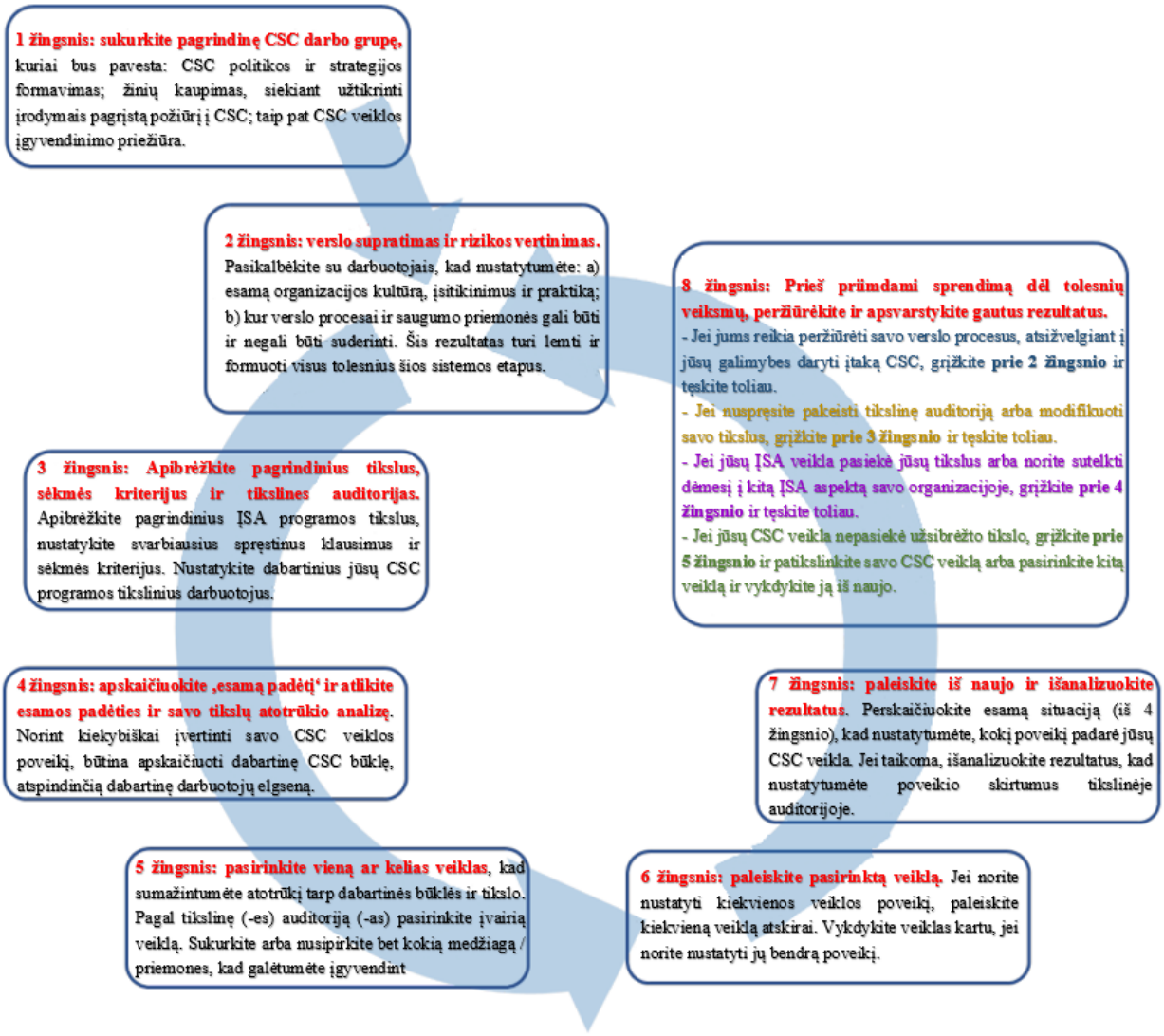
Ketvirtas žingsnis – apskaičiuoti dabartinę padėtį ir atlikti dabartinės padėties ir savo tikslų atotrūkio analizę.

Penktas žingsnis – pasirinkti vieną ir daugiau veiklų.

Šeštas žingsnis – paleisti (testuoti) pasirinktą veiklą.

Septintas žingsnis – pakartotinai paleisti dabartinės situacijos veiklą ir išanalizuoti rezultatus.

Aštuntas žingsnis – prieš priimant sprendimą dėl tolesnių veiksmų, peržiūrėti ir apsvarstyti gautus rezultatus.



Šaltinis: išversta pagal "Cyber Security Culture in organisations" ENISA 2017 m. p. 10

2 pav. **Rekomendacijos KSK programos įgyvendinimui organizacijose**

Taigi, remiantis pateikta informacija ataskaitoje, galime teigti, kad kibernetinio saugumo klausimui spręsti organizacijoje reikia papildomų pastangų, o tai be abejo gali turėti įtakos darbuotojų elgsenai ypač jei organizacijos viduje nėra iki galo iškomunikuota apie saugumo reikalavimų naudą bei sąnaudas. Žmonės patys sukuria palankią aplinką grėsmėms ir pažeidžiamumas todėl reikia kurti ir palaikyti kibernetinio saugumo kultūrą (Reegard ir kt. 2019).

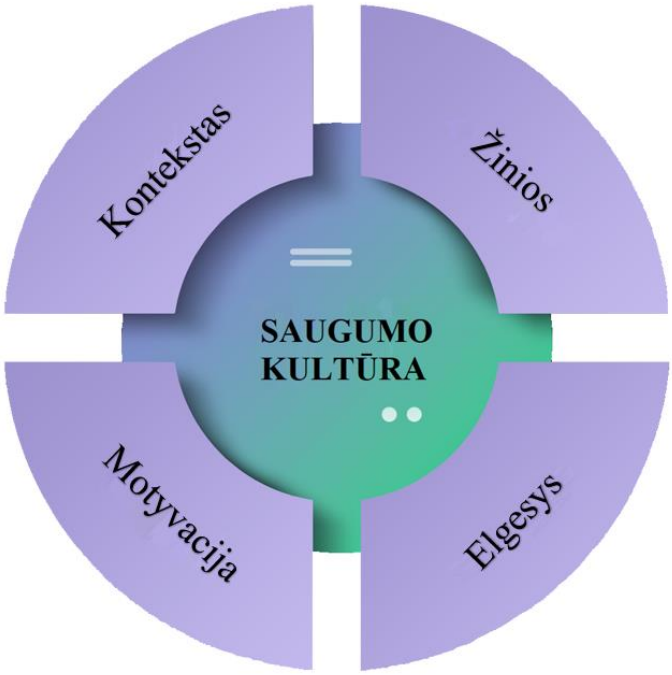
Taigi norint turėti aukštą KSK lygį, organizacijos užduotis – glaudus darbuotojų tarpusavio bendradarbiavimas. Organizacija turėtų aiškiai įvardinti, o žmogus suprasti kokios yra grėsmės, su kuriomis jie susiduria; kokia yra saugumo politika organizacijos viduje, kurios visi turi laikyti bei atsakomybė, kuria kiekvienas turi prisiimti.

Taigi jei organizacija imsis tinkamų veiksmų ir sukurs tvirtą kibernetinio saugumo kultūros pagrindą – turės stiprią kibernetinio saugumo kultūrą ir veiksmingą gynybą nuo kibernetinių atakų.

1.4. Kibernetinio saugumo organizacijoje modeliai

Į bet kokią informaciją, finansinę, karinę, vyriausybine ar asmenine, saugoma kibernetinėje erdvėje gali būti įsibrauta. Todėl labai svarbu turėti mechanizmus, kurie galėtų pagerinti bendruomenės bei organizacijų kibernetinio saugumo padėtį. Jei žmogus žinos kaip elgtis, kad išvengtų rizikos tai turės didelės naudos. Todėl organizacijoms reikia patikimų sąmoningumo skatinimo priemonių, kad netaptų kibernetinių nusikaltėlių aukomis. Vienas iš būdų kaip galima išugdyti stiprią kibernetinio saugumo kultūrą – kibernetinio saugumo modelių pritaikymas organizacijose.

SoSafe organizacijos pateiktoje ataskaitoje „Human Risk Review 2022“ apžvelgiamos kibernetinio saugumo tendencijos bei informuotumo didinimo metodai, kuriuos rekomenduojama taikyti organizacijoms, kad jos gebėtų apsisaugoti nuo vis sumanesnių kibernetinių nusikaltėlių. Ataskaitoje teigiama, kad 85% atakų prasideda nuo žmogiškojo veiksnio, nes individą visada galima atakuoti naudojant panašius būdus, net jei pačios priemonės ir skiriasi. Tačiau tuo pat metu žmogus yra svarbus ir apsaugant organizaciją nuo kibernetinių atakų – kitaip sakant žmogus organizacijai tuo pat metu yra ir jos turtas ir jos grėsmė. Todėl teisingas žmogaus elgesys gali apsaugoti organizacijas nuo didelių nuostolių. Tikslas yra kurti tvarią saugumo kultūrą, padėti žmogui matyti savo elgesį ir paskatinti praktikuoti saugią elgseną. Minėtoje ataskaitoje aprašomas vienas iš kibernetinio saugumo modelių - Elgsenos saugumo modelis (*The Behavioral Security Model*) (3 pav.). Šiuolaikinės saugumo kultūros tikslas nėra suteikti tik sausas žinias ar pažymėti *varneles,* vietoj to ji turėtų padėti ir motyvuoti individą pažvelgti į savo elgesį ir praktikuoti saugumo gaires. *Sisteminės sąmoningumo didinimo priemonės gali iki 90% sumažinti sėkmingo sukčiavimo atakos riziką* (Sosafe, 2022). Pateiktame Elgsenos saugumo modelyje yra keturios kryptys į kurias rekomenduojama atsižvelgti vienodai.



Šaltinis: išversta pagal „Human Risk Review 2022“, p. 51

3 pav. **Elgsenos saugumo modelis**

Kontekstas - ne kiekvienas asmuo organizacijoje turi tą patį pradinį žinių lygį: atskiras žmogaus vaidmuo turi didelę įtaką kibernetinės rizikos vystymuisi. Pavyzdžiui, darbuotojai einantys vadovaujančias pareigas, žmonės, turintys įmonės mobilųjį telefoną, žmonės, turintys tam tikrų prieigos teises ir priemones arba finansų skyriaus darbuotojai priskiriami didesniam pavojui, nes kibernetiniai nusikaltėliai naudojasi jų padėtimi tikslinėms atakoms. Taip pat įtakos rizikai turi įmonės pramonės šaka.

Todėl organizacijos turėtų sukurti sąlygas, kurios būtų palankios saugiam elgesiui. Pavyzdžiui, jei nėra sukurtos pranešimų teikimo grandinės ar aiškių kontaktinių asmenų galimų incidentų įmonėje, atitinkamas elgesys pranešant tampa labai sudėtinga. Kita vertus, jei darbuotojai gali greitai pranešti apie įtartinus elektroninius laiškus ir lengvai, pavyzdžiui, naudodami mygtuką "Pranešti apie sukčiavimą" (angl. Phishing Report Button), tai gerokai palengvina veiksmus atitinkamai. Remiantis "SoSafe" platformos duomenimis, iki 70 proc. aktyviai įsitraukti į gynybą įdiegus mygtuką. Naudodamiesi šiuo kolektyviniu sąmoningumą galima išvengti daugybės potencialiai pavojingų situacijų.

Kartu kontekstas turi būti suprantamas kitaip. Asmeninis kontekstas darbuotojų daro įtaką individualiai mokymosi patirčiai. Pavyzdžiui, ne visiems darbuotojams reikia informacijos, kaip saugiai naudotis įmonės mobiliuoju telefonu, jei jie apskritai juo nesinaudoja. Todėl mokymosi patirtis

turėtų būti pritaikyta darbuotojams: Pavyzdžiui, personalizuotuose mokymosi kuriuose išsamiau aptariami individualūs besimokančiųjų rezultatai ir tai, ko jie išmoko, siekiama paversti apčiuopiama ir aktualia nauda.

Žinios - norint parodyti tam tikrą elgseną, reikia turėti žinių apie teisingą elgseną. Todėl pirmas žingsnis link tvirtos saugumo kultūros tradiciškai yra žinių suteikimas, pavyzdžiui, kaip sukurti saugius slaptažodžius arba kaip atpažinti apgaulingus elektroninius laiškus. Tačiau anksčiau žinios buvo dažnai perduodamos linijiniu būdu ir didelėmis dozėmis. Po ilgų vaizdo įrašų ar seminarų sekdavo paprastas žinių testas, kuris pademonstruodavo ko išmokta. Tačiau jau seniai žinoma, kad linijinis ir masinis mokymasis tik ribotu mastu padeda įgyti ilgalaikių žinių. Jau šeštajame dešimtmetyje vokiečių psichologas Hermanas Ebbinghausas įrodė, kad moksleiviai pamiršta didžiąją dalį dalykų jau po kelių dienų. Ebbinghausas taip pat nustatė, kad stabili atmintis engramos (žinių "įspaudai" smegenyse) geriau formuojasi, kai žinios yra dalijamos ir aktyviai kartojamos (Sosafe, 2022). Todėl, norėdamos perduoti kibernetinio saugumo žinias, organizacijos turėtų pasitelkti mokymosi psichologija pagrįstų metodų. Modulinis mokymas ir nuolatinis skatinimas mokytis išlygina užmaršumo kreivę ir taip ilgainiui sumažina žmogiškąją riziką. Rezultatai "SoSafe Awareness" platformos rezultatai rodo, kad nuolatinis mokymas didina įsitraukimą 30 proc. ir net iki 90 proc. įvadiniame etape. Štai kaip darbuotojai efektyviai ir tvariai įsimena žinias.

Motyvacija - saugiam elgesiui visada turi įtakos tam tikri veiksniai. Tai galima lengvai iliustruoti pasitelkiant kasdienį kelių eismo pavyzdį: nors žinome, kad mums draudžiama važiuoti 80 km/h miesto centre, taip pat turime suprasti, kodėl, kad iš tikrųjų laikytumėmės taisyklių. Esant stipriai saugumo kultūrai, darbuotojai ne tik žino apie kibernetinę riziką bet ir supranta, kaip jie gali aktyviai kovoti su ja savo individualiomis aplinkybėmis. Tokiai kultūrai būdinga tai, kad ji palanki dalyvių motyvacijai ir pabrėžia priemonių aktualumą. Už motyvacijos ir saugumo kultūros stiprinimą organizacijoje atsakinga vadovybė ir tai apima procesų pritaikymą pagal informacijos saugumo aspektus ir tai yra pokyčių valdymo klausimas. Naujausi tyrimai rodo, kad vadovų įsipareigojimas vaidina lemiamą vaidmenį. Jei vadovai įtraukia darbuotojus ankstyvuoju etapu ir tiesiogiai su jais bendrauja, darbuotojai daug labiau linkę keisti savo elgseną ir net patys skatinti plėtrą, o tai teigiamai veikia žmogiškosios rizikos mažimo aspektą. Akivaizdų poveikį turi ir žaidimų taikymas mokymų metu: naudojant šį metodą, saugumo suvokimo mokymų aktyvumo lygis padidėja iki 50 % (Sosafe, 2022).

Elgesys - galiausiai žmogiškoji rizika organizacijoje priklauso nuo to, kaip gerai darbuotojai išmoko ko buvo mokomi, įgyvendina praktiškai ir puoselėja saugias idėjas. Kontekstas, žinios, ir motyvacija.

Tačiau lemiamą reikšmę turi tai kiek saugus elgesys tampa "kūnu ir krauju". Norint mokyti saugaus elgesio, svarbu suteikti reikiamų žinių motyvuojančiu būdu, pavyzdžiui, pasitelkiant žaidimo priemones. Elgesio psichologija taip pat rodo: ypač nuolatinis, atsitiktinis mokymasis stiprina įpročius. Išugdytas elgesys nuolat išbandomas atliekant nuolatines atakų simuliacijas, pavyzdžiui, įtraukiamas į aktyvią darbuotojų atmintį. Rezultatai "SoSafe Awareness Platform" rodo, kad sukčiavimo paspaudimų skaičius išlieka žemas ir pranešimų dažnis laikui bėgant išlieka aukštas (Sosafe, 2022).

Kitas šiame darbe nagrinėjamas kibernetinio saugumo modelis yra Bendruomenės kibernetinio saugumo brandos modelis (*angl. Community Cyber Security Maturity Model, CCSMM*) (pav. 4), kurį sukūrė CIAS Infrastruktūros užtikrinimo ir saugumo centras (angl. The Center for Infrastructure Assurance and Security). CIAS yra Teksaso universiteto San Antonijuje (UTSA) dalis, kuri priklauso Nacionaliniam pasirengimo kibernetiniam saugumui konsorciumui (NCPC, 2023). Bendruomenės kibernetinio saugumo brandos modelio tikslas, kad tai veiktų kaip koordinuotas planas, kuris padėtų apsibrėžti ko reikia kuriant kibernetinio saugumo programą, orientuotai į visos bendruomenės pasirengimą ir reagavimą į kibernetinius incidentus. *CCSMM gali padėti bendruomenėms nustatyti, ką reikia padaryti kuriant gyvybingą ir tvarią kibernetinio saugumo programą, ko reikia norint pasirengti aptikti kibernetinę ataką, parengti planus, kaip reaguoti atakos metu, ir nustatyti, ką daryti įvykus atakai* (CIAS, 2023).

CCSMM apsibrėžia tris svarbiausias nuostatas: 1) Kriterijus, kuriuo galima įvertinti dabartinę bendruomenės kibernetinio saugumo programos ir padėties būklę, 2) veiksmų planas, padedantis bendruomenei sužinoti, kokių veiksmų reikia imtis, kad būtų pagerinta jos saugumo būklė, ir 3) bendras atskaitos taškas, leidžiantis skirtingų bendruomenių ir valstijų atstovams aptarti savo atskiras programas ir susieti jas tarpusavyje.

Bendruomenės kibernetinio saugumo brandos modelis turi penkis lygius ir kiekviename lygyje atvaizduojamos savybės, kuriomis bendruomenė turėtų pasižymėti keturių dimensijų atžvilgiu (4 pav.). Tobulinimo lygia yra sutelkti į keturias sritis – dimensijas (Sąmoningumas, dalijimasis informacija, politika ir planai).

Šaltinis: išversta pagal UTSA „The Community Cyber Security Maturity Model“ (CIAS)

4 pav. **Bendruomenės kibernetinio saugumo brandos modelis**

Pirmas lygis – pradinis: kai kurie procesai ar programos gali būti įdiegti, tačiau 1 lygio bendruomenė neturi visų pagrindinės programos elementų.

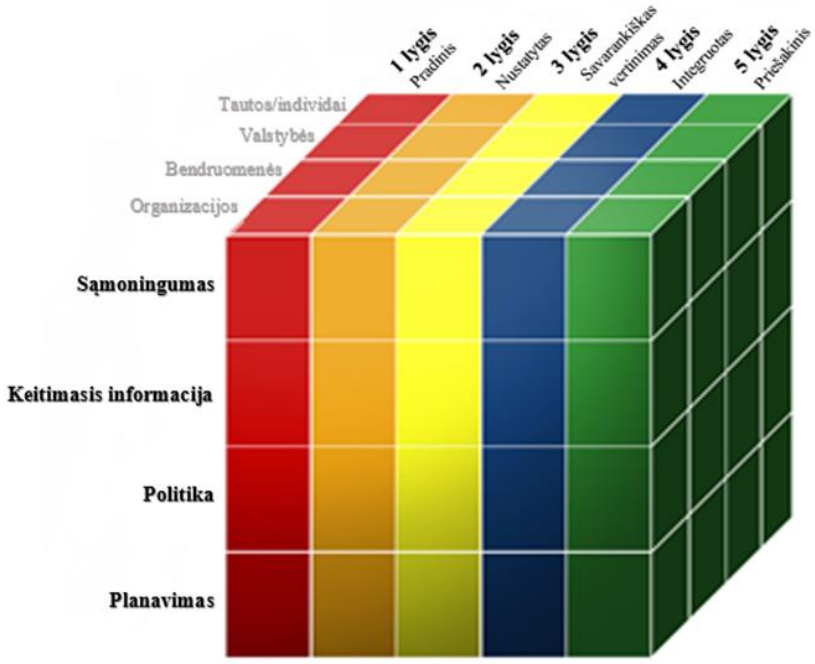
Antras lygis – nustatytas: nustatyta pagrindinė programa su visų keturių dimensijų elementais ir procesais.

Trečias lygis – savarankiškai vertinimas: įgyvendinta minimali gyvybinga ir tvari programa.

Ketvirtas lygis – integruotas: kibernetinis saugumas integruotas visoje bendruomenėje ir apima visus bendruomenės piliečius ir organizacijas. Ketvirto lygio bendruomenė taip pat bendradarbiauja su valstybe ir kitomis valstybinėmis bendruomenėmis.

Lygis penktas - priešakinis: bendruomenė laikosi visiškai budrios kibernetinio saugumo pozicijos.

Sukūrus dvimatį CCSMM modelį (4 pav.) išryškėjo, kad aukštesniuose modelio lygiuose reikia daugiau. Kaip galime matyti ketvirto lygio aprašyme – bendruomenės dalijasi informacija su valstybe ir su kitomis bendruomenėmis. Todėl tapo akivaizdu, kad šis modelis iš tiesu turėtų būti ir yra trimatis (5 pav.).



Šaltinis: adaptuota pagal UTSA „The Community Cyber Security Maturity Model“ (CIAS)

5 pav. **3D Bendruomenės kibernetinio saugumo modelis CCSMM kubas**

3D modelio (5 pav.) tikslas išplėsti sistemos galimybes, kad tai būtų lankstus ir pritaikomas įrankis visiems kibernetinio saugumo programos aspektams. Išplėtus CCSMM modelį į 3D modelį, užtikrinama visiems šalies gyventojams tobulėjimo pažanga. CCSMM kubas kaip planas, kuris pritaikomas: tautoms/individams, valstybėms, bendruomenėms ir organizacijoms (CIAS).

2. KIBERNETINIO SAUGUMO KONCEPTO RAIŠKA INDIVIDO LYGNEMYJE

2.1. Taikomųjų tyrimų, aptariant kibernetinį saugumą viešajame sektoriuje analizė

Darbuotojų suvokimas apie kibernetinį saugumą darbo aplinkoje yra labai svarbus saugios darbo vietos palaikymo aspektas. Tai reiškia, kiek darbuotojai supranta su kibernetiniu saugumu susijusią riziką ir kokį vaidmenį jie atlieka saugodami savo organizacijos skaitmeninį turtą. Kibernetinis saugumas yra glaudžiai susijęs su skaitmeninis raštingumu, nes skaitmeninio raštingumo įgūdžiai būtini, kad asmenys suprastų ir praktikuotų veiksmingą kibernetinį saugumą. Šiandien 90% darbų ir veiklų reikalingi skaitmeniniai įgūdžiai, technologijoms nuolat tobulėjant, svarbu nuolat atnaujinti ir tobulinti skaitmeninio raštingumo įgūdžius. Nors Lietuvoje gerinamas skaitmeninis raštingumas, tačiau pagal 2019 m. Europos Komisijos skaitmeninės ekonomikos ir visuomenės indeksą skaitmeninių įgūdžių lygis Lietuvoje vis dar žemesnis už ES vidurkį (Šarpienė, 2019). Skaitmeninė transformacija neaplenkė ir viešojo sektoriaus, teikiamos viešosios paslaugos su pagreičiu perkeliamos į skaitmeninę erdvę tai ypač išryškėjo COVID – 19 pandemijos metu. Vis daugiau dirbama su vis augančiu jautrios informacijos srautu. Todėl yra labai svarbūs darbuotojų skaitmeniniai įgūdžiai, nes kibernetinės atakos metu prarasti ar atskleisti tokio tipo duomenys gali sukelti daug žalos.

Toliau šiame darbe bus apžvelgti tyrimai bei ataskaitos susijusios su individo kibernetinio saugumo įgūdžiais bei viešojo sektoriaus gebėjimai apsisaugoti nuo kibernetinių grėsmių.

2.1.1. Ataskaitos „Lietuvos kibernetinio saugumo kompetencijų žemėlapis“ apžvalga

Šiame darbe apžvelgiant ataskaitą „Lietuvos kibernetinio saugumo kompetencijų žemėlapis“ susifokusuota į atliktą kokybinį tyrimą *„Visuomenės požiūrio į kibernetinį saugumą tyrimas“* (Bukauskas ir kt. „Ataskaita Lietuvos kibernetinio saugumo kompetencijų žemėlapis“, 2022 m. p.37) ir į žvalgomąjį tyrimą „*Žvalgomasis kibernetinio saugumo ir IT specialistų tyrimas*“ (L. Bukauskas ir kt. „Ataskaita Lietuvos kibernetinio saugumo kompetencijų žemėlapis“, 2022 m. p.53), nes abu šie tyrimai artimai koreliuoja su rašomo darbo tema.

Minimoje ataskaitoje kokybinio tyrimo tikslas buvo išsiaiškinti apie visuomenės kibernetinio saugumo sampratą bei koks yra kibernetinio saugumo švietimo poreikis. Taigi tyrimo rezultatai atskleidė, kad jaunesnioji (pagal amžių) visuomenės dalis jaučia kibernetinio švietimo trūkumą, o štai vyresnioji (pagal amžių) visuomenės dalis nežino arba nemano, kad tai yra svarbu. Atsiskleidžia ir gana ryškus skirtumas apie visuomenės kibernetinio saugumo švietimo poreikį tarp visuomenės sluoksnių. Mažesnes pajamas gaunančių, bedarbių ar be aukštojo išsilavinimo asmenys taip pat nežino

arba nemano, kad kibernetinis švietimas yra svarbu, o štai didesnes pajamas gaunantieji ir su aukštą išsilavinimą turintys asmenis identifikuoja, kad trūksta visuomenės švietimo apie kibernetinį saugumą bei kibernetines grėsmes. Didesnė visuomenės dalis vis dar tapatina IT srities specialistus su KS srities specialistais ir negali atskirti pagrindines šių specialistų funkcijas, trūksta ir *informacijos apie skirtingas KS specialisto roles ir galimybes įvairiausių profilių žmonėms siekti karjeros šioje srityje*.

Remiantis ataskaita jaunesnioji (pagal amžių) visuomenės dalis išreiškia susidomėjimą KS srityje ir noriai dalyvautų veikloje susijusia su kibernetiniu saugumu. Šiai dienai kibernetinio saugumo srityje daugiausiai dirba vyrų, tačiau moterys taip pat *palankiai vertina veiklos galimybes šioje srityje ir mano, kad jų turėtų būti apylygiai su vyrais*.

Tam, kad galima būtų išryškinti KS problematiką specialisto akimis, atliktas žvalgomasis tyrimas. Buvo siekiama surinkti Lietuvoje dirbančių kibernetinio saugumo specialistų nuomonę. Ekspertu nuomone KS saugumo specialistai turi turėti didesnį IT žinių bagažą. Privatus sektorius investuoja į savo specialistus, sudaro sąlygas mokytis ir tobulėti bei kelti kvalifikaciją. Tačiau viešajame sektoriuje, tas deja vyksta vangiai. Pažymėtina, kad trūksta įvairių rolių KS specialistų, tačiau didžiausias poreikis techninio profilio. Dėl šios priežasties dažnu atveju vienas darbuotojas dengia kelių rolių funkcijas.

Apibendrinat šio tyrimo dalį remiantis ataskaitos duomenimis Lietuvoje yra pakankamai žemas KS srities brandos lygis. Visuomenė tapatina KS specialistus su IT sistemų administratoriais ir yra susiformavusi nuomonė, kad KS funkcijas gali atlikti IT specialistai. Taip pat nustatyta, kad *KS specialistai mažai specializuoti, nes dauguma samdomų KS specialistų turi atlikti daug skirtingiems vaidmenims tenkančių veiklų* (Bukauskas ir kt., 2022).

2.1.2. Nacionalinės kibernetinio saugumo pratybos „Kibernetinis skydas 2022“ ataskaitos apžvalga

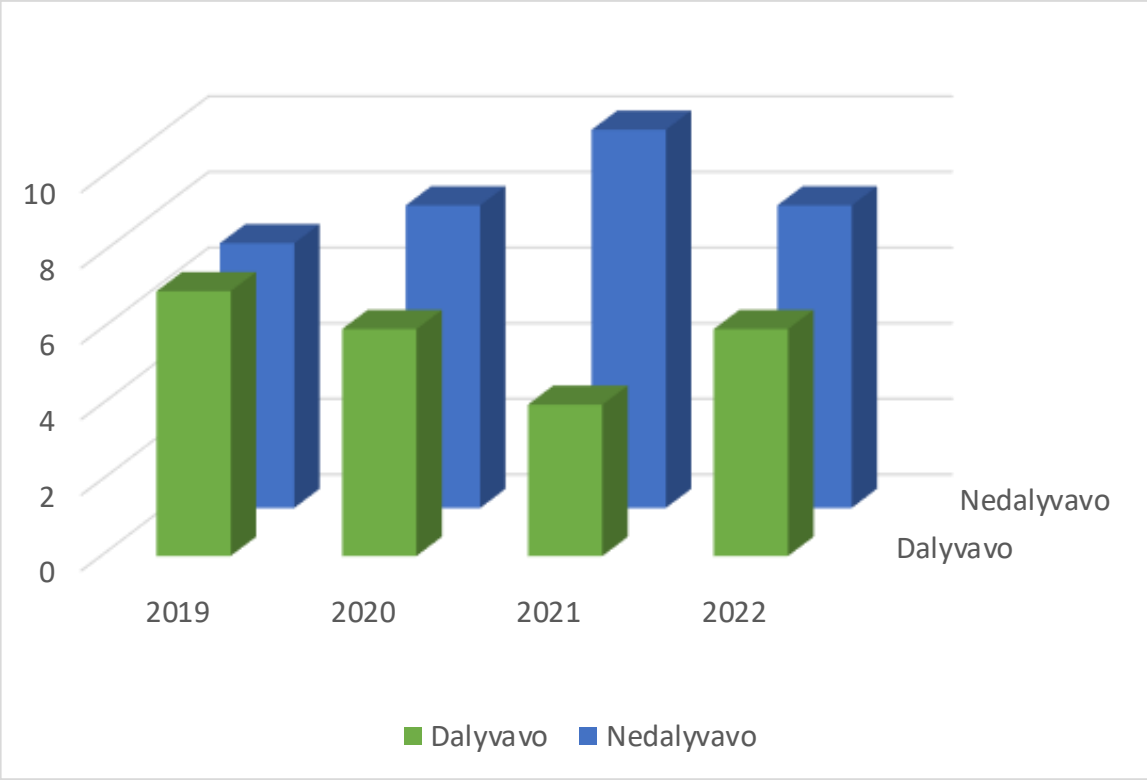
Kibernetinio saugumo pratybos skirtos padėti organizacijoms išbandyti kibernetinio saugumo mechanizmus, nustatyti silpnąsias vietas ir organizacijos pažeidžiamumą bei patobulinti reagavimo į incidentus procedūras. Dalyvauti šiose pratybose organizacijoms yra naudinga, nes pratybų metų gaunama vertingų įžvalgų. 2022 m. spalio 18-20 dienomis Nacionalinis kibernetinio saugumo centras (NKSC) prie Krašto apsaugos ministerijos, bendradarbiaudamas kartu su Kauno technologijos universitetu, organizavo didžiausias šiais metais nacionalines kibernetinio saugumo pratybas "Kibernetinis skydas 2022". Iš viso pratybose dalyvavo 116 organizacijų iš jų 107 dalyvavusios organizacijos yra valstybės informacinių išteklių valdytojai ir ypatingos svarbos informacinių išteklių

valdytojai arba tvarkytojai. Akcentuota, kad tai didžiausias dalyvių skaičius per visą tokių pratybų istoriją. Po pratybų vyko vietos instruktorių, kurie koordinavo pratybas savo organizacijose, apklausa. Rezultatai parodė, kad beveik visi (97 proc.) vietos instruktorių sutiko su teiginiu, jog pratybos "Kibernetinis skydas 2022" buvo naudingos jų organizacijoms, nes tai atskleidžia ties kuriais kibernetinio saugumo klausimais organizacijai reikia susikoncentruoti.

Kibernetinio saugumo pratybos gali atskleisti organizacijos saugumo priemonių pažeidžiamumą ir spragas, kurios anksčiau galėjo būti nepastebėtos. Šios pratybos gali padėti organizacijoms nustatyti sritis, kuriose vis dar reikia tobulėti. Pavyzdžiui organizacijos gali išbandyti savo reagavimo į incidentus planus ir procedūras imituojamoje aplinkoje. Tai gali padėti joms nustatyti reagavimo planų trūkumus ar neveiksmingumą ir atlikti reikiamus pakeitimus, kad pagerintų savo gebėjimą reaguoti į tikrą kibernetinę ataką. Taip pat organizacijoje svarbus darbuotojų bendravimo ir bendradarbiavimo aspektas. Pratybos taip pat gali padėti pagerinti įvairių organizacijos komandų ir skyrių bendravimą ir bendradarbiavimą. Dirbdamos kartu imituojamoje aplinkoje, komandos gali geriau suprasti savo funkcijas ir atsakomybę kibernetinės atakos metu ir sukurti veiksmingesnius bendravimo kanalus. Kibernetinio saugumo pratybos didina informuotumą apie kibernetinio saugumo svarbą bei moko darbuotojus geriausios kibernetinių grėsmių nustatymo ir reagavimo į jas praktikos. Tai gali padėti sumažinti žmogiškųjų klaidų ar aplaidumo riziką, dėl kurios gali įvykti sėkminga kibernetinė ataka.

Vis tik, remiantis ataskaita „Kibernetinis skydas 2022“ , dalyvių pratybose skaičius buvo nepakankamas, *kad būtų pasiektas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarime Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ nustatytas vertinimo kriterijus. 4 kriterijus „Nacionalinėse kibernetinio saugumo pratybose dalyvaujančių ypatingos svarbos informacinės infrastruktūros ir valstybės informacinių išteklių valdytojų dalis, ne mažesnė nei nurodyta“ 2021 m. – 60%, 2023 m. – 70%, tad numanomas 65% kriterijus 2022 m. nebuvo pasiektas. Faktiškai pasiekta 32,1 proc. arba 107 vnt. (pratybose KS2021 – 21,7% arba 87 vnt.).* Taip pat pažymėta, kad LR ministerijų dalyvavimas šiose pratybose buvo *vangus,* iš 14 ministerijų dalyvavo tik 6 ministerijos, palyginus 2019 - 2022 m. ministerijų aktyvumą dalyvaujant pratybose pastebima, kad kasmet sulaukiama mažesnio ministerijų įsitraukimo į kibernetinio saugumo pratybas. Tikėtina, kad dėl tokio neaktyvaus ministerijų dalyvavimo pratybose joms pavaldžios įstaigos irgi nesirenka dalyvauti pratybose ir tai kelia tam tikrą susirūpinimą. Visų pirma nepavyksta pasiekti nustatyto kriterijaus įgyvendinimo, o taip pat šių dienų kontekste dėl karinio konflikto

Ukrainoje nesame pakankamai pasiruošę atremti kibernetines atakas. Todėl svarbu paskatinti įstaigų įsitraukimą dalyvauti kibernetinio saugumo pratybose.



Šaltinis: adaptuota pagal ataskaitą „Kibernetinis skydas 2022“, 2022

6 pav. **LR ministerijų dalyvavimas pratybose „Kibernetinis skydas“**

2022 m. populiariausia ir dažniausiai dalyvaujančių organizacijų pasirinkta pratybų "Kibernetinis skydas 2022" siužetinė linija buvo socialinės inžinerijos instrumentas t.y. buvo vykdoma suklastotų laiškų arba *fišingo (*angl. *phishing)* simuliacija. Šio pratimo metu buvo siekiama patikrinti darbuotojų budrumą ir atsparumą tokio tipo atakoms. Ataskaitos duomenimis pratybų dalyviams buvo išplatinta 56 tūkst. laiškų. 13% dalyvių nepavyko atpažinti suklastoto laiško. Atsižvelgiat į tai, kad pratybos vyko tik 3 dienas, o dalyvių skaičius nepakankamas kaip teigiama nagrinėjamoje ataskaitoje galima daryti prielaidą, kad rezultatai galėtų būti dar didesni.

Šioje ataskaitoje pratybų rezultatai išryškino būtinybę stiprinti darbuotojų kibernetinio saugumo įgūdžius ir poreikį vykdyti aktyvesnį darbuotojų kibernetinio saugumo švietimą.

2.1.3. Kibernetinis saugumas ir darbas nuotoliniu būdu, literatūros apžvalga

Masinis nuotolinio darbo arba kitaip hibridinio darbo organizavimas dėl Covid-19 pandemijos protrūkio, prasidėjo 2020 m. kovo mėn. ir tebevyksta iki šiol. Šiame skyriuje bus nagrinėjamos to pasekmės, nes svarbu suprasti kaip organizacijos prisitaikė prie naujos darbo aplinkos ir ar sugebėjo išlaikyti arba sumažinti kibernetinės rizikos poveikį.

Kai 2020 m. pradžioje buvo paskelbtas COVID-19 ligos protrūkis tikriausiai niekas neįsivaizdavo kaip pasikeis gyvenimas per ateinančias savaites ir mėnesius. Siekiant suvaldyti ligos plitimą buvo imtasi daug drastiškų priemonių. Milijonai žmonių visame pasaulyje buvo uždaryti ir todėl turėjo atlikti visas veikalas iš namų. Tai reiškia, kad mokymosi įstaigos, įmonės ir daugybe kitų organizacijų turėjo pradėti dirbti nuotoliniu būdu naudodamiesi kibernetine erdve ir skaitmeninėmis priemonėmis. Žmonėms teko per naktį pereiti prie skaitmeninio rėžimo ir visai nesvarbu ar jie turėjo tam reikalingų įgūdžių ar ne ir ar iš vis turėjo technines galimybes ir prieigą prie interneto (Pawlicka ir kt., 2021). Šis staigus perėjimas iš įprastinės darbo aplinkos į skaitmeninę turėjo įtakos ir kibernetiniam saugumui. Greičiausiai buvo tikimasi, kad kai mokymosi įstaigos, įmonės, daugybe kitų organizacijų bei pavieniai asmenys pritaps naujoje realybėje - žmonių skaitmeniniai įgūdžiai pagerės. Tačiau, dėl pandemijos, įtempta ir sudėtinga padėtis tik sudarė palankesnes sąlygas piktavaliams ir sukčiams. 2020 – 2021 m. pastebėtas nekenėjiško pobūdžio incidentų skaičiaus augimas, nes COVID-19 pandemija tapo daugybės žmogaus klaidų ir netinkamo sistemų konfigūravimo priežastimi todėl 2020 m. dauguma pažeidimų buvo padaryti dėl žmogiškojo klaidos faktoriaus (ENISA, 2021). Kibernetinės grėsmės, susijusios su pandemija ir to rezultatu – darbas nuotoliniu būdu, išnaudojimas tampa įprastiniu reiškiniu. Dėl šios priežasties susidarė palankios sąlygos rengti išpuolius, todėl pastebima, kad vis daugiau kibernetinių išpuolių į organizacijas ir įmones nukreipiama pasinaudojant nuotolinio darbo faktoriumi (ENISA, 2021).

COVID-19 metu atlikti tyrimai parodo, kad nuotolinis darbas turi neigiamą poveikį darbuotojų gerovei ir psichikos sveikatai. Kai kurie tyrimai rodo, kad nuotolinis darbas skatina nuolatinį darbo režimą, kuris skatina protinį ir fizinį nuovargį kas gali turėti įtakos darbuotojo budrumui (RISCS, 2021).

Pandemijos metu dėl staiga padidėjusios priklausomybės nuo technologijų, kurios padeda susijungti ir tęsti veiklas iš mažiau saugios, kibernetiniu požiūriu, namų aplinkos padarė didelį poveikį organizacijoms visame pasaulyje. COVID-19 pandemijos metu padaugėjo paskirstytas atsisakymas aptarnauti (angl. Distributed Denial of Services, DDoS) atakų. Pastebėtas pagausėjimas kenkėjiškų interneto svetainių, tiek į įprastas svetaines įdiegtų specialių kodų ar kenkėjiškos programos, kuriuose

vartojami tokie žodžiai kaip "corona-virus". Kibernetiniai nusikaltėliai aktyviai naudojosi socialinę žiniasklaidą siųsti kenkėjiškėms pranešimams kaip pvz. pavyzdžiui, netikras COVID-19 informacines programėles. Taip pat pasitelkė elektroninio pašto kompromitavimo sukčiavimo būdus platinant kenėjiškus priedus organizacijoms ir kaip įrankį pasitelkdami COVID – 19 ligą. O darbas nuotoliniu būdu padidino vidinių grėsmių riziką ir organizacijos patyrė kibernetinę ataką paprasčiausiai dėl to, kad darbuotojas dirbo už organizacijos saugumo ribų (RISCS, 2021). Kibernetiniai piktavaliai aktyviai naudojosi COVID - 19 pandemija ir taikėsi į namuose dirbančius darbuotojus ENISA 2021; Chapman, 2020). ENISA (2021) pateiktame kibernetinių grėsmių ataskaitoje apžvelgė tuo metu aktualias kibernetines grėsme ir apžvelgiant į tai pateikė rekomendacijas visiems skaitmeninės erdvės vartotojams kaip išlikti saugiems kibernetinėje aplinkoje.

Apibendrinant, galima daryti išvadą, kad saugiam darbui nuotoliniu būdu būtinas efektyvesnis darbuotojų paruošimas. COVID – 19 pandemijos metu, kuomet įvyko ypač greitas perėjimas prie darbo iš namų, išryškėjo, kad dauguma organizacijos darbuotojų nebuvo tinkamai paruošti atpažinti kibernetines grėsmes dėl to kibernetiniai piktavaliai tuo pasinaudojo. Organizacijoms visame pasaulyje tai turėjo neigiama poveikį.

2.2. Kibernetinio saugumo viešajame sektoriuje užtikrinimo būdai ir šalių praktika

2.2.1 Jungtinės Karalystės Vyriausybės kibernetinio saugumo strategija 2022-2030

2022 m. JK pristatė *Vyriausybės kibernetinio saugumo strategija 2022-2030*. Šioje strategijoje išdėstomos JK vyriausybės požiūris į kibernetinio atsparumo viešajame sektoriuje stiprinimą. Poreikis didinti kibernetinį atsparumą tampa vis aktualesnis, vyriausybės audito ir rizikos komiteto reguliariai teikiamose ataskaitose nuolat pabrėžiama, kad kibernetinis saugumas yra viena svarbiausių rizikų ir COVID-19 pandemija padidino šią riziką bei iš esmės pakeitė vyriausybės darbo pobūdį, nes hibridinis darbas tapo norma. Akcentuota, kad vyriausybė išlieka ir išliks patrauklus taikinys įvairiems piktavaliams. JK NKSC nagrinėtais atvejais laikotarpiu nuo 2020 m. rugsėjo mėn. iki 2021 m. rugpjūčio mėn. iš 777 tirtų incidentų net 40 % buvo susiję su viešuoju sektoriumi. Pagrindinė šios strategijos taikumo sritis – įvairios viešojo sektoriaus organizacijos, įskaitant: vyriausybės departamentus, nepriklausomas įstaigas, agentūras, vietos valdžios institucijas ir kitas platesnio masto viešojo sektoriaus organizacijas.

Jungtinės Karalystės Vyriausybės kibernetinio saugumo strategija 2022-2030 – tai išsamus planas, kuriame išdėstytas Jungtinės Karalystės vyriausybės požiūris į šalies kibernetinės erdvės saugumo ir atsparumo užtikrinimą. Strategija siekiama apsaugoti Jungtinę Karalystę nuo kibernetinių

grėsmių, skatinti inovacijas ir remti ekonomikos augimą, kartu užtikrinant, kad skaitmeninio pasaulio nauda būtų prieinama visiems piliečiams. Strategijos vizija ir tikslas:

Vizija – šia strategija siekiama užtikrinti, kad pagrindinės vyriausybės funkcijos - nuo viešųjų paslaugų teikimo iki nacionalinio saugumo aparato veikimo - būtų atsparios kibernetinėms atakoms, stiprinant JK kaip suverenią valstybę ir įtvirtinant jos, kaip demokratinės ir atsakingos kibernetinės galios, autoritetą.

Tikslas – iki 2025 m. Vyriausybės ypatingos svarbos funkcijos turi būti gerokai apsaugotos nuo kibernetinių atakų, o ne vėliau kaip 2030 m. visos Vyriausybės organizacijos visame viešajame sektoriuje turi būti atsparios žinomiems pažeidžiamumams bei atakų metodams.

Šiai vizijai ir tikslui pasiekti reikės iš esmės pakeisti vyriausybės požiūrį į kibernetinį saugumą. Be to, kad ir toliau stiprinti organizacijų kibernetinį atsparumą vyriausybė "ginsis kaip vienas", kad galėtų įveikti iššūkius su kuriais susiduriama. Todėl ši strategija grindžiama dviem pagrindiniais ir vienas kitą papildančiais strateginiais *ramsčiais (angl. Pillar)*, kurie apibrėžia ir lemia vyriausybės požiūrį į kibernetinį atsparumą.

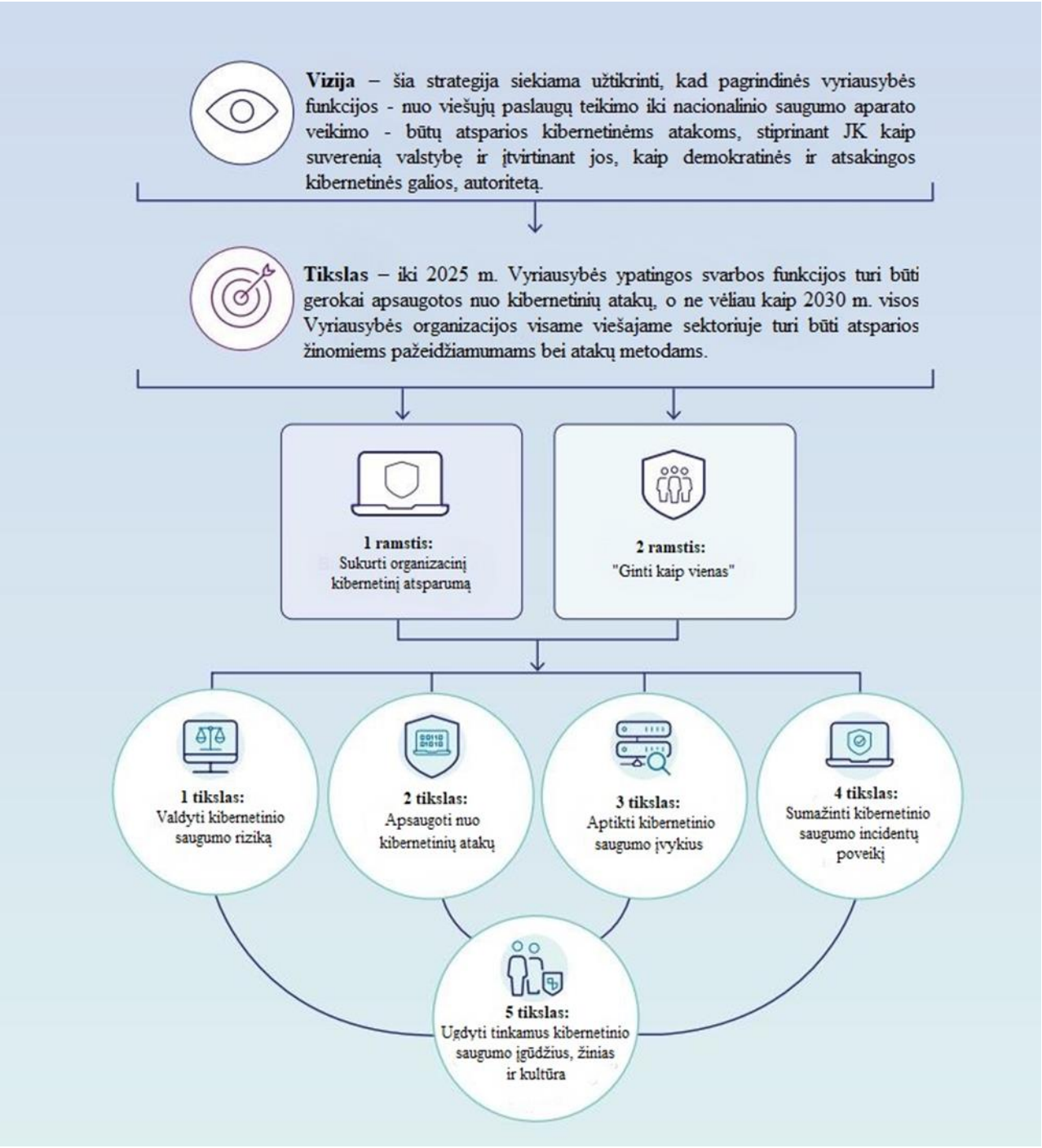
- Sukurti tvirtą organizacijos kibernetinio saugumo atsparumo pagrindą:

Pagrindinis tikslas - užtikrinti, kad vyriausybinės organizacijos turėtų tinkamas struktūras, mechanizmus, priemones ir paramą kibernetinio saugumo rizikai valdyti.

- "Gintis kaip vienas":

„Gintis kaip vienas“ reiškia, kad dėl grėsmės masto ir spartos reikia imtis visapusiškesnių ir vieningesnių atsakomųjų veiksmų. Siekdama į tai reaguoti, vyriausybė įsteigs Kibernetinio koordinavimo centrą. Svarbiausia bus formuoti tvirtas partnerystes visoje vyriausybėje, kad būtų pakeista kibernetinio saugumo duomenų ir žvalgybinės informacijos apie grėsmes naudojimo tvarka. Šie strateginiai *ramsčiais (angl. Pillar)* paremti 5 tikslai ir grindžiami 14 principų, kurie paremti 39 rezultatais, nurodančiais, ką reikia pasiekti, o ne kontroliniu sąrašu, ką reikia padaryti. Kiekvienas papildomas rezultatas yra susijęs su gerosios praktikos rodikliais (IGP). IGP naudojami rengiant konkretiems sektoriams skirtus CAF profilius, kuriuose pateikiama nuomonė apie tinkamą ir proporcingą tų organizacijų kibernetinį saugumą.

Strategija paremta šiais tikslais: Valdyti kibernetinio saugumo rizikas; Apsaugoti nuo kibernetinių atakų; Aptikti kibernetinio saugumo įvykius; Sumažinti kibernetinio saugumo incidentų poveikį; Ugdyti tinkamus kibernetinio saugumo įgūdžius, žinias ir kultūrą (7 pav.).



Šaltinis: išversta pagal „Government Cyber Security Strategy 2022-2030“, p.27

7 pav**. Jungtinės Karalystės Vyriausybės kibernetinio saugumo strategija 2022-2030**

Valdyti kibernetinio saugumo rizikas – siekdama valdyti kibernetinę saugumo riziką, vyriausybinės organizacijos turės rizikos valdymo procesus ir galės nustatyti, įvertinti ir suprasti rizikas. Sisteminei

rizikai veiksmingai valdyti bus užtikrintas: pakankamas bendras matomumas, aiški atskaitomybę, informacijos pasidalijimas visoje vyriausybėje.

Apsaugoti nuo kibernetinių atakų – visose vyriausybinėse organizacijose bus priimtos proporcingos saugumo priemonės. Vyriausybė plėtos bendrus pajėgumus, priemones bei paslaugas bendriems kibernetinio saugumo klausimams spręsti.

Aptikti kibernetinio saugumo įvykius – kad aptiktų kibernetinio saugumo įvykius, kol jie dar netapo incidentais vyriausybė turi stebėsenos pajėgumus. Glaudesnis koordinavimas leis vyriausybei operatyviau naudotis stebėsenos duomenimis ir tokiu būdu bus užtikrintas spartesnis bei didesnio masto incidentų aptikimas, o taip pat tai palengvins nuoseklų reagavimą bei pajėgumų sutelkimą aptinkant sudėtingesnes kibernetines atakas.

Sumažinti kibernetinio saugumo incidentų poveikį – tikėtina, kad dėl veiksmingo rizikos valdymo, taikant sustiprintus aptikimo pajėgumus bei proporcingas ir tinkamas apsaugos priemones vyriausybė taps gerokai sunkiau pažeidžiamu taikiniu, bet numanoma, kad išvengti visų kibernetinio saugumo incidentų nepavyks. Todėl vyriausybė bus maksimaliai pasirengusi ir gebės reaguoti į kibernetinio saugumo incidentus, o svarbiausias šio tikslo komponentas bus - sukurti mechanizmus, leidžiančius pratybų metu išbandyti bei pasimokyti iš incidentų ar vos neįvykusių incidentų taip ugdant tinkamus kibernetinio saugumo įgūdžius, žinias ir kultūrą

Ugdyti tinkamus kibernetinio saugumo įgūdžius, žinias ir kultūrą – jei nebus pakankamai susifokusuota į reikiamų kibernetinio saugumo įgūdžių bei žinių ugdymą, o taip pat į kultūrinius pokyčius kibernetinio saugumo srityje visoje vyriausybėje šios strategijos vizijos bei tikslų nebus įmanoma pasiekti. Iš esmės šioje strategijoje pripažįstama, kad svarbu ugdyti kibernetinio saugumo kultūrą bei investuoti į darbuotojų mokymus, kad būtų skatinamas nuolatinis tobulėjimas.

Apibendrinus, JK Vyriausybės kibernetinio saugumo strategiją 2022-2030, joje pripažįstamas kintantis kibernetinio saugumo grėsmių pobūdis bei poreikis laikytis koordinuoto ir įvairiapusio požiūrio, kad būtų galima veiksmingai kovoti su kibernetinio saugumo grėsmėmis. išryškėja siekis sukurti saugią ir atsparią kibernetinę erdvę, kuri remtų: ekonomikos augimą, saugotų nacionalinį saugumą ir užtikrintų piliečių bei įmonių saugumą ir privatumą.

2.2.2 Baltijos šalių patirtis kibernetinio saugumo užtikrinimo srityje

Kadangi nauji skaitmeniniai produktai ir paslaugos tampa neatsiejama mūsų kasdienio gyvenimo dalimi, daugėja informacijos saugumo pažeidimų. Europos audito rūmu (2019)

informaciniame pranešime teigiama, kad viešajame ir privačiajame sektoriuose visoje ES, taip pat tarptautiniu lygmeniu yra daug kibernetinio saugumo valdymo trūkumų. Tai mažina pasaulio bendruomenės gebėjimą reaguoti į kibernetines atakas ir jas apriboti bei kenkia nuosekliam ES masto požiūriui. Todėl reikia stiprinti kibernetinio saugumo valdymą. Atsižvelgiant į didėjantį kibernetinio saugumo įgūdžių trūkumą pasaulyje, labai svarbu didinti įgūdžius ir informuotumą visuose sektoriuose ir visuomenės lygmenyse. Šiuo metu ES mastu nėra daug mokymo, sertifikavimo ar kibernetinės rizikos vertinimo standartų (Europos rūmų auditas, 2019).

Įvairiose Europos Sąjungos valstybėse narėse labai skiriasi pagrindiniai kibernetinio saugumo įgūdžiai, atitinkamai ir bendras kibernetinio saugumo lygis. Nuolatinis kibernetinio piliečio įgūdžių mokymo medžiagos tobulinimas taip pat buvo laikomas svarbiu dėl nuolatinės kibernetinės veiklos aplinkos plėtros. Šiandien kasdieninėje skaitmeninėje aplinkoje stiprūs piliečių kibernetiniai įgūdžiai būdas pasiruošti ir atremti kibernetines grėsmes taip stiprinant bendrą valstybės kibernetinio saugumo lygį. Toliau šiame darbe bus analizuoti trijų valstybių – Lietuvos, Latvijos ir Estijos piliečių kibernetiniai įgūdžiai remiantis šalių kibernetinio saugumo strategijomis.

Lietuva. Pagal pasaulinį kibernetinio saugumo indeksą Lietuva yra 6 vietoje. Pagal Nacionalinis kibernetinio saugumo indeksą – 2 vietoje. Gyventojų skaičius šalyje ~ 2 900 000 gyventojų (NCSI, 2023)

Lietuvos kibernetinio saugumo strategijoje (2018) teigiama, kad siekiant stiprinti kibernetinio saugumo kultūrą, visuomenei turėtų būti suteikiamos pagrindinės kibernetinio saugumo žinios įvairiuose švietimo lygmenyse, nes tai padės stiprinti bendrą kibernetinio saugumo supratimą. Remiantis NKSC kasmetinėmis kibernetinio saugumo ataskaitomis matyti, kad didelė dalis Lietuvos gyventojų nesupranta kibernetinių nusikaltimų keliamos rizikos. 2021 -2022 m. šalyje buvo registruoti 4 088 kibernetinio saugumo incidentai (KAM, 2022), todėl reikia didinti piliečių informuotumą siekiant stiprinti kibernetinio saugumo kultūrą. Svarbu efektyviai ir reguliariai skleisti ir keistis informaciją apie naujausias grėsmes ir kitus veiksnius, galinčius kelti grėsmę asmens duomenų saugumui ar sudaryti sąlygas žmonėms susidurti su kibernetiniais nusikaltimais skaitmeninėje erdvėje.

Lietuvos kibernetinio saugumo strategijoje siekiant valstybės atsparumo kibernetinėms grėsmėms bei didinti visuomenės informuotumą apie kibernetinį saugumą iškelti 5 strateginiai tikslai: **Stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą** – šiam tikslui pasiekti bus kuriamas sisteminis požiūris į kibernetinį saugumą ir prevencinę veiklą, gerinant kibernetinio saugumo rizikos nustatymą, vertinimą ir prognozavimą. Bus užtikrinamas visuomenės

informuotumas apie kibernetinio saugumo būklę bei vykdomos kitos kibernetinį saugumą ir prevencinę veiklą stiprinančios priemonės ir veiksmai.

Užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą – šiam tikslui pasiekti bus tobulinama teisinė sistema, konsoliduojant teisėsaugos institucijų profesinius įgūdžius tirti nusikalstamas veikas skaitmeninėje erdvėje. Kad uždavinys būtų įgyvendintas bus skatinama visuomenė savisaugos kultūra ir atsakingas elgesys kibernetinėje erdvėje.

Skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą – šiam tikslui pasiekti bus vystomi didelę pridėtinę vertę kibernetiniam saugumui nešančios veiklos ir moksliniai tyrimai. Kuriant kibernetinio saugumo inovacijas bus skatinamas viešojo sektoriaus, privataus sektoriaus, mokslo ir studijų institucijų bendradarbiavimas.

Stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą – šiam tikslui pasiekti bus kuriamas viešojo ir privataus sektorių tvarus bendradarbiavimo procesas kibernetinio saugumo srityje. Skatinamas viešojo bei mažo ir vidutinio privataus sektorių kibernetinio saugumo vertinimo atlikimas siekiant didinti organizacijų brandos lygį kibernetinio saugumo srityje.

Stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą – šiam tikslui pasiekti kibernetinio saugumo srityje bus plėtojamas tarptautinis, tarpvalstybinis ir Baltijos šalių bendradarbiavimas, o taip pat plėtojant dvišalį Lietuvos ir Jungtinių Amerikos Valstijų bendradarbiavimą kibernetinės gynybos ir saugumo srityje (KAM, 2018).

Lietuvoje siekiant užtikrinti kibernetinį saugumą privatus sektorius, valstybinės institucijos ir aukštosios mokyklos siūlo įvairias kibernetinio saugumo programas ir veiklas stiprinant bendrą kibernetinį saugumą šalyje. *2021 m. buvo organizuoti 13 772 susitikimai, kurių metu visuomenė mokyta, kaip atpažinti nusikaltimus elektroninėje erdvėje ir kaip nuo jų apsisaugoti* (KAM, 2021, p 11). Lietuvos bankai, policija ir bibliotekos aktyviai dalyvauja kibernetinio saugumo mokymuose (KAM, 2021). Taip pat piliečių informuotumas apie kibernetinį saugumą skatinamas per tradicinę ir socialinę žiniasklaidą, kaip pvz. interneto portalas draugiškas internetas - naudojamas skleisti informaciją piliečiams apie saugų elgesį internete bei reklamuoti renginius susijusius su saugiu naudojimusi internetu. Portale esagumas siūlomos saugumo mokymo temos pradedant techninėmis temomis tokiomis kaip – antivirusinės programos, šnipinėjimo programos bei kenkėjiškos programos ir baigiant temomis, labiau orientuotomis į privatumą ir e. prekybą. Portalo naudotojai taip pat gali užduoti klausimus kibernetinio saugumo ekspertams.

Viena iš galimybių atnaujinti įgūdžius ar persikvalifikuoti – LCC tarptautinio universiteto organizuojama kibernetinio saugumo mokymo programa "LCC Cybersecurity Bootcamp". Ji skirta ribotų IT įgūdžių turintiems asmenims, kurie norėtų pasirengti darbui kibernetinio saugumo sektoriuje. Kibernetinio saugumo magistrantūros studijas siūlo keturi Lietuvos universitetai: Mykolo Romerio universitetas – „Kibernetinio saugumo valdymas“; Vilniaus Gedimino technikos universitetas – „Informacijos ir Informacinių technologijų sauga“; Vilniaus universitetas – „Kompiuterinis modeliavimas“ ir Kauno technologijos universitetas – „Informacijos ir informacinių technologijų sauga“.

Remiantis Nacionalinės kibernetinio saugumo būklės ataskaita – kibernetinio saugumo atakos tampa vis sudėtingesnės (KAM, 2021), o kibernetinio saugumo ekspertai svarsto ar bendroji kibernetinio saugumo kompetencija didėja pakankamai sparčiai, kad būtų galima sumažinti atotrūkį tarp visuomenės kibernetinės gynybos įgūdžių ir kibernetinių piktavalių atakų įgūdžių. Geresnius kibernetinio saugumo įgūdžius turi jaunoji karta ir IT specialistai, tačiau yra daug vartotojų, kurie neturi elementarių kibernetinio saugumo žinių, taip pat labai naivių vartotojų, kurie yra lengvas sukčių taikinys. Lietuviai taip pat jaučia informacijos poreikį kovojant su melagingomis naujienomis (Skaržauskienė, 2020). Kadangi didžioji dalis sėkmingų kibernetinių atakų įvykdoma pasinaudojant žmogiškosiomis silpnybėmis, šiems aspektams reikia skirti daug dėmesio. Todėl labai svarbu atpažinti sukčiavimą ir kitas sukčiavimo formas. Taip pat labai svarbu suprasti saugumo valdymo procesus, pavyzdžiui, programinės įrangos atnaujinimus ir reguliarų slaptažodžių keitimą (KAM, 2022).

Latvija. Pagal pasaulinį kibernetinio saugumo indeksą Latvija yra 15 vietoje. Pagal Nacionalinis kibernetinio saugumo indeksą 26 vietoje. Gyventojų skaičius šalyje ~ 2 000 000 gyventojų (NCSI, 2023)

Latvijos kibernetinio saugumo strategija parengta 2019 m. Joje pabrėžiama, kaip svarbu, kad visi piliečiai žinotų apie riziką, kuri jiems kyla interneto aplinkoje, ir apie priemones, galinčias užkirsti kelią pavojui. Siekiant užtikrinti kibernetinį saugumą, labai svarbu, kad kiekvienas asmuo žinotų apie saugumo problemas kasdieniame gyvenime ir būtų budrus šiuo atžvilgiu. Siekiama didinti visuomenės informuotumą apie kibernetinį saugumą rengiant konkrečiam amžiui pritaikytas gaires ir mokomąją medžiagą, taip pat organizuojant socialinės žiniasklaidos saugumo kampanijas. Konkrečioms tikslinėms grupėms siūlomi sudėtingesni ir išsamesni mokymai kibernetinio saugumo temomis. Be to, mokiniai ir mokytojai turi būti geriau informuojami apie informacijos saugumą, privatumo apsaugą ir patikimas interneto paslaugas. Turėtų būti teikiama daugiau paramos Latvijos vaikų ir jaunimo

informuotumui apie kibernetinį saugumą didinti, pavyzdžiui, pasitelkiant neformalųjį švietimą, žaidimus ir konkursus (MOD, 2019).

Latvijos kibernetinio saugumo strategijoje siekiant tobulinti viešojo ir privačiojo sektoriaus kibernetinio saugumo pajėgumus didinant atsparumą kibernetinėms atakoms ir gerinant visuomenės informuotumą apie esamas internetines grėsmes bei pažangių skaitmeninių ir kibernetinių įgūdžių ugdymui informacinių ir ryšių technologijų sektoriaus ekspertams, o taip pat platesnei visuomenei iškelti 5 strateginiai tikslai:

Kibernetinio saugumo skatinimas, skaitmeninio saugumo rizikos mažinimas – siekiant šio tikslo bus sukurta visapusiška krašto apsaugos sistema, kuri būtų įgyvendinama glaudžiai bendradarbiaujant viešajam ir privačiajam sektoriams bei visai visuomenei. Šie subjektai kartu sustiprintų kibernetinės erdvės saugumą ir gynybą. Bendrą supratimą ir koordinuotą reagavimą į krizes bus ugdoma rengiant bendrus krizių valdymo mokymus nacionalinėms saugumo agentūroms, valdžios institucijoms ir privačiajam sektoriui.

Stiprinti informacijos ir ryšių technologijos atsparumą, teikti visuomenei svarbius informacijos ir ryšių technologijos sprendimus ir paslaugas – šiam tikslui pasiekti bus parengtas atsakingo saugumo pažeidžiamumų atskleidimo reglamentavimo sistema. Tolesnis IRT atsparumo stiprinimas Latvijos diplomatinėse atstovybėse užsienyje. Reguliarus CERT.LV įsiskverbimas į vyriausybinių IRT sprendimus ir infrastruktūrą testavimas.

Visuomenės informavimas, švietimas ir moksliniai tyrimai – siekiant šio tikslo bus siekiama palengvinti asignavimų gavimą kibernetinio saugumo tyrimų ir plėtros projektams, kuriuose daugiausia dėmesio skiriama aktualiems iššūkiams. Didinti mokinių ir mokytojų informuotumą apie informacijos saugumą, privatumo saugumą ir patikimas interneto paslaugas. Gerinti visuomenės informuotumą apie saugą internete bei teikti pažangius kibernetinio saugumo mokymus konkrečioms tikslinėms grupėms. Parengti ir įgyvendinti metinį daugiainstitucinį veiksmų ir kampanijų planą su kibernetinio saugumo informaciniais renginiais ir informuotumo didinimo kampanijomis. Didinti paramą Latvijos vaikų ir jaunimo dalyvavimui neformaliajame švietime kibernetinio saugumo srityje. Skatinti visuomenės ir savivaldybių institucijų darbuotojų informuotumą apie IRT saugą.

Tarptautinis bendradarbiavimas – suformuluoti ir pristatyti Latvijos nacionalinę poziciją, dalyvauti tarptautinėse bendradarbiavimo programose ir platformose, stiprinti Šiaurės ir Baltijos šalių bendradarbiavimą, aktyviai dalyvauti NATO ir ES iniciatyvose ir, be kita ko, padėti šalims partnerėms stiprinti kibernetinės gynybos pajėgumus. Toliau tęsti pradėtus ir pradėti naujus tarptautinius kibernetinių nusikaltimų mažinimo veiksmus bendradarbiavimo programas. Bendradarbiauti su

įvairiomis tarptautinėmis organizacijomis ir agentūromis, kovojančiomis su elektroniniais nusikaltimais.

Teisinė valstybė kibernetinėje erdvėje, kova su elektroniniais nusikaltimais – Padidinti valstybinės policijos ir nacionalinių saugumo tarnybų gebėjimus tirti kibernetinio saugumo atvejus bei incidentus, stiprinti valstybės policijos ir nacionalinio saugumo tarnybų institucinius gebėjimus. Pagerinti naudotojų identifikavimą remiant perėjimą prie IPv6 viešajame sektoriuje ir taip paskatinti privatųjį sektorių pasekti šiuo pavyzdžiu (MOD, 2019).

Kovo 14 d. Latvijos vyriausybė patvirtino Gynybos ministerijos parengtą "Latvijos kibernetinio saugumo strategijos 2023-2026“ – projektą, kuriame apibrėžiamos pagrindinės nacionalinės kibernetinio saugumo politikos veiksmų kryptys ir įvardijami ateities iššūkiai. Naujame dokumente apibrėžtos 5 pagrindinės veiklos kryptys: kibernetinio saugumo valdymo tobulinimas, kibernetinio saugumo skatinimas ir atsparumo stiprinimas, visuomenės informavimas, švietimas ir moksliniai tyrimai, tarptautinis bendradarbiavimas ir teisingumas kibernetinėje erdvėje, kibernetinių nusikaltimų prevencija ir kova su jais (LSM.lv).

CERT.LV yra Latvijos centrinė kibernetinio saugumo institucija, veikianti prie Gynybos ministerijos (Latvijas Republikas Aizsardzības ministrija), ji teikia informaciją ir rengia mokymus plačiajai visuomenei (CERT.LV). Pavyzdžiui, prieš svarbius įvykius, tokius kaip rinkimai, ji rengia informacines kampanijas. Ji taip pat socialinėje žiniasklaidoje skelbia pranešimus apie Latvijos kibernetinę būklę (ENISA, 2021). CERT.LV prižiūrimame portale esidross.lv pateikiama daug naudingų patarimų apie kibernetinį saugumą ir nurodymų, kaip saugiai naudotis skaitmeniniais prietaisais. Aptariamos tokios temos kaip asmens duomenų valdymas ir privatumas, įrenginių, programinės įrangos ir socialinių tinklų saugumas. Be to, portale pateikiama patarimų, kaip kalbėtis su vaikais apie saugą internete. Informacija apie dažniausiai pasitaikančias grėsmių rūšis, taip pat rekomendacijos, kaip jų išvengti ir spręsti problemas, pasitarnauja kaip konkreti pagalba valdant kibernetinį saugumą.(esidross.lv). Portale mana.latvija.lv yra skyrius "Saugumas internete" (Drošība internetā), kuriame pateikiami patarimai, kaip saugiai naudotis internetu ir mobiliaisiais įrenginiais, kaip saugoti asmens duomenis, taip pat patarimai, kur kreiptis pagalbos, pavyzdžiui, sukčiavimo atveju (mana.latvija.lt). NIC (Tinklo informacijos centras) parengė nemokamą internetinį kursą "Kibernetinio saugumo pagrindai"(Cybersecurity Basics). Jis skirtas kaip įvadas žmonėms, neturintiems techninio išsilavinimo (nic.lv).

Kibernetinio saugumo magistrantūros studijas Latvijoje siūlo trys universitetai: Verslo ir finansų aukštoji mokykla (Banku augstskola) – Kibernetinio saugumo vadybos profesinio magistro

studijų programą, Rygos technikos universitetas (Rīgas Tehniskā universitāte) – Kibernetinio saugumo inžinerijos studijų programą ir Vidžemės taikomųjų mokslų universitetas (Vidzemes Augstskola) – Kibernetinio saugumo inžinerijos magistro studijų programą. Taip pat Žiemgalos regiono žmogiškųjų išteklių ir kompetencijų ugdymo centras (Zemgales reģiona kompetenču attīstības centrs) – savivaldybės mokymo įstaiga, kurios tikslas - užtikrinti piliečių mokymąsi visą gyvenimą. Institutas organizuoja kursus – Kibernetinis saugumas, kompiuterinės sistemos ir programinė įranga.

Latvijoje kibernetinio pilietiškumo įgūdžių iš dalies mokoma mokykloje. Vis dėlto kibernetinio saugumo įgūdžius reikia atnaujinti, o tai iššūkis - rasti geriausią būdą, kaip pasiekti piliečius ir surengti gerą informuotumo didinimo kampaniją (Valstybės policija). Pastangas didinti informuotumą stabdo darbuotojų ir lėšų trūkumas. Ateityje siekiama mokyklų kibernetinio saugumo mokymą susieti su civilinės gynybos mokymu. Pagal Valstybės gynybos koncepciją , kibernetinis saugumas turėtų būti įtrauktas į mokymo programą ir viena iš civilinės gynybos pamokų temų. Kibernetinio saugumo strategijoje teigiama, kad svarbu užtikrinti, jog visi, kurie gali susidurti su sukčiavimu elektroniniu paštu ar socialine inžinerija, išmanytų kibernetinį saugumą. Visi suinteresuotieji subjektai yra vienodai svarbūs tinklų ir informacinių sistemų saugumui. Tai reiškia, kad visi turėtų vienodai gerai žinoti, kokia rizika jiems gresia internete ir kokių veiksmų jie gali imtis, kad išvengtų tokio poveikio (MOD, 2019).

Estija. Pagal pasaulinį kibernetinio saugumo indeksą Estija yra 3 vietoje. Nacionalinis kibernetinio saugumo indeksas – 3 vieta. Gyventojų skaičius ~ 1 300 000 gyventojų (NCSI, 2023).

Nacionalinė Estijos kibernetinio saugumo strategija 2019-2022 tai jau trečiosios kartos kibernetinio saugumo strategija, tai tik patvirtina, kad kibernetinis saugumas ir kibernetinė gynyba ir toliau išlieka Estijos prioritetu. Estijos kibernetinio saugumo strategija - tikslai apima kibernetinio raštingumo visuomenės skatinimą, o tam reikia didinti piliečių, valstybės ir privačiojo sektoriaus informuotumą apie kibernetinį saugumą. Visi kibernetinėje erdvėje veikiantys piliečiai yra atsakingi už kibernetinio saugumo įgūdžių ugdymą. Švietimo sistemoje kibernetinis saugumas aptariamas visais švietimo lygmenimis kaip skaitmeninių kompetencijų ugdymo dalis. Svarbu nuolat atnaujinti mokinių ir mokytojų skaitmeninių kompetencijų modeliuose numatytus kibernetinio saugumo komponentų įgūdžius, nepamirštant įgūdžių matavimo. Kibernetinio saugumo strategijoje pabrėžiama prevencinių veiksmų svarba. Būtina kalbėti apie vyraujančius pavojus plačiajai visuomenei ir teikti patarimus, kaip sumažinti riziką. Įvairios agentūros turi bendradarbiauti, kad plačioji visuomenė būtų

geriau informuota apie kibernetines grėsmes ir priemones, kurių reikia imtis po galimos atakos (MEAC, 2019).

Estijos nacionalinė kibernetinio saugumo strategija grindžiama penkiais strateginiais tikslais:

Užtikrinti Estijos skaitmeninių sistemų, paslaugų ir duomenų prieinamumą, vientisumą ir konfidencialumą stiprinant šalies kibernetinio saugumo pajėgumus ir plėtojant veiksmingą kibernetinės rizikos valdymo praktiką.

Skatinti tarptautinį bendradarbiavimą ir dalijimąsi informacija kibernetinio saugumo klausimais, aktyviai dalyvaujant tarptautiniuose forumuose ir iniciatyvose, dalijantis informacija su kitomis šalimis ir bendradarbiaujant su kitomis valstybėmis vykdant su kibernetiniu saugumu susijusius projektus.

Užtikrinti veiksmingą kibernetinio saugumo valdymą Estijoje sukuriant aiškią reguliavimo sistemą, užtikrinant veiksmingą įvairių valdžios institucijų ir suinteresuotųjų subjektų veiklos koordinavimą ir skatinant viešojo ir privačiojo sektorių partnerystę kibernetinio saugumo srityje.

Ugdyti kompetentingą ir kvalifikuotą kibernetinio saugumo srities darbo jėgą skatinant kibernetinio saugumo švietimą ir mokymą bei remiant konkurencingos ir novatoriškos kibernetinio saugumo pramonės plėtrą Estijoje.

Didinti Estijos piliečių, įmonių ir kitų suinteresuotųjų subjektų informuotumą apie kibernetinio saugumo riziką ir geriausią praktiką, skatinant kibernetinio saugumo supratimą ir švietimą bei teikiant rekomendacijas, kaip išlikti saugiems internete.

Estijos informacinių sistemų tarnyba (Riigi Infosüsteemi Amet, RIA) koordinuoja informuotumo apie kibernetinį saugumą didinimą Estijoje, renka informaciją apie piliečių informuotumo apie kibernetinį saugumą lygį ir, remdamasi gautais rezultatais, organizuoja veiklą. RIA reguliariai rengia informavimo kampanijas, skirtas Estijos kibernetiniam saugumui gerinti. RIA reagavimo į incidentus skyrius CERT-EE siekia užkirsti kelią su kibernetiniu saugumu susijusioms rizikingoms situacijoms ir mažinti saugumo riziką. CERT reguliariai organizuoja įvairius renginius ir informacines kampanijas, skelbia įspėjimus ir pranešimus naudotojams apie Estijos sistemose ir taikomosiose programose nustatytas saugumo spragas (RIA, 2021).

Aukštosiose mokyklose kibernetinio saugumo galima mokytis pagal dvi skirtingas magistrantūros programas. Talino technologijos universitetas (Tallinna Tehnikaülikool, TalTech) kartu su Tartu universitetu (Tartu Ulikool) siūlo magistrantūros programą "Kibernetinis saugumas". Tarptautinę magistrantūros programą "Cyberus Erasmus Mundus Master in Cybersecurity" vykdo

Pietų Bretanės universitetas (Université Bretagne Sud) kartu su Talino technologijos universitetu (Tallinna Tehnikaülikool, TalTech).

Yra keletas galimybių mokytis savarankiškai, pavyzdžiui, NATO kibernetinės gynybos sąmoningumo e. mokymosi kursu siekiama pagerinti bendrojo naudotojo informuotumą apie kibernetinio saugumo riziką ir priemones šiai rizikai mažinti (ccdcoe.org)

Pastaraisiais metais Estijos gyventojų kibernetinės higienos lygis padidėjo. Jaunimas į kibernetinio saugumo sritį pritraukiamas per įvairius konkursus pavz.: "CyberPin", "CyberDrill", "CyberCracker" ir "CyberSpike", tačiau dar yra kur tobulėti. Pavyzdžiui, žmonės tampa sukčiavimo aukomis arba praranda savo skaitmeninių paslaugų kontrolę spustelėję neteisingas nuorodas. Estijos piliečiams siekiama pabrėžti, kad kibernetinis saugumas yra ne tikslas, o priemonė. Tai reiškia, kad saugumu reikia pasirūpinti tada, kai norite ką nors daryti. (RIA, 2022).

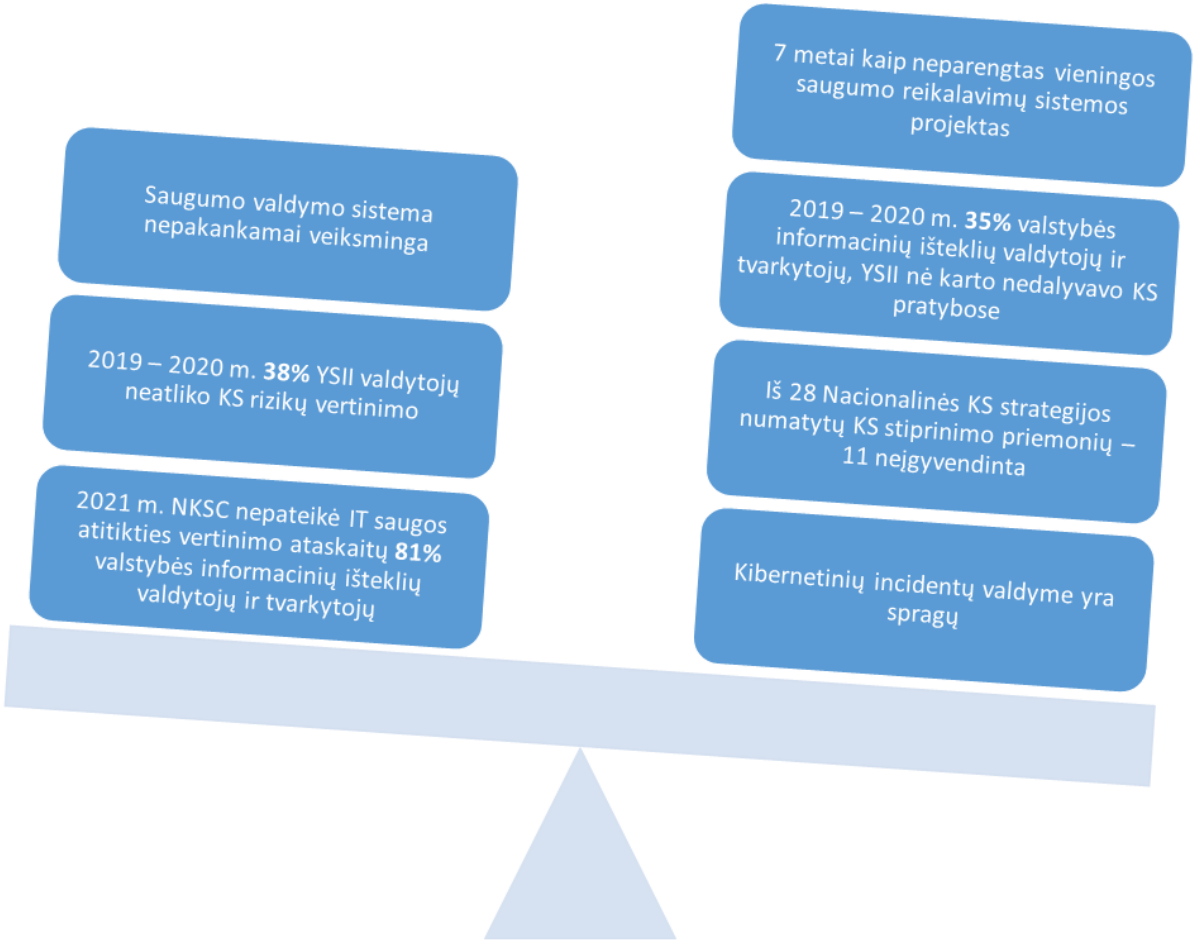
2.3. Esama Lietuvos kibernetinio saugumo padėtis viešajame sektoriuje

2.3.1 Valstybinio audito ataskaita „Kibernetinio saugumo užtikrinimas“

Valstybės kontrolės valstybinio audito ataskaitoje (2022) teigiama, kad tik veiksmingai veikianti KS užtikrinimo sistema sustiprintų reagavimą kibernetinėms grėsmėms, nes dėl neveiksmingai veikiančios KS užtikrinimo sistemos, atsparumas kibernetinėms grėsmėms išlieka žemas ir negalima efektyvi apsauga ypatingos svarbos informacinėms sistemoms (YSII), valstybės informaciniams ištekliams.

Ruošiant ataskaitą buvo atlikta 212 kibernetinio saugumo subjektų (Valstybės informacinių išteklių valdytojai ir tvarkytojai; YSII valdytojai) apklausa. Audito atlikimo laikotarpis 2019 – 2021 m. 2022 m. spalio 27 d. pristatyti valstybinio audito „*Kibernetinio saugumo užtikrinimo*“ ataskaitos rezultatai (8 pav.).

Nustatyta, kad nėra užtikrinamas tinkams KS rizikos ir incidentų valdymas nacionaliniu lygiu taip pat nesudarytos tinkamo sąlygos stebėsenai vykdyti dėl atitikties saugo reikalavimų, kibernetinio saugumo planavimo įgyvendinimui neužtikrintas nuoseklumas, identifikuotos spragos kibernetinio saugumo ir elektroninės informacijos saugos teisinime reguliavime. Būtina tobulinti kibernetinio saugumo užtikrinimo sistemą.



Šaltinis: adaptuota pagal „Kibernetinio saugumo užtikrinimas“ 2022

8 pav. **Pagrindiniai rezultatai**

Aptariant audito rezultatus išryškėjo 3 esminės problemos: nepakankamai veiksminga saugumo valdymo sistema; nepakankamai veiksmingas kibernetinių incidentų valdymas; kibernetinio saugumo planavimo įgyvendinimui neužtikrinamas nuoseklumas.

Institucijos tiriančios bei valdančios kibernetinius incidentus (NKSC, VDAI, Lietuvos policija) ne visais atvejais keitėsi informacija apie kibernetinius incidentus. Dėl šios priežasties gali nukentėti kibernetinio saugumo subjektai ir visuomenė, nes minėtos institucijos nesudaro palankių sąlygų greičiau nustatyti įvairių rūšių kibernetinius incidentus bei teikti informaciją kompetentingoms institucijoms, kad šios gebėtų laiku užkardyti nusikalstamas veikas ar pažeidimus. Yra sudarytos sąlygos perduoti informacijai apie kibernetinius incidentus per Kibernetinio saugumo informacinį tinklą, kuriuo KS subjektai ir kibernetinius incidentus valdančios ir (ar) tiriančios institucijos gali naudotis keičiantis ar perduodant informaciją apie KS incidentus. Tačiau buvo nustatyta, kad

kibernetinio saugumo subjektai šiuo tinklu naudojasi pasyviai ir todėl šio tinklo veikla buvo įvertinta kaip neefektyvi. Pasiūlyta apsvarstyti ir plačiau pritaikyti naudojimui.

Siekiant sustiprinti KS subjektų gebėjimus veiksmingai atremti kibernetines atakas vykdomos konsultacijos kibernetinio saugumo klausimais, KS pratybos bei mokymai, bet buvo nustatytas – nepakankamas rezultatyvumas. Nacionalinės kibernetinio saugumo pratybos rengiamos kasmet, o taip pat yra organizuojami kibernetinio saugumo mokymai bei kitos veiklos: teikiamos metodinės rekomendacijos, konsultuojama KS klausimais. Tačiau pažymėta, kad KS subjektų įsitraukimas į šias veiklas – nepakankamas: nustatyta, kad laikotarpiu 2019 – 2020 m. 35% apklaustųjų **niekada nedalyvavo** KS pratybose, o 55% nedalyvavo KS mokymuose. Net 26% KS subjektu neturi kibernetinių incidentų valdymo plano, nepasitvirtinę kibernetinių incidentų valdymo plano.

Nebuvo užtikrintas nuoseklus KS planavimo įgyvendinimas – laikotarpiu 2019–2021 m. Nacionalinės KS strategijos įgyvendinimo rezultatų peržiūra nebuvo vykdoma kasmet, nebuvo renkama ir sisteminama informacija apie strategijos įgyvendinimo rezultatus, Strategijos vykdytojai stebėjimą atliko ne pilna apimtimi (stebėjo ne visas priemones ir vertinimo kriterijus). Laikotarpiu 2019–2021 m. iš 28 Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstituciniame veiklos plane numatytų priemonių – 11 neįgyvendinta. Atliekant vertinimą, pagal numatytus vertinimo kriterijus, 2021 m. Nacionalinės kibernetinio saugumo strategijos įgyvendinimo rezultatus, nustatyta, kad nacionalinių KS planavimo dokumentų nustatyti tikslai bei uždaviniai stiprinant valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą, o taip pat skatinant kibernetinio saugumo kultūrą ir inovacijų plėtrą, nėra visiškai pasiekti dėl nenuoseklaus suplanuotų kibernetinio saugumo stiprinimo priemonių įgyvendinimo ir nepakankamos stebėsenos.

Kibernetinio saugumo užtikrinimui teikiamos rekomendacijos, nustatant *Rekomendacijų* įgyvendinimo priemones bei terminus. Stebėti aktualią informaciją apie rekomendacijų įgyvendinimo būklę bei rezultatus ir įvykusius pokyčius galima Valstybės kontrolės interneto svetainėje Rekomendacijų įgyvendinimas | Lietuvos Respublikos valstybės kontrolė (valstybeskontrole.lt).

Apibendrinant, galima daryti prielaida, kad iš esmės KS subjektų pasirengimas atremti kibernetines atakas neatitinka kibernetinių grėsmių. Dėl dinaminių kibernetinės aplinkos pokyčių bei vertinant dabartinius geopolitinius iššūkius Lietuvai labai svarbu stengtis įgyvendinti Rekomendacijas kaip įmanoma per trupiausią laikotarpį, taip užtikrinant YSII, valstybės informacinių išteklių efektyvesnį kibernetinį saugumą.

3.TYRIMO „ ORGANIZACIJOS IR INDIVIDO SĄVEIKA UŽTIKTINANT KIBERNETINĮ SAUGUMĄ“ METODOLOGIJA.

3.1. Tyrimo metodologija

Šiame tyrime pasirinkta nagrinėti kibernetinio saugumo aspektus viešajame sektoriuje. Kadangi kibernetinį saugumą viešajame sektoriuje vis dar galima laikyti besiformuojančia sritimi, šiuo darbu noriu prisidėti bei papildyti kibernetinio saugumo srities įžvalgas apie incidentų prevenciją viešajame sektoriuje per organizacijos ir individo sąveikos prizmę.

Tyrimo metodika ir organizavimas. Siekiant atskleisti organizacijos ir individo sąveiką užtikrinant kibernetinį saugumą bei kibernetinio saugumo kultūros ugdymą viešajame sektoriuje tyrimui organizuoti pasirinktas **kombinuotas tyrimas,** taikant **kokybinio** (ekspertinio interviu metodus) ir **kiekybinio** (antrinių statistinių duomenų , duomenys paimti iš „ISACA“ internetinių svetainių (prieiga per internetą: https://www.isaca.org/) ir anketinės apklausos metodus, viešųjų įstaigų darbuotojų anketinė apklausa (kurie tiesiogiai dalyvauja kibernetinio saugumo veiklose) **tyrimo strategijas** bei atliekant lyginamąją gautų duomenų analizę. Tyrimo instrumentavimui (1 lentelė) pasitelkta mokslinės literatūros bei juridinių dokumentų kokybinio turinio (anglų k. ***Content*** analizė). Siekiant nustatyti esamą kibernetinio saugumo elgseną individo ir organizacijos bei kibernetinio saugumo kultūrą Lietuvos viešajame sektoriuje buvo atlikti **kokybinis** ir **kiekybinis** tyrimai. **Kokybinio** tyrimo metu siekiama išsiaiškinti viešojo sektoriaus darbuotojų tarpusavio bendradarbiavimo efektyvumą ir įstaigos dedamas pastangas siekiant stiprinti kibernetinį saugumą. **Kiekybinio** tyrimo metu siekiama išsiaiškinti viešojo sektoriaus darbuotojų įsitraukimą į kibernetinį saugumą bei tokios kultūros puoselėjimą ir supratimą apie esamas grėsmes.

Tyrimo tikslas. Išanalizuoti organizacijos ir individo sąveikos, užtikrinant kibernetinį saugumą, tobulinimo galimybes Lietuvos viešajame sektoriuje.

Tyrimo uždaviniai:

1. Ištirti viešojo sektoriaus darbuotojų kibernetinio saugumo kultūrą.
2. Identifikuoti viešojo sektoriaus darbuotojų suvokimą apie kibernetinio saugumo keliamas rizikas ir grėsmes.
3. Pagrįsti organizacijos ir individo sąveiką viešajame sektoriuje, užtikrinant kibernetinį saugumą, parengiant Gaires „Kibernetinės kultūros viešajame sektoriuje tobulinimas“.

Tyrimo reprezentatyvumo pagrindimas.

Empirinio tyrimo imties sudarymui pasirinkta ***netikimybinės atrankos*** tipas, ***stratifikuotos atrankos būdu.***

Ekspertinio interviu tyrimo dalyviai buvo atrenkami pagal šiuos kriterijus:

1. Sertifikuoti specialistai tiesiogiai susiję su kibernetinio saugumo vykdomomis programomis ir darbuotojų kvalifikacijos kėlimu viešajame sektoriuje (lektoriai, mentoriai, ugdymo programų rengimo ir vertinimo ekspertai).
2. Dirbantys kibernetinio saugumo ugdymo platformose nemažiau 3-5 m.
3. Pareigūnai kibernetinių incidentų tyrėjai

Anketinės apklausos respondentų atrankos pagrindimas.

Respondentai atrinkti taip *pat* ***stratifikuotos*** atrankos būdu, taikant šiuos kriterijus:

1. Asmenys, esantys viešojo sektoriaus specialistai, tiesiogiai dalyvaujantys kibernetinio saugumo kultūros mokymuose.
2. Darbuotojai kurie tiesiogiai atsakingi už kibernetinio saugumo kultūros vystymą organizacijoje.

Tyrimo metodai:

Ekspertinis interviu metodas. Kokybiniam tyrimui pasirinktas ekspertinis interviu (N=4). Tyrimu siekiama surinkti reikiamą informaciją iš specialistų, kurie tiesiogiai susiję su kibernetinio saugumo vykdomomis programomis ir darbuotojų kvalifikacijos kėlimu viešajame sektoriuje.

Antrinių statistinių duomenų analizės metodas, taikant aprašomąją statistiką, padės pagrįsti esminę organizacijos ir individo sąveikos problematiką stiprinant kibernetinį saugumą organizacijoje.

Anketinė apklausa. Anketinė apklausa skirta, Lietuvos viešojo sektoriaus darbuotojams, kuriu funkcijos tiesiogiai susijusios su kibernetiniu saugumu organizacijoje.

Gautų duomenų analizė. Analizuojant siekiama išsiaiškinti specialistų bei viešojo sektoriaus darbuotojų nuomonę apie esamą kibernetinio saugumo veiksmingumą institucijoje. Remiantis analizės išvadomis bus rengiamos rekomendacijos siekiant tobulinti ir stiprinti kibernetinį atsparumą įstaigoje stiprinat tarpusavio bendradarbiavimą skatinant kibernetinio saugumo kultūrą.

Tyrimo eiga:

1 etapas. Šiame etape atliekama antrinių statistinių duomenų analizė, kuri yra susijusi su KS personalu kibernetinio saugumo supratimu ir darbuotojų įgūdžiais, ištekliais, kibernetinėmis grėsmėmis bei kibernetinio saugumo brandos lygiu.

2 etapas. Tyrimo dalyvių, atsakingų už kibernetinio saugumo kultūros *klimatą* organizacijos viduje ir kompetencijų ugdymą tyrimas. Šiame etape atliekamas kokybinis tyrimas – ekspertinis interviu. Interviu dalyviai specialistai susiję su kibernetinio saugumo darbuotojų švietimo plėtojimu organizacijos viduje. Šiuo tyrimu siekiama išsiaiškinti kokie procesai yra vykdomi siekiant vystyti kibernetinę saugumo kultūrą bei stiprinant tarpusavio darbuotojų sąveiką stiprinat kibernetinį saugumą viešajame sektoriuje, su kokiomis problemomis yra susiduriama.

3 etapas. Šiame etape atliekamas kiekybinis tyrimas – viešojo sektoriaus darbuotojų anketinė apklausa. Tyrimu siekiama nustatyti darbuotojų supratimą apie kibernetinį saugumą elektroninėje erdvėje, gebėjimą saugiai elgtis su informaciją ir jų požiūrį į kibernetinio saugumo ugdymą organizacijos viduje.

4 etapas. Šiame etape bus aptariami gauti rezultatai, siekiant išsiaiškinti kaip vertinamas kibernetinis saugumas organizacijos viduje ir kiek yra tarpusavy sąveikaujama. Tikslas palyginti gautus duomenis iš mokslinės literatūros bei dokumentų kokybinio turinio analizių ir ekspertinės interviu bei anketinės apklausos turinio analizių. Interpretavus analizės rezultatus parengiant rekomendacijas/gaires kibernetinio saugumo atsparumui kibernetinėms grėsmėms, didinti organizacijos viduje per tarpusavio sąveikos stiprinimą bei kibernetinės kultūros viešajame sektoriuje tobulinimui. Taip užtikrinat pajėgesnį ir efektyvesnį kibernetinį saugumą organizacijose.

1. lentelė. Tyrimo instrumentarijus

Tyrimo kriterijai	Tyrimo indikatoriai	Taikomi metodai
Informuotumo apie kibernetinį saugumą identifikavimas	1. Teorinis kibernetinio saugumo ir kibernetinės kultūros samprata organizacijoje pagrindimas. 2. Kibernetinio saugumo iššūkių indentifikavimas ir teorinis pagrindimas.	Mokslinės literatūros ir dokumentų analizė
Kibernetinio saugumo vertinimas organizacijoje bei kibernetinio saugumo skatinimas organizacijoje ir darbuotojų įsitraukimo raiška	1. Kibernetinio saugumo skatinimo būdų, organizacijose, indentifikavimas. 2. Kibernetinio saugumo valdymo modeliai bei strategijos. 3. Kibernetinio saugumo kultūros skatinimas atskirų	Mokslinės literatūros ir dokumentų analizė Ekspertinis interviu Viešojo sektoriaus darbuotojų anketinė apklausa

	šalių nacionaliniuose dokumentuose.	
Kibernetinio saugumo atsakomybių pasiskirstymas	1. Kibernetinio saugumo suvokimas apie kibernetines grėsmes ir rizikas viešojo sektoriaus darbo aplinkoje. 2. Organizacijos ir individo bendradarbiavimo spragos užtikrinant kibernetinį saugumą organizacijoje.	Mokslinės literatūros ir dokumentų analizė Ekspertinis interviu Viešojo sektoriaus darbuotojų anketinė apklausa
Nustatyti veiksnius, kurie gali turėti įtakos organizacijos gebėjimui užkirsti kelią kibernetinio saugumo incidentams. Parengti Gaires „Kibernetinės kultūros viešajame sektoriuje tobulinimas“.	1. Įvertinti organizacijos ir darbuotojo tarpusavio sąveiką užtikrinant ir stiprinant organizacijos kibernetinį saugumą 2. Parengti Gaires „Kibernetinės kultūros viešajame sektoriuje tobulinimas	Kombinuoto tyrimo strategija, taikant ekspertinį interviu ir anketinę apklausą Lyginamoji gautų duomenų analizė

3.2. Kombinuoto tyrimo organizavimas

Kokybinio tyrimo organizavimas. Tyrime dalyvauti buvo pakvieti 11 ekspertų, kurie susiję su kibernetinio saugumo vykdomomis programomis ir darbuotojų kvalifikacijos kėlimu kibernetinio saugumo srityje. Iš visų pakviestų ekspertų tyrime sutiko dalyvauti 4 ekspertai. Tyrimas atliktas gruodžio 5 – sausio 09 dienomis.

Kiekybinio tyrimo organizavimas. Tyrimui atlikti pasirinkta – anketinė apklausa. Siekiant pasiekti didesnį tyrimo dalyvių skaičių buvo pasirinktas klausimyno pildymas tiesiogiai internetinėje svetainėje https://forms.office.com . Anketinės apklausos nuoroda buvo siunčiama el. paštu. Tyrimo dalyviams (523 adresatai) kovo 1 d. buvo išsiųsta anketinės apklausos forma. Tyrimo dalyviams suteikta galimybė savarankiškai ir jiems tinkamu laiku bei jiems patogioje aplinkoje sudalyvauti anketinėje apklausoje bei pateikti savo atsakymus. Kombinuoto tyrimo etapų veikla atvaizduojama 2 lentelėje.

2 lentelė. Kombinuoto tyrimo eiga

Etapas	Veikla	Tikslai
Pasirengimas tyrimui	Suformuluojamas tyrimo metodas. Ruošiamas anketinės apklausos	Parengti tyrimo anketinės apklausos ir ekspertinio interviu klausimynai.

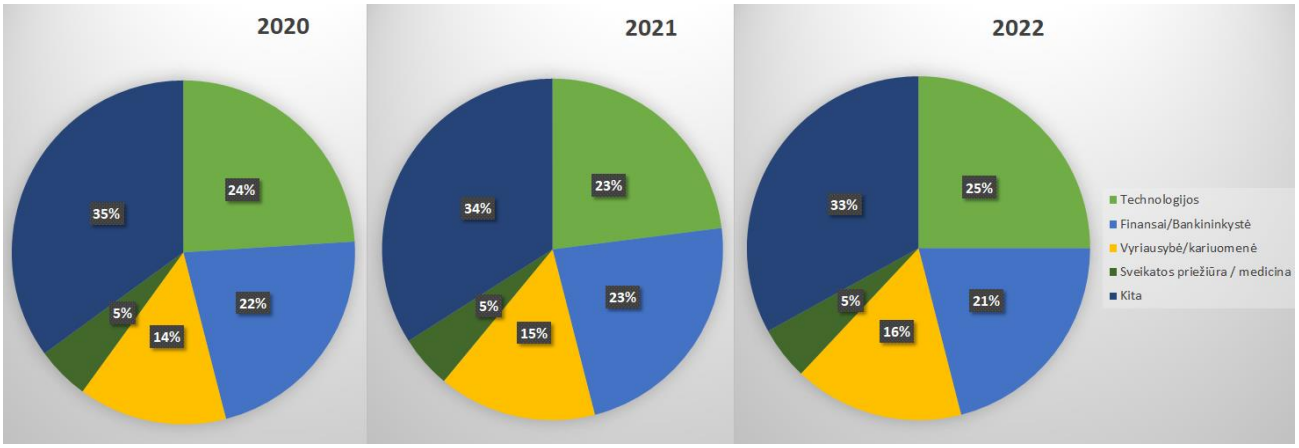
	klausimynas, rengiami ekspertinio interviu klausimai.	
Tyrimo eiga	Anketinė apklausos nuoroda išsiunčiama el. paštu tyrimo dalyviams (N=523). Ekspertinio interviu dalyviams išsiunčiami interviu klausimai (N=4).	Tyrimo pristatymas respondentams. Surinkta informacija apie darbuotojų kibernetinio saugumo supratimą bei esamą kibernetinio saugumo situaciją institucijoje.
Duomenų analizė	Analizuojama gauta informacija. Apibendrinami gauti duomenys. Rengiamos tyrimo išvados bei rezultatai.	Tyrimo rezultatų interpretavimas, vertinimas bei išvados.

Tyrimo etika. Kombinuoto tyrimo tikslas buvo išsiaiškinti ekspertų įžvalgas apie kibernetinį saugumą viešajame sektoriuje bei darbuotojų įsitraukimą į kibernetinį saugumą, o taip pat apie kibernetinės kultūros puoselėjimą organizacijoje ir supratimą apie esamas grėsmes. Tyrimo dalyviams pristatytas tyrimo tikslas ir gautas susitikimas dalyvauti tyrime. Visi tyrimo dalyviai tiek ekspertiniame interviu, tiek anketinėje apklausoje, dalyvavo savanoriškai. Siekiant išsaugoti tyrimo dalyvių anonimiškumą tyrime nėra atskleidžiamos tyrimo dalyvių vardai, pavardės ir pareigybės, todėl tyrimo dalyviams (ekspertams) buvo priskirti kodai informantas Nr. I1, I2, I3 ir t.t. Anketinės apklausos dalyviams taipogi buvo užtikrintas anonimiškumas, o tyrimo rezultatai pateikti tik apibendrinta forma.

4.TYRIMO DUOMENŲ ANALIZĖ IR INTERPRETACIJA

4.1. Antrinių statistinių duomenų analizė

Šiame skyriuje bus nagrinėjami duomenis remiantis ISACA parengtomis kibernetinio saugumo būklės 2020 m. 2021 m. ir 2022 m. ataskaitomis. Šios ataskaitos tai kasmetinės *ISACA* pasaulinės kibernetinio saugumo būklės tyrimo rezultatai, ataskaitose atsispindi aktualūs kibernetinio saugumo iššūkiai ir tendencijos. *ISACA* apklausos tikslinė grupė apima asmenys, kurie dirba kibernetinio saugumo srityje. Tyrimo respondentai atstovauja daugiau nei 17 veikos sričių iš skirtingų sektorių (9 pav.).

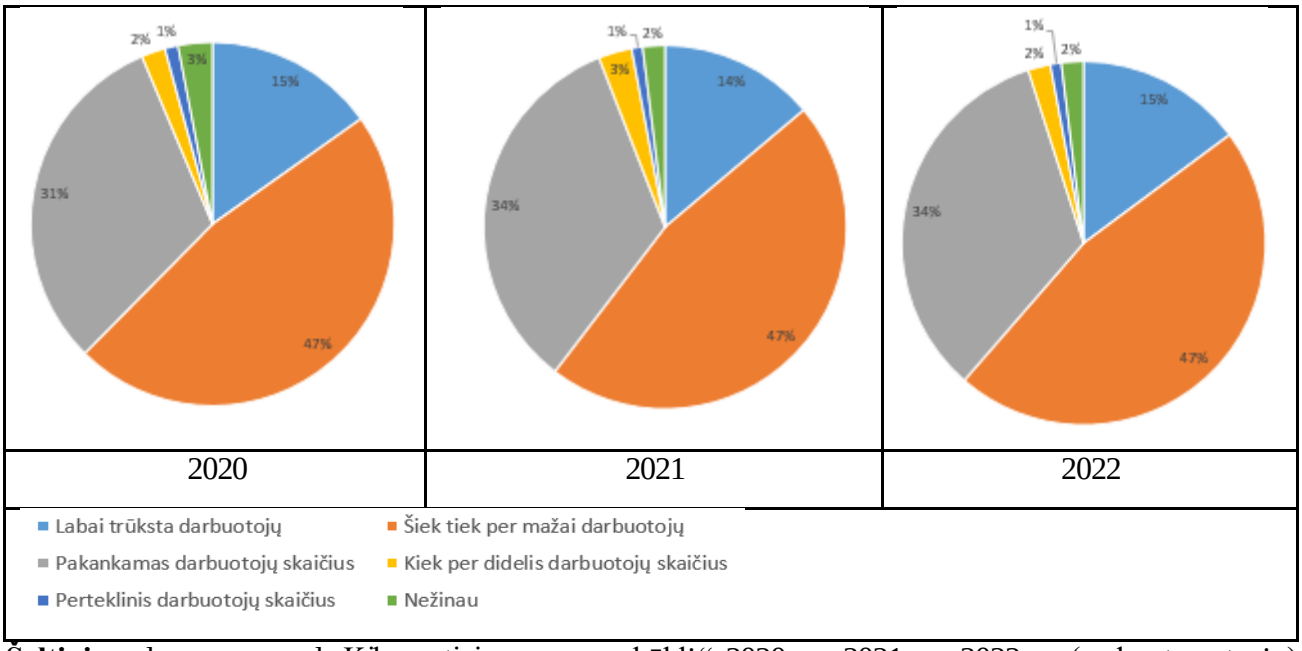


Šaltinis: „Kibernetinio saugumo būklė“ 2020 m., 2021 m., 2022 m.

9 pav. **Organizacijos veiklos sritis**

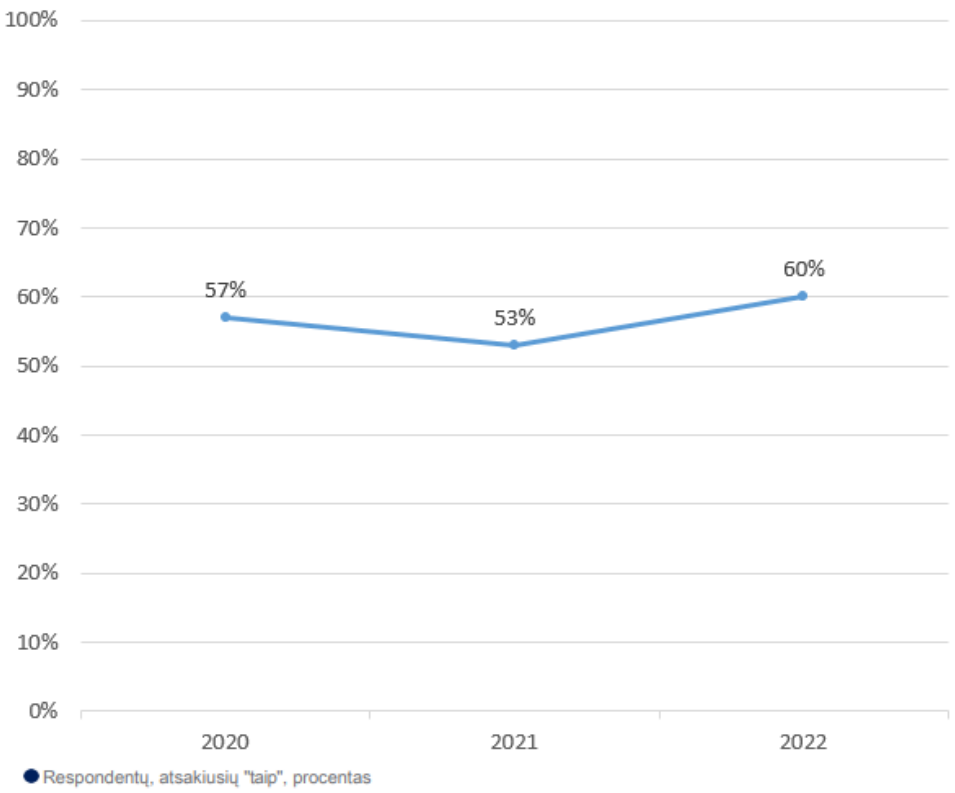
Kibernetinio saugumo būklės ataskaitose analizuojami apklausos rezultatai ir pateikiami duomenis, kurie susiję su kibernetinio saugumo personalu ir jų įgūdžiais, ištekliais, kibernetinėmis grėsmėmis bei kibernetinio saugumo brandos lygiu. Šių ataskaitų duomenų analizė atitinka darbe iškeltam **Tyrimo tikslui -** *Išanalizuoti esamą kibernetinio saugumo situaciją viešajame sektoriuje bei įvertinti organizacijos ir individo sąveiką, užtikrinant kibernetinį saugumą*.

2020 – 2022 m. apklausos rezultatai dėl organizacijose esamo KS personalo kasmet beveik sutampa. 14 – 15% apklausos dalyvių nurodo, kad jiems labai trūksta KS srities darbuotojų, 47% apklaustųjų identifikuoja, kad KS darbuotojų skaičius organizacijoje yra kiek nepakankamas (10 pav.). Taigi kibernetinio saugumo personalo trūkumas išlieka. Šių atsakymų analizė patvirtina tai, kad organizacijose, kuriuose trūksta darbuotojų susiduria ir su darbuotojų sulaikymo problemomis. 2022 m. 60 % tyrimo dalyvių nurodė, kad sunku išlaikyti kvalifikuotus KS specialistus, o tai yra 7% daugiau negu 2021 metais (11 pav.).



Šaltinis: adaptuota pagal „Kibernetinio saugumo būklė“ 2020 m., 2021 m., 2022 m. (sudaryta autorės)

10 pav. **Organizacijų kibernetinio saugumo personalas**

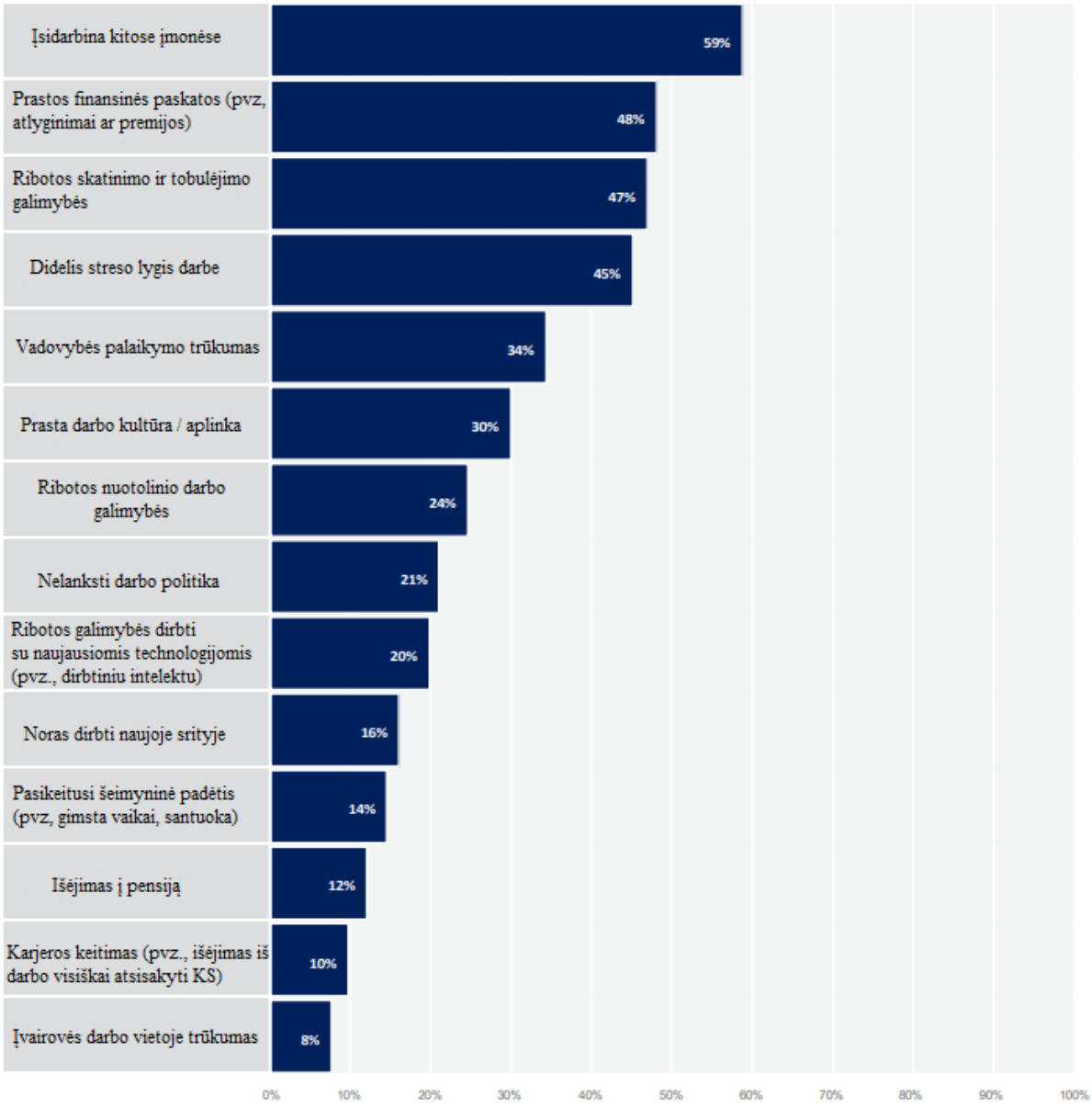


Šaltinis: adaptuota pagal **„**Kibernetinio saugumo būklė“ 2022 m.

11 pav. **Sunkumai sulaikant kvalifikuotus KS specialistus**

Kvalifikuotų KS specialistų sulaikymo sunkumai tikėtina susijęs su darbuotojų perdegimu dėl besitęsiančių COVID-19 pandemijos padarinių. Tai plačiai paplitęs nenoras grįžti į biurus siekiant geresnės darbo ir asmeninio gyvenimo pusiausvyros, nes dėl pandemijos išaugo lanksčių darbo sąlygų lūkesčiai, kurie tapo svarbiais aspektais darbuotojams vertinant galimus karjeros pokyčius. Darbuotojai taip pat atsisako darbo vietų, kurios reikalauja daugiau negu duodama (ISACA, 2022).

Tyrimo metu išryškėjo ir tam tikri veiksniai, kurie, apklausos respondentų nuomone, lemia kibernetinio saugumo specialistų sprendimus atsisakyti savo pareigų organizacijoje. 48% respondentų nurodė, kad priežastis yra prastos finansinės paskatos, 45% apklausos dalyvių teigė, kad apsisprendimą atsisakyti savo pareigų darbovietėje lemia patiriamas didelis stresas darbo aplinkoje. Apklausoje taip pat paminėti tokie veiksniai kaip: ribotos skatinimo ir tobulėjimo galimybės- 47%; vadovybės palaikymo trūkumas – 34%; ribotos nuotolinio darbo galimybės – 24% (12 pav.).

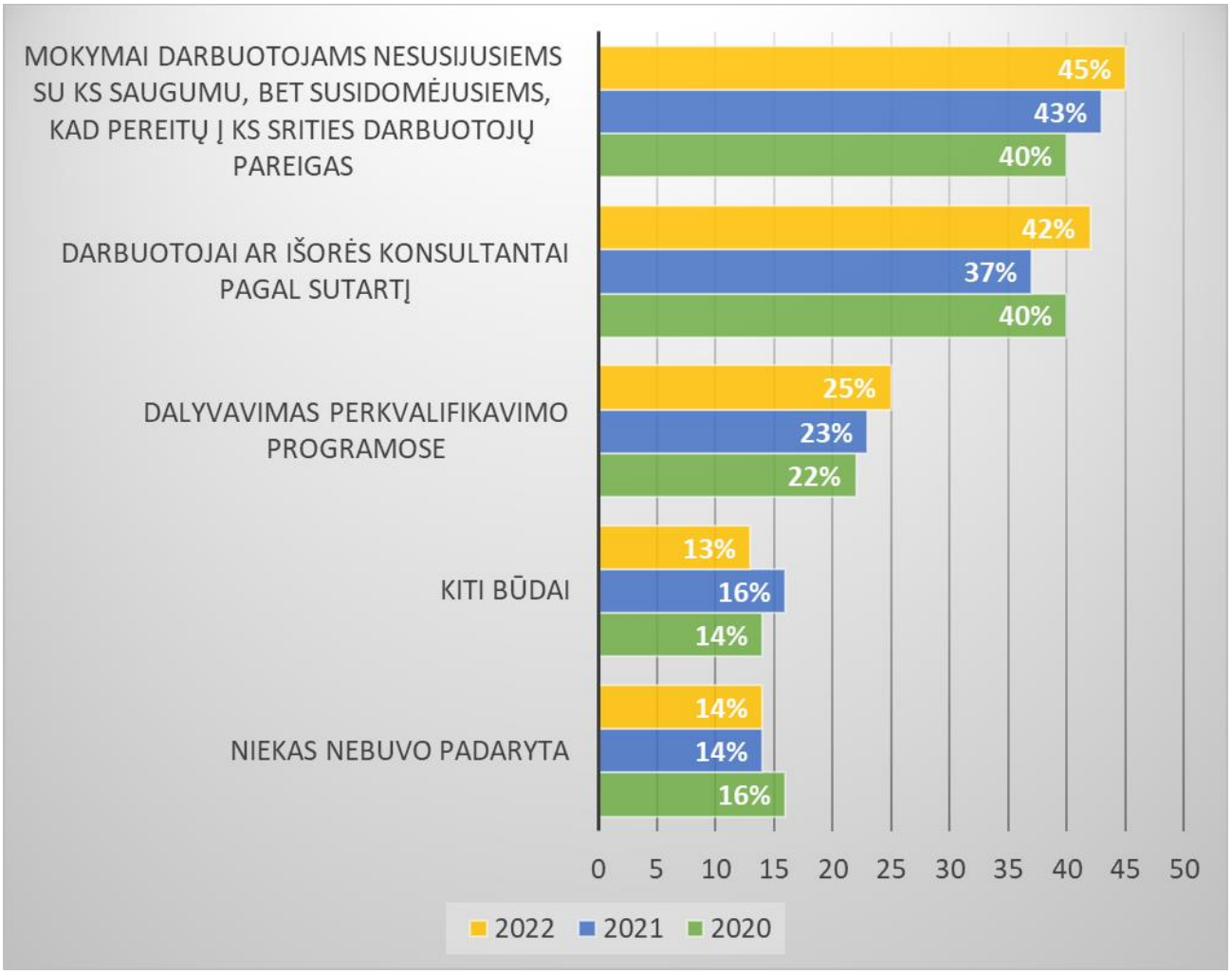


Šaltinis: adaptuota pagal „Kibernetinio saugumo būklė“ 2022 m.

12 pav. **Priežastys lemiančios KS specialistus atsisakyti savo pareigų organizacijoje**

Remiantis apklausos duomenimis pastebėta, kad darbuotojų skaičius, jų sulaikymas ir kibernetinės atakos yra tam tikra prasme tarpusavyje susiję. Organizacijos, kuriose trūksta kibernetinio saugumo darbuotojų, daug dažniau susiduria ir su darbuotojų sulaikymo problemomis. Per pastaruosius metus nepakankamai darbuotojų turinčios organizacijos patyrė daugiau kibernetinių išpuolių - tai reiškė, kad esamiems darbuotojams teko didesnis darbo krūvis ir dėl to darbuotojų tarpe atsirado tam tikras nepasitenkinimas ir noras palikti dabartinį darbą. Atitinkamai organizacijos susidūrė su kvalifikuotų KS specialistų praradimų (ISACA, 2020; ISACA, 2022).

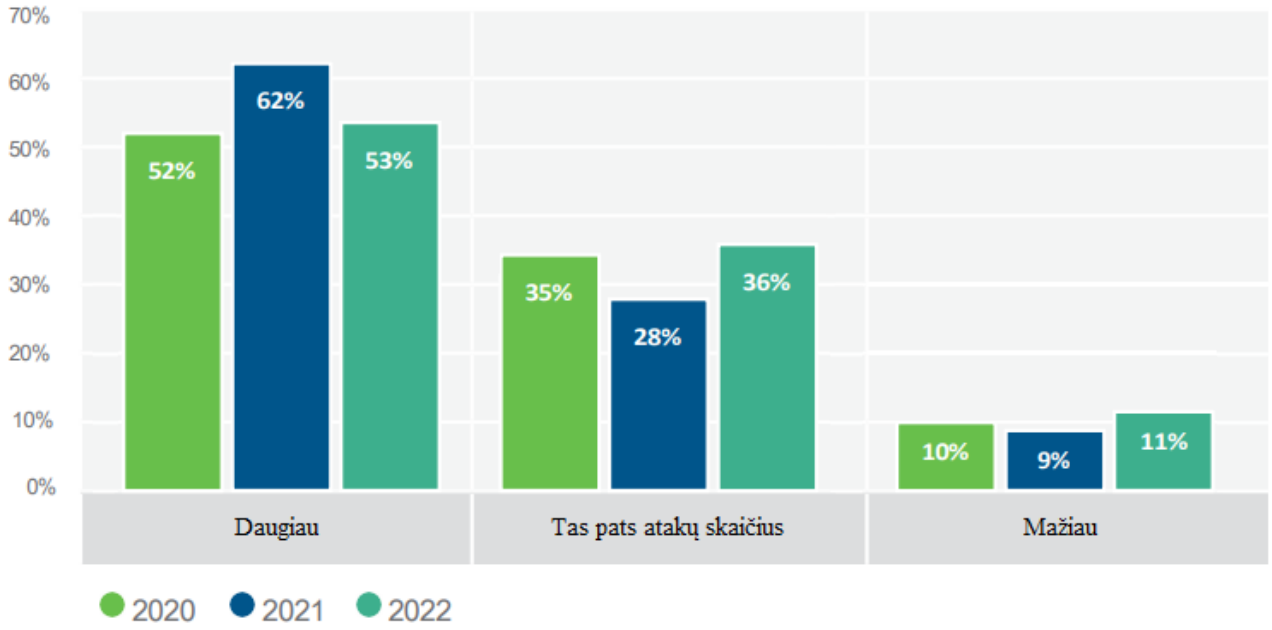
Kad pašalintų kibernetinio saugumo įgūdžių trūkumą dauguma organizacijos ėmėsi veiksmų. Pagrindinės priemonės, kuriomis siekiama sumažinti KS įgūdžių trūkumus: organizacijos darbuotojų mokymas – 45% (2022) ir aktyvesnis išorės konsultantų pasitelkimas – 42% (2022). Kitos priemonės (13 pav.).



Šaltinis: „Kibernetinio saugumo būklė“ 2020 m., 2021 m., 2022 m.

13 pav. **Kibernetinio saugumo įgūdžių trūkumo mažinimo priemonės**

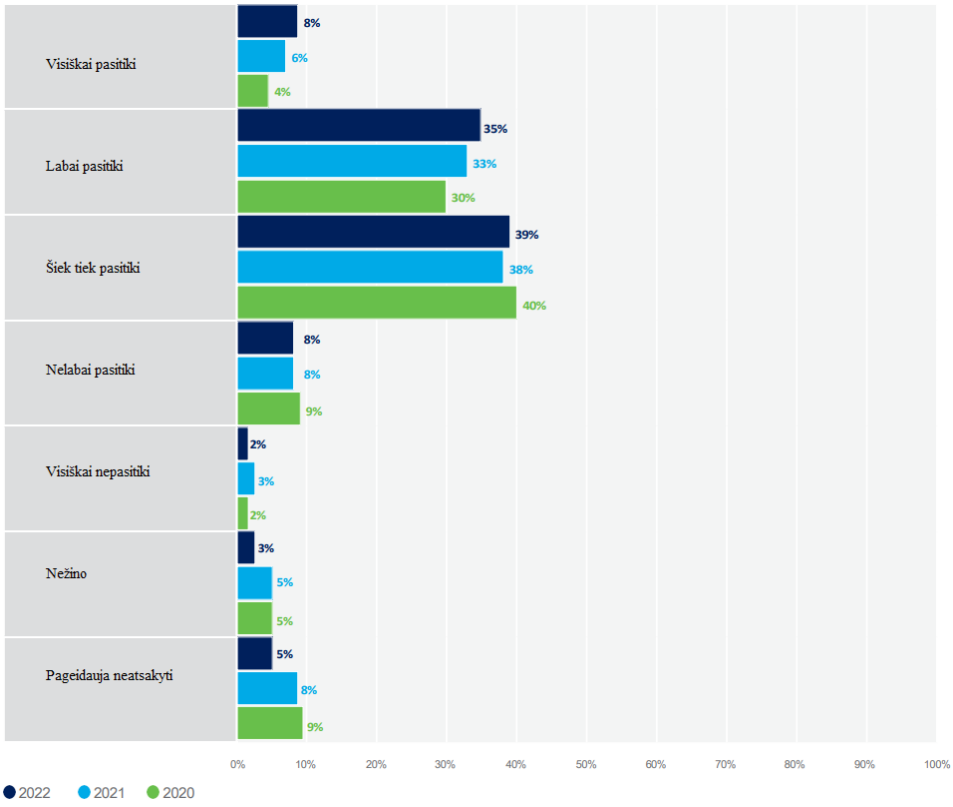
Nepaisant įdėtų pastangų organizacijos kasmet patyria vis daugiau kibernetinių atakų. Respondentų duomenimis jų organizacijos 2021 m. patyrė 62% daugiau kibernetinio saugumo atakų – tai 10% daugiau nei prieš tai buvusiais metais. (14 pav.) pateiktas 3 metų palyginimas.



Šaltinis: adaptuota pagal „Kibernetinio saugumo būklė“ 2022 m.

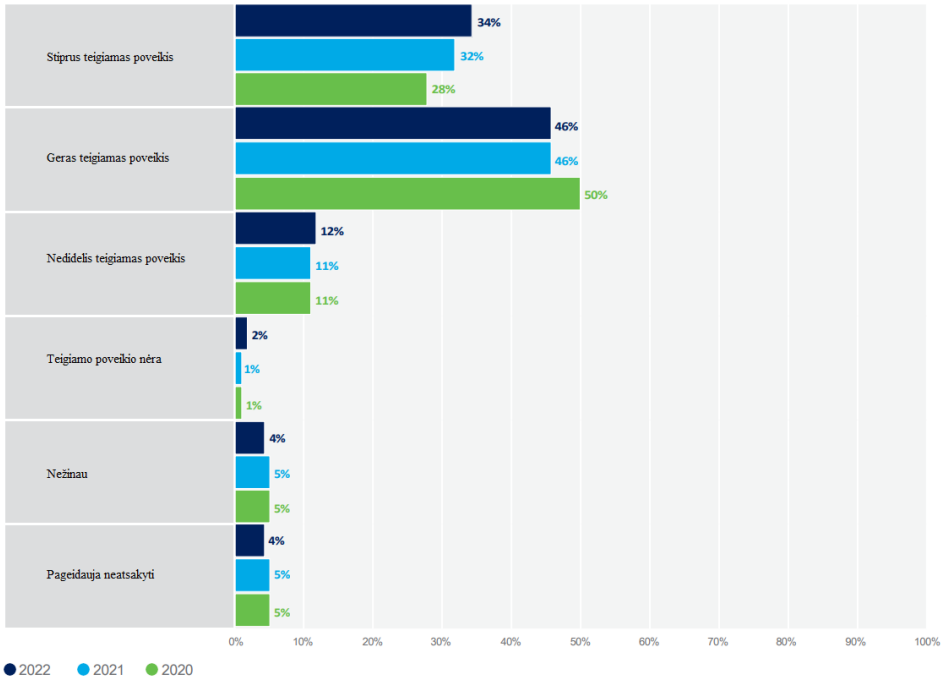
14 pav. **Kibernetinio saugumo atakų palyginimas 2020 – 2022 m.**

Didėjant kibernetinių atakų skaičiui beveik pusė išsivysčiusių rinkų vartotojų pripažįsta, kad gali tapti kibernetinių nusikaltimų aukomis (ISACA, 2022). Kartu su didėjančiu kibernetinių atakų skaičiumi auga ir pasitikėjimas organizacijos KS komandos gebėjimu apsiginti nuo kibernetinių grėsmių. 2022 m. – 82% tyrimo dalyvių išreiškė pasitikėjimą organizacijos KS komanda gebėjimu aptikti kibernetines grėsmes ir į jas sureaguoti. Ir šis pasitikėjimas KS komanda kasmet auga - 2020 m. – 74%; 2021 m. – 77% (15 pav.). Tokiam bendram darbuotojų sąmoningumui įtakos turi kibernetinio saugumo švietimo ir sąmoningumo ugdymo programos. Bendrai 2022 m. 80 % respondentų atsakė, kad KS ugdymo programos turi tam tikrą teigiamą poveikį darbuotojams (16 pav.).



Šaltinis: adaptuota pagal „Kibernetinio saugumo būklė“ 2022 m.

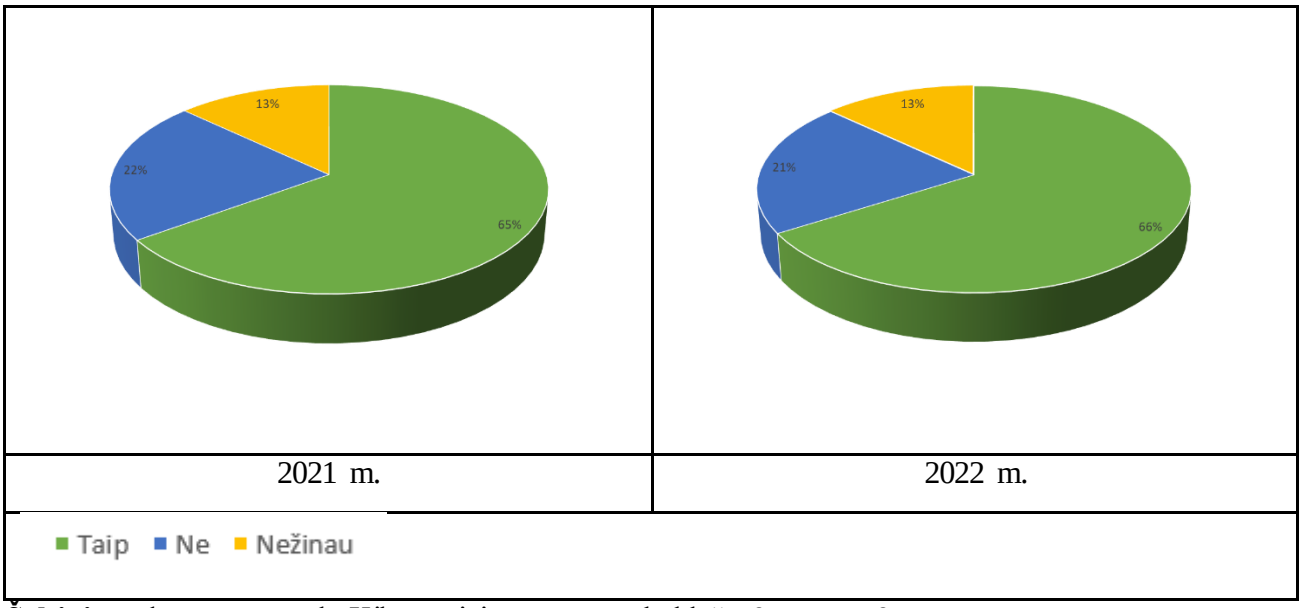
15 pav. **Pasitikėjimas KS komandos gebėjimu aptikti ir reaguoti į kibernetines grėsmes**



Šaltinis: adaptuota pagal „Kibernetinio saugumo būklė“ 2022 m.

16 pav. **KS švietimo ir sąmoningumo ugdymo programos poveikis**

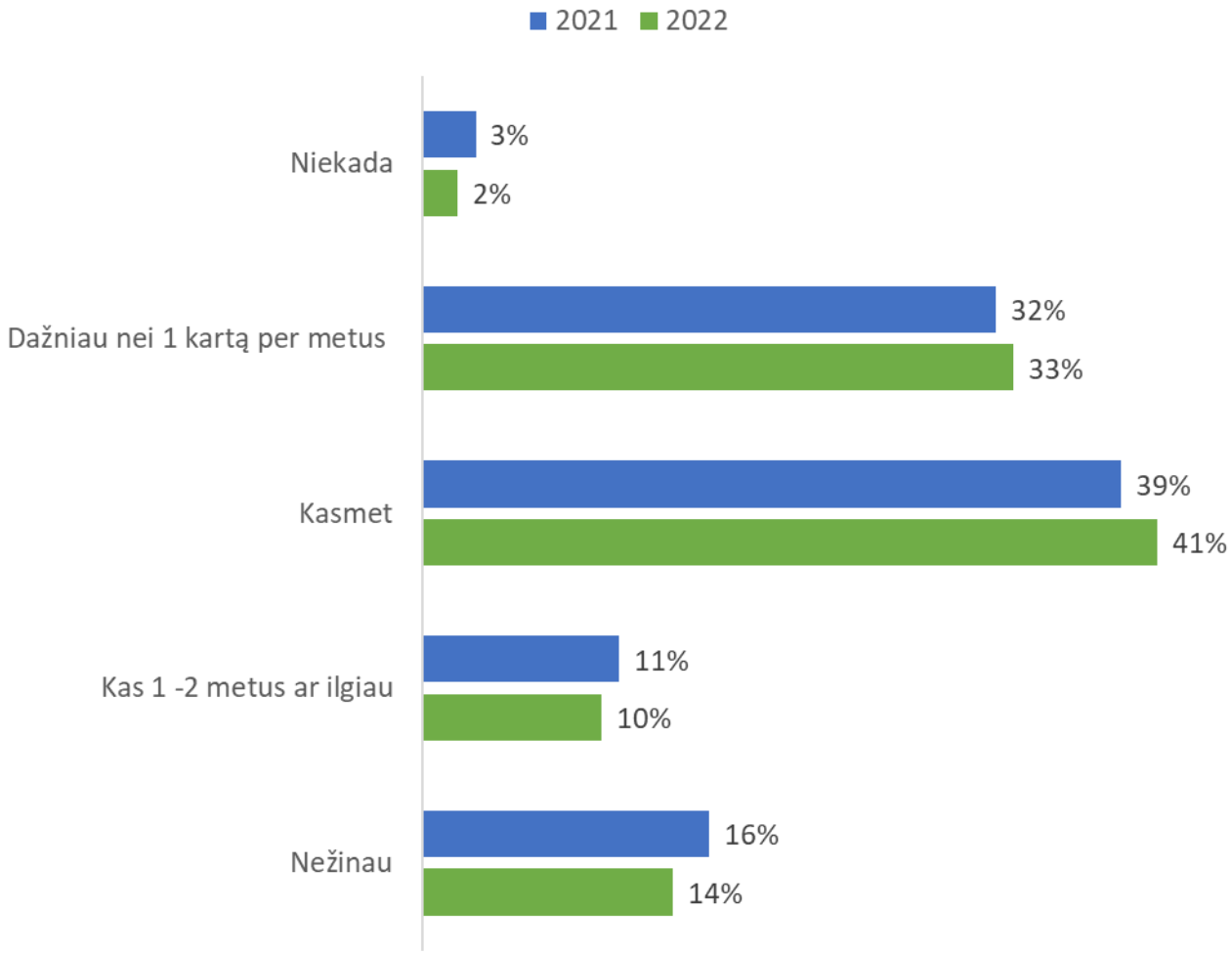
2021 m. ISACA išplėtė kasmetinės kibernetinio saugumo būklės apklausos temas, kad gautų duomenų organizacijų kibernetinio saugumo brangumo lygiui nustatyti. Tyrimo duomenimis 2021 m. – 65% ir 2022 m. – 66% organizacijų atlieka kibernetinės brandos vertinimus darbovietėje (17 pav.).



Šaltinis: adaptuota pagal „Kibernetinio saugumo būklė“ 2021 m.; 2022 m.

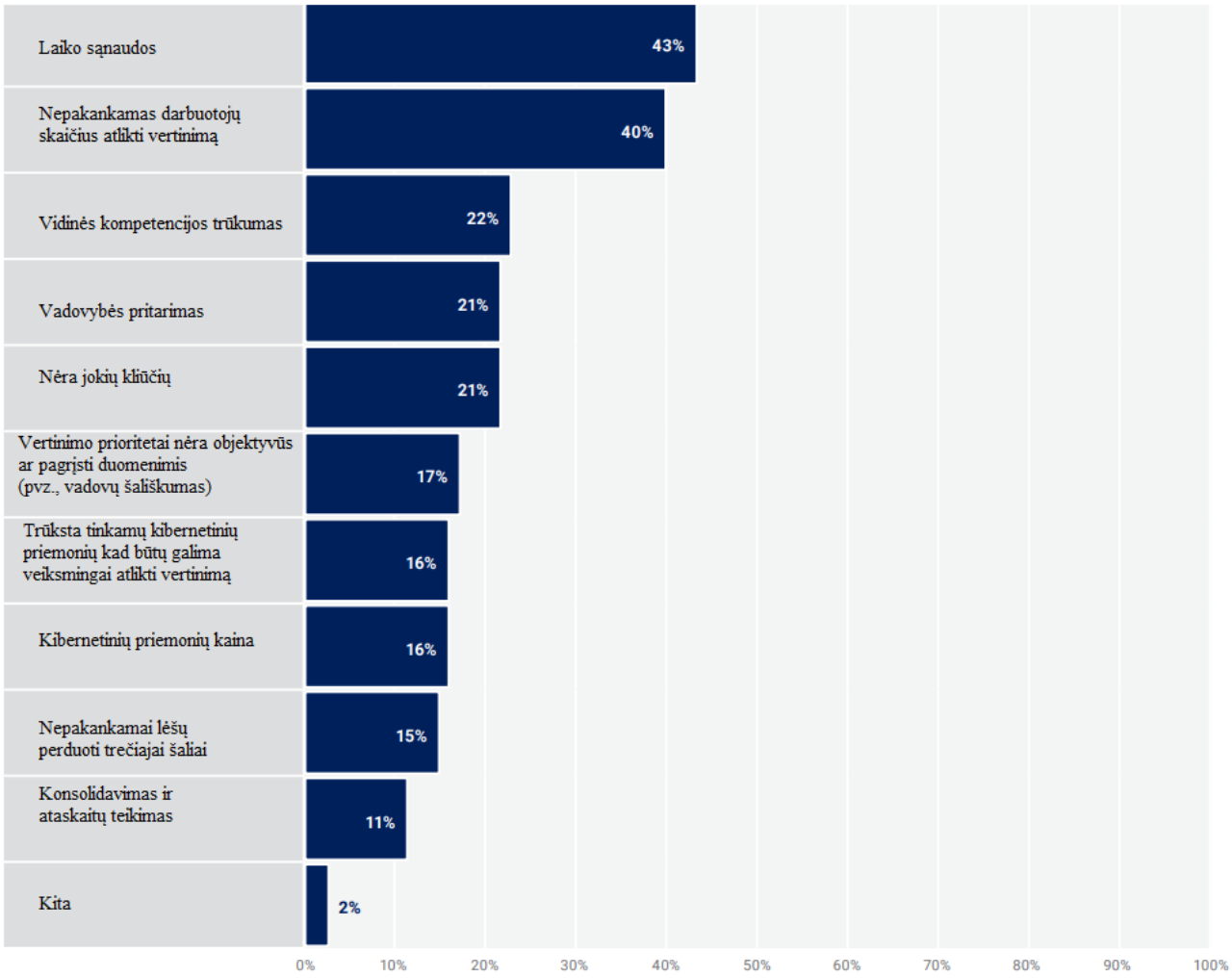
17 pav. **Kibernetinės brandos vertinimas**

Tyrimo dalyvių teigimu jų darbovietės taip pat atlieka kibernetinės rizikos vertinimus. 2022 m. 41% respondentų nurodė, kad kibernetinės rizikos vertinimus atlieka kasmet. Organizacijos, kurios kibernetinės rizikos vertinimus atlieka dažniau nei kartą per metus – 33% (18 pav.). Kibernetinės rizikos vertinimai yra labai svarbūs veiksmingam rizikos veiksnių stebėjimui ir reagavimui į kibernetines grėsmes pajėgumų stiprinimui. Tačiau kai kurios organizacijos susiduria su daug kliūčių, trukdančiu kibernetinės rizikos vertinimą atlikti dažniau. Tyrimo respondentai pagrindinėmis kliūtimis, atlikti organizacijos rizikos vertinimą, įvardino - laiko sąnaudos 43% , nepakankamas darbuotojų skaičius atlikti vertinimą – 40%. Kitos kliūtis (19 pav.).



Šaltinis: adaptuota pagal „Kibernetinio saugumo būklė“ 2022 m.

18 pav. **Kibernetinės rizikos vertinimas**



Šaltinis: adaptuota pagal „Kibernetinio saugumo būklė“ 2022 m.

19 pav. **Kibernetinės rizikos vertinimo kliūtys**

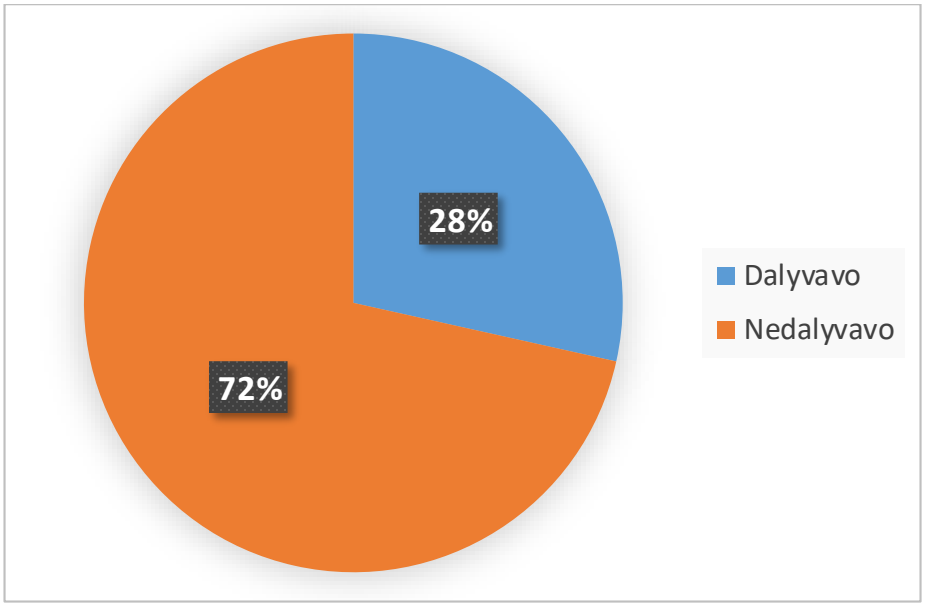
*Apibendrinat, remiantis **tyrimo kriterijumi** - informuotumo apie kibernetinį saugumą identifikavimas, galima daryti prielaidą, kad organizacijose dėl nuolatinio KS saugumo specialistų trūkumo ir dėl kitų darbuotojų kibernetinio saugumo įgūdžių stokos, informuotumas apie kibernetinį saugumą galimai nepakankamas. Tačiau organizacijos deda pastangas siekiant didinti darbuotojų informuotumo lygį apie kibernetinį saugumą ir jo grėsmes. Remiantis **tyrimo kriterijumi** - kibernetinio saugumo vertinimas organizacijoje bei kibernetinio saugumo skatinimas organizacijoje ir darbuotojų įsitraukimo raiška. Galima teigti, kad darbuotojai yra įtraukiami į kibernetinio saugumo mokymo programas bei veiklas. Patys darbuotojai labai teigiamai vertina tokias kibernetinio saugumo ugdymo programas, atitinkamai galima daryti prielaidą, kad darbuotojai pakankamai aktyviai įsiraukia į kibernetinio saugumo skatinimo veikalas. Analizuojant pateiktus duomenis galima*

matyti, kad organizacijos iš esmės vertina kibernetinį saugumą darbovietėje – daugiau nei pusė tyrimo dalyvių atlieka savo organizacijos kibernetinės brandos vertinimus, kas yra labai svarbu keliant bendrą organizacijos kibernetinio saugumo lygį. Atliepiant ***tyrimo kriterijų*** *– nustatyti veiksnius, kurie gali turėti įtakos organizacijos gebėjimui užkirsti kelią kibernetinio saugumo incidentams, nustatyta, kad organizacijos susiduria su tam tikrais veiksniais trukdančiais pasiekti maksimalų kibernetinio saugumo lygį. Darbovietėje stengiamasi atlikti kibernetinės rizikos vertinimus, atsižvelgiant į tai, kaip greitai keičiasi skaitmeninės ekosistemos, tokius vertinimus atlikti vertėtų dažniau. Tačiau dauguma organizacijų susiduria su daug kliūčių, trukdančiu dažnai atlikti kibernetinės rizikos vertinimą. Galimai dėl šių sunkumų ir kitų apribojimų organizacijos negali atlikti vertinimus dažniau nei kartą per metus. Todėl pasakyti, kad organizacijos nevertina kibernetinio saugumo darbovietėje būtų neteisinga.*

Išanalizavus pateiktus duomenis ir aptariant ***tyrimo kriterijų*** *- kibernetinio saugumo atsakomybių pasiskirstymas, galime teigti, kad organizacijose yra suprantamos kibernetinio saugumo rizikos ir atsakomybė už organizacijos kibernetinį saugumą, galimai, pasiskirsto tarp visu darbuotojų. Iš esmės organizacijų darbuotojai pasitiki komandos gebėjimais aptikti kibernetines grėsmes ir sureaguoti į jas. O kibernetinio saugumo ir sąmoningumo ugdymo mokymai daro teigiamą poveikį bendram darbuotojų suvokimui apie kibernetines grėsmes ir ugdo darbuotojų atsakomybę šioje srityje.*

4.2. Anketinės apklausos kiekybinė turinio analizė ir interpretavimas

Dalyvauti tyrime buvo pakvieti **523** dalyviai dirbantys viešajame sektoriuje, respondentai atrinkti**,** taikant ***netikimybinės atrankos*** tipą ***stratifikuotos*** atrankos būdu. Klausimyno pildymas organizuotas tiesiogiai internetinėje svetainėje https://forms.office.com 2023 m. kovo 1 – 6 dienomis. Respondentai tyrime dalyvavo visiškai laisva valia, anonimiškai ir savanoriškai. Iš visų pakviestų dalyvių tyrime sudalyvavo tik **149** respondentai. Sulaukus mažiau nei pusės dalyvių aktyvumo tyrime (20 pav.) galime matyti, kad kibernetinis saugumas viešajame sektoriuje vis dar nėra prioritetinis klausimas.



20 pav. **Viešojo sektoriaus atstovų dalyvavimas anketinėje apklausoje**

Anketinės apklausos duomenų vertė:

- Duomenis yra svarbūs, nes jais vertinamas Lietuvos viešojo sektoriaus įsitraukimas ir informuotumo lygis kibernetinio saugumo srityje. Kadangi didesnė dalis atakų tenka valstybiniam sektoriui (LR VSD ir Antrasis operatyvių tarnybų departamentas prie KAM , 2023) svarbu įsivertinti darbuotojų kompetencijas šiame sektoriuje.
- Duomenis gali būti vertingi valdžios institucijoms, kurie vertina organizacijų KS brandos lygį ir skatiną informuotumą apie kibernetinį saugumą.
- Duomenis taip pat gali būti naudingi tyrėjams, kurie domisi šia sritimi.

Toliau šiame skyriuje nagrinėjami tyrimo dalyvių atsakymai į klausimus. Anketinės apklausos apibendrinti bei sugrupuoti į keturias grupes rezultatai, atspindintys **tyrimo kriterijus** pateikiami lentelėje (žr. 3 lentelė):

1. *Informuotumo apie kibernetinį saugumą identifikavimas*;
2. *Kibernetinio saugumo vertinimas organizacijoje bei kibernetinio saugumo skatinimas organizacijoje ir darbuotojų įsitraukimo raiška*;
3. *Kibernetinio saugumo atsakomybių pasiskirstymas*.

Pirmoji klausimų grupė susijusi su informuotumu apie kibernetinį saugumą, remiantis **tyrimo kriterijumi** - *informuotumo apie kibernetinį saugumą identifikavimas*. Pirmai klausimų grupei priskiriami 1 – 2 ir 6 klausimai.

Antroji ir trečioji klausimų grupė susijusi su kibernetiniu saugumu organizacijoje ir kibernetinio saugumo skatinimu organizacijoje ir darbuotojų įsitraukimu, remiantis **tyrimo**

kriterijumi - *kibernetinio saugumo vertinimas organizacijoje bei kibernetinio saugumo skatinimas organizacijoje ir darbuotojų įsitraukimo raiška*. Antrai ir trečiai klausimų grupėms priskiriami 3 – 5, 7 – 9 ir 11 – 12 klausimai.

Ketvirtoji klausimų grupė susijusi su kibernetinio saugumo atsakomybių pasiskirstymu, remiantis **tyrimo kriterijumi** - *kibernetinio saugumo atsakomybių pasiskirstymas*. Ketvirtai klausimų grupei priskirtas 10 klausimas.

3 lentelė. Informuotumo kibernetinio saugumo klausimu lygio nustatymo tyrimas (N=149)

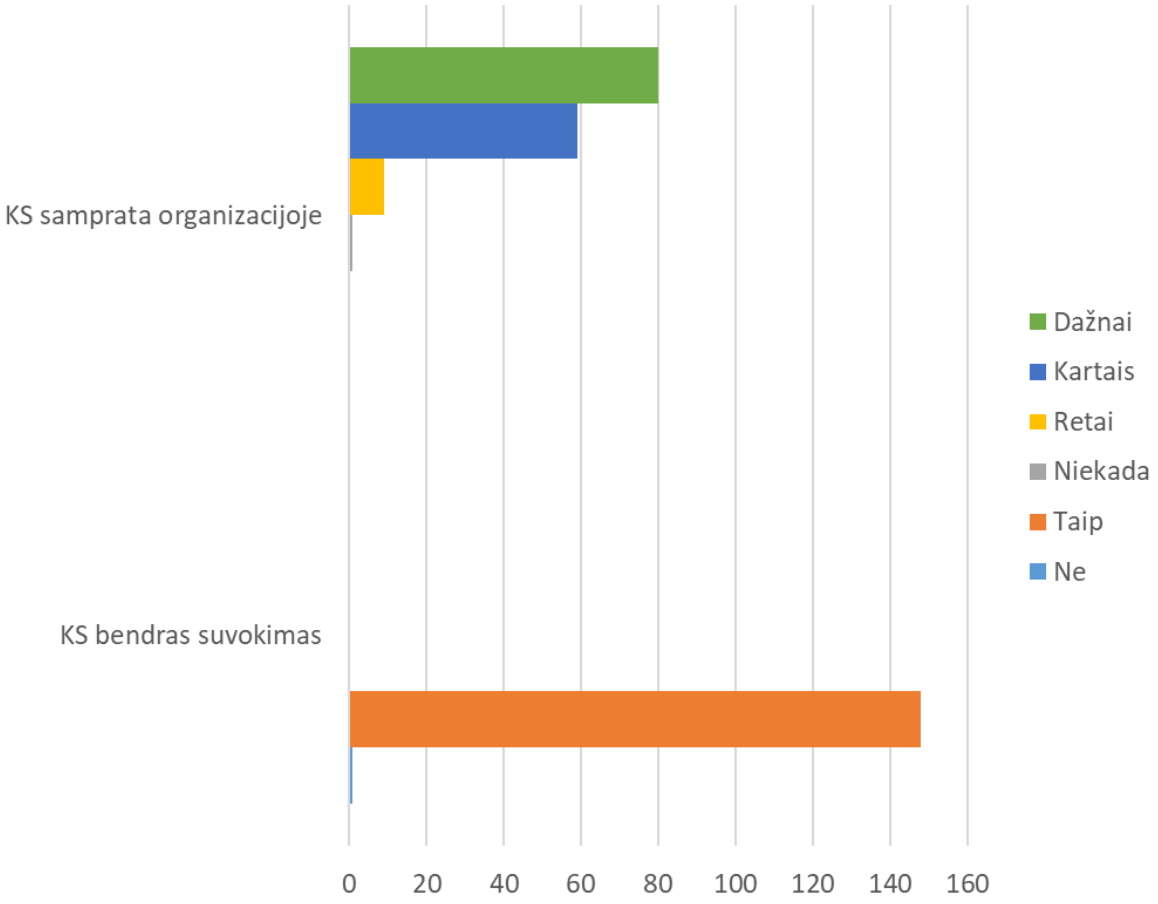
Grupės (tyrimo kriterijus)	Klausimai	Atsakymų dažnis	Išraiška procentais (%)
Informuotumas apie kibernetinį saugumą	1. *Ar kada nors girdėjote terminą "kibernetinis saugumas" arba "kibernetinio saugumo kultūra"?*		
	Taip	148	99
	Ne	1	1
	2. *Kaip dažnai girdite, kad Jūsų darbovietėje būtų kalbama apie kibernetinį saugumą?*		
	Dažnai	80	53
	Kartais	59	40
	Retai	9	6
	Niekada	1	1
	6. *Ar žinote, kam privalote pranešti apie kibernetinio saugumo incidentus?*		
	Taip	140	94
	Ne	9	6
Kibernetinis saugumas organizacijoje	3. *Ar Jūsų darbovietėje kalbama apie kibernetinio saugumo skatinimą?*	137	92
	Taip	12	8
	Ne		
	4. *Ar Jūsų darbovietėje yra vertinamas kibernetinio saugumo lygis?*		
	Taip	86	58
	Ne	3	2
	Nežinau	60	40
	5. *Ar Jūsų darbovietėje taikoma kibernetinio saugumo politika ar strategija?*		
	Taip	96	64
	Ne	3	2
	Nežinau	50	34
Kibernetinio saugumo skatinimas organizacijoje ir darbuotojų įsitraukimas	7. *Ar Jūsų darbovietėje rengiami kibernetinio saugumo mokymai darbuotojams?*		
	Taip	106	71
	Ne	16	11
	Nežinau	27	18
	8. *Ar dalyvaujate kibernetinio saugumo mokymuose?*		
	Taip	99	66
	Ne	7	5

	*į klausimą neatsakė	43	29
	9. *Ar dalyvautumėte kibernetinio saugumo mokymuose?*		
	Taip	41	28
	Ne	2	1
	*į klausimą neatsakė	106	71
	11. *Ar žinote kokios priemonės naudojamos „populiarinti“ kibernetinio saugumo kultūrą Jūsų darbovietėje?*		
	Taip	84	56
	Ne	65	44
	12. *Kokios tai priemonės (PAŽYMĖTI VISUS TINKANČIUS)*		

Plakatai	Istorijos	Patarimų lapai	Vaizdo įrašai	Žaidimai	Išorės konsultantų pristatymai	Mokymai	Kita
4	12	29	17	4	36	72	18

Kibernetinio saugumo atsakomybių pasiskirstymas	10. *Kaip manote, ar kibernetinis saugumas laikomas pirmiausia tos srities žmonių atsakomybe darbovietėje, ar prie kibernetinio saugumo stiprinimo turi prisidėti visi?*		
	Kibernetinio saugumo srities specialistų	6	4
	Kolektyvinis indėlis	143	96

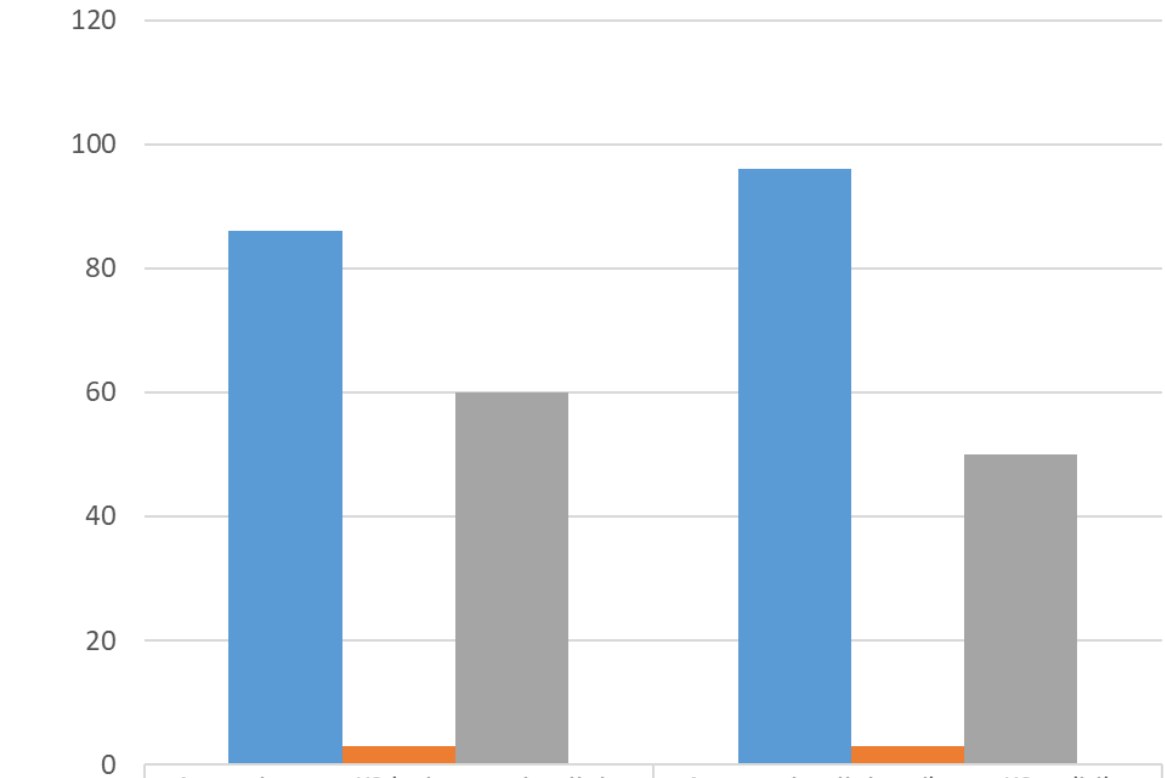
Pirmoji klausimų grupė išryškino, kad bendras darbuotojų suvokimas apie kibernetinį saugumą yra teigiamas - atsakydami į klausimą *Ar kada nors girdėjote terminą "kibernetinis saugumas" arba "kibernetinio saugumo kultūra"?* teigiamai atsakė 99 % (N=148) anketinės apklausos dalyvių. Taip pat organizacijų darbuotojai yra informuoti ir žino kam reikia pranešti apie kibernetinio saugumo incidentus – teigiamai atsakė 94% (N=140) respondentų. Tačiau vis tik kibernetinio saugumo informuotumas organizacijoje nėra pakankamas, nes organizacijoje, šia – kibernetinio saugumo tema, nėra pakankamai komunikuojama. Kibernetinį saugumą ir kultūrą organizacijoje supranta ne visi organizacijos darbuotojai, tyrimo rezultatai pavaizduoti diagramoje (21 pav.) - KS suvokimas suskirstytas į dvi grupes: bendras, anketinės apklausos dalyvių, supratimas apie kibernetini saugumą ir kiek apie kibernetinį saugumą yra komunikuojama organizacijos viduje.



21 pav. **Kibernetinio saugumo samprata organizacijoje**

Antroji ir trečioji klausimų grupė atskleidė organizacijos ir individų požiūrį į kibernetinį saugumą organizacijoje viduje. Didesnė dalis respondentų 92 % (N=137) patvirtino jog darbovietėje yra diskutuojama apie kibernetinio saugumo skatinimą. 8 % (N=12) organizacijų pažymėjo, kad kibernetinio saugumo skatinimo klausimais organizacijos viduje nekalbama. Buvo siekiama nustatyti ar tai turi įtakos kaip organizacijoje yra vertinamas kibernetinio saugumo lygis ir ar yra taikoma kibernetinio saugumo politika (22 pav.). Tokie rodikliai tai taip pat vienas iš būdų parodyti organizacijos kibernetinio saugumo brandos lygį. Vertinant gautus rezultatus išryškėjo, kad maždaug trečdalis organizacijų darbuotojų (40% (N=60)) nežino ar jų darbovietėje vertinamas kibernetinis saugumas ir 34% (N=50) darbuotojų nežino ar jų darbovietėje yra taikoma kibernetinio saugumo politika. Po 2% (N=3) anketinės apklausos dalyvių nurodė, kad jų organizacijose kibernetinio saugumo lygis yra nevertinamas ir kibernetinio saugumo politika ar strategija nėra taikoma.

Atsižvelgiant į tyrimo rezultatus, pastebėta, kad nors daugumoje organizacijų diskutuojama apie kibernetinio saugumo skatinimą, darbuotojai to neidentifikuoja kaip kad jų darbovietės vertintų kibernetinio saugumo lygį.

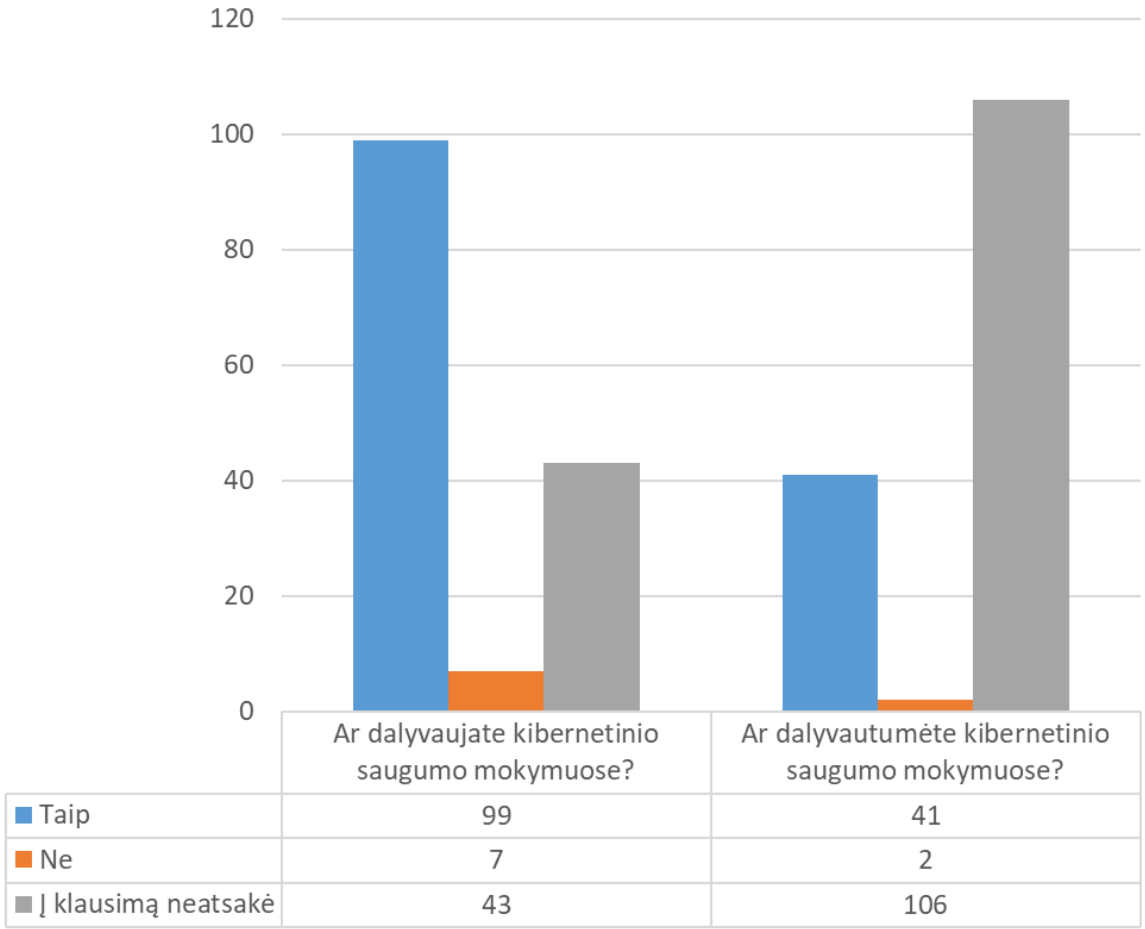


	Ar vertinamas KS lygis organizacijoje	Ar organizacijoje taikoma KS politika
Taip	86	96
Ne	3	3
Nežinau	60	50

22 pav. **Organizacijos kibernetinio saugumo lygis**

Siekiant sužinoti kaip organizacijose skatinamas kibernetinis saugumas ir kaip darbuotojai įsitraukia į kibernetinio saugumo ugdymą organizacijoje. Buvo klausiama ar organizacijose yra organizuojami kibernetinio saugumo mokymai. Kibernetinio saugumo mokymai tai vienas iš būdų stiprinti organizacijų kibernetinio saugumo pajėgumus. Atsakydami į klausimą ar darbovietėje yra rengiami kibernetinio saugumo mokymai – teigiamai atsakė 71% (N=106) anketinės apklausos dalyvių, 11% (N=16) respondentų nurodė, kad kibernetinio saugumo mokymai jų organizacijose nevyksta ir 18% (N=27) – nežino ar tokie mokymai yra rengiami jų darbovietėje. Tyrimas atskleidė ir pačių darbuotojų įsitraukimą į kibernetinio saugumo skatinimo programą organizacijoje. Buvo

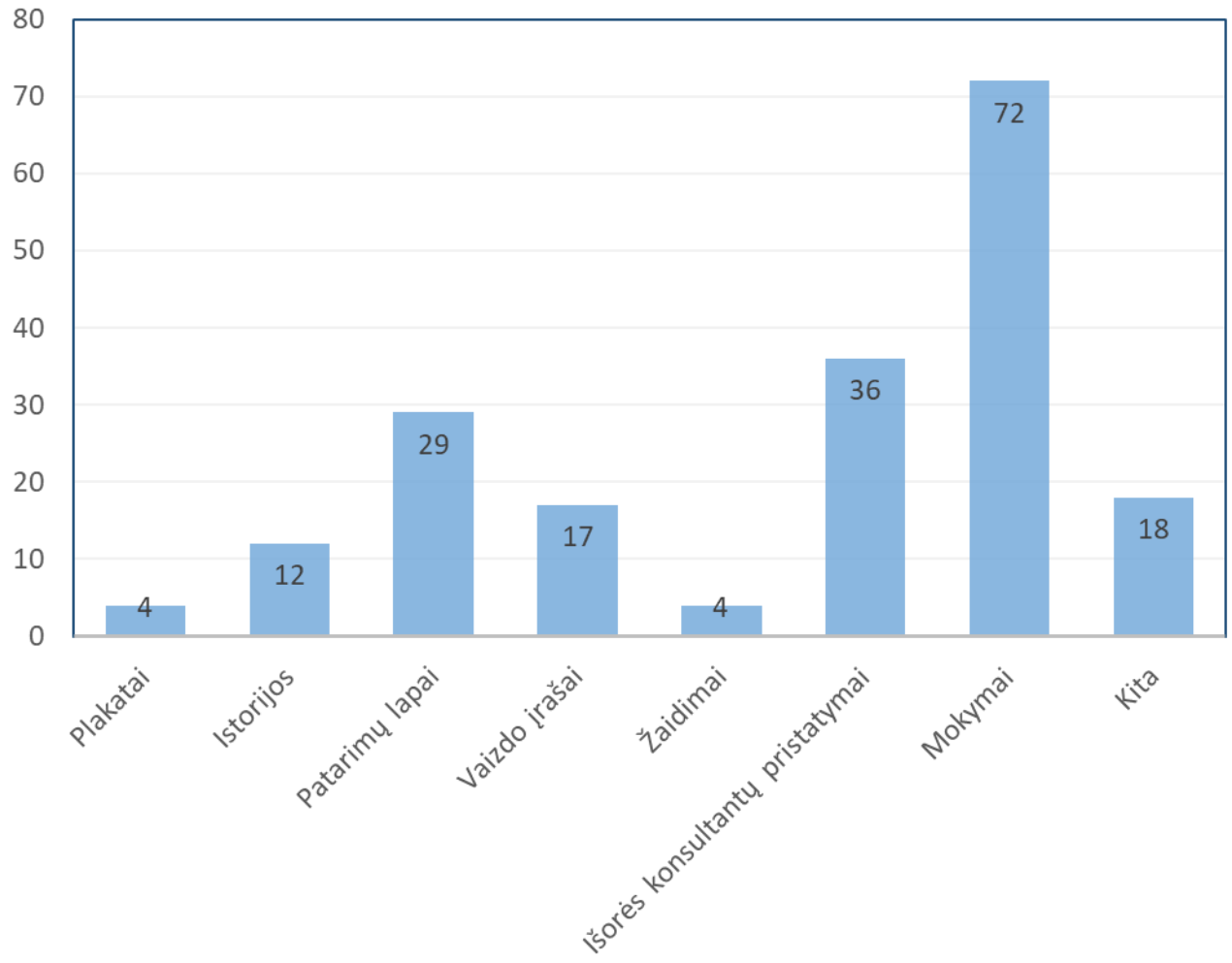
klausiama ar darbuotojai dalyvauja organizuojamuose kibernetinio saugumo mokymuose – 66% (N=99) apklaustųjų nurodė, kad kibernetinio saugumo mokymuose dalyvauja, 5% (N=7) respondentų tokiose mokymuose nedalyvauja ir 29% (N=43) anketinės apklausos dalyvių atsakymo nepateikė apie dalyvavimą kibernetinio saugumo mokymuose. Paklausus tyrimo dalyvių ar jie ateityje dalyvautų kibernetinio saugumo mokymuose, 28% (N=41) tyrimo dalyvių nurodė, kad dalyvautų, 1% (N=2) - nedalyvautų ir net 71% (N=106) tyrime dalyvavusių viešojo sektoriaus atstovų atsakymo nepateikė dėl savo įsitraukimo dalyvauti kibernetinio saugumo mokymuose ateityje (23 pav.).



	Ar dalyvaujate kibernetinio saugumo mokymuose?	Ar dalyvautumėte kibernetinio saugumo mokymuose?
Taip	99	41
Ne	7	2
Į klausimą neatsakė	43	106

23 pav. **Darbuotojų dalyvavimas kibernetinio saugumo mokymuose**

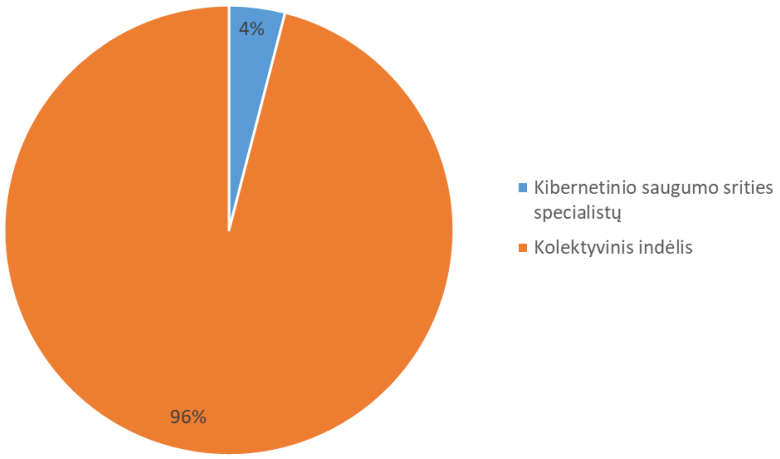
Darbuotojų buvo klausiama ar jie žino kokios priemonės naudojamas jų darbovietėje kibernetinės kultūros skatinimui organizacijoje. 56% (N=84) apklaustųjų nurodė, kad žino kokiomis priemonėmis yra skatinama kibernetinio saugumo kultūra organizacijoje. 44% (N=65) atsakė, jog nežino. Tyrimo dalyvių taip pat buvo prašoma pažymėti jiems žinomas kibernetinio saugumo kultūros skatinimo priemones organizacijoje (24 pav.).



24 pav. **Kibernetinės saugumo kultūros skatinimo priemonės**

Iš pateiktų, tyrimo dalyvių, atsakymų matome, kad dalis darbuotojų yra pasiruošę įsitraukti į įvairias kibernetinio saugumo veiklas ir taip plėsti turimas žinias, suvokimą bei patirtį, tuo pačiu kelti kibernetinio saugumo kultūros lygį organizacijoje. Tačiau esant nepakankamam darbuotojų įsitraukimui į organizacijos kibernetinio saugumo kultūros vystymo veiklas organizacijoms kyla grėsmė patirti kibernetinio saugumo iššūkius.

Ketvirtoji klausimų grupė atskleidė darbuotojų požiūrį į kibernetinio saugumo užtikrinimą organizacijoje ir kieno, darbuotojų nuomone, tai atsakomybė. Vis dar yra manančių 4% (N=6), kad už kibernetinį saugumą organizacijoje atsakingas KS srities specialistas. 96% (N=143) tyrimo dalyvių mano, kad tai yra visų organizacijoje dirbančių atsakomybė (25 pav.).



25 pav. **Kibernetinio saugumo atsakomybių pasiskirstymas**

Tačiau tyrimo rezultatai leidžia daryti prielaidą, kad darbuotojų įsitraukimas į kibernetinį saugumą yra nepakankamas. Nors darbuotojai patvirtina, kad kibernetinis saugumas darbo aplinkoje yra visų darbuotojų atsakomybė, bet tuo pačiu darbuotojų įsitraukimas į kibernetinio saugumo veiklas yra vangus.

*Apibendrinat kiekybinio tyrimo rezultatus pastebimas darbuotojų vangumas ir abejingumas kibernetinio saugumo srityje. Dalyvauti tyrime buvo pakviesti **523** viešajame sektoriuje atstovai, tačiau tyrime sudalyvavo tik **149** respondentai kas sudaro **28 %** visų pakviestų dalyvių. Tai kelia susirūpinimą turint omeny, kad valstybinis sektorius yra patrauklus taikinys įvairiems piktavaliams (JK Vyriausybės kibernetinio saugumo strategija 2022; LR VSD 2023;).*

Nagrinėdami tyrime sudalyvavusių respondentų atsakymus, galima teigti, kad iš esmės judame teisinga linkme. Tyrimo dalyviai supranta kibernetinio saugumo svarbą bei atsakomybės tarpusavyje pasidalijimą stiprinant kibernetinį saugumą ir tuo pačiu atsparumą kibernetinėms grėsmėms organizacijoje. Tačiau svarbu pažymėti, kad darbuotojų įsitraukimas į kibernetinio saugumo veiklas yra nepakankamas ir todėl ne visi darbuotojai gali turėti vienodą kibernetinio saugumo supratimą, nes ši sritis nuolat vystosi ir pasiekti, tarp darbuotojų, vienodą kibernetinio saugumo supratimą gali būti sudėtinga. Daugelis organizacijos darbuotojų vis dar gali turėti žinių spragų apie aktualias ir naujausias kibernetines grėsmes arba klaidingai suvokti kibernetinio saugumo aspektus ir dėl to

organizacija gali būti pažeidžiama kibernetinių grėsmių. Apskritai tai yra neigiamas poveikis bendrai organizacijos kibernetinio saugumo laikysenai.

Tokį tyrimo dalyvių pasiskirstymą galėjo lemti jog vis dar yra darbuotojų, kurie nesidomi saugaus elgesio principais kibernetinėje erdvėje, o galbūt tai galėtų būti komunikacijos spraga institucijos viduje dėl saugaus elgesio elektroninėje erdvėje.

Galima daryti išvadą, kad dėl nepakankamo įsitraukimo į kibernetinio saugumo veiklas organizacijoje viešasis sektorius Lietuvoje, galima sakyti, lieka menkai pasirengęs atremti kibernetines atakas. Dėl šios priežasties darbuotojai gali nežinoti, nesugebėti atpažinti ir tinkamai sureaguoti į iškilusias kibernetines grėsmes organizacijoje. Dėl tokio nepakankamo pasirengimo rizika tapti kibernetinių atakų aukomis dar labiau padidėja, o tai gali turėti rimtų pasekmių, įskaitant didesnį kibernetinių atakų pažeidžiamumą, kenkėjiškų programų ir kibernetinių grėsmių plitimą.

Siekiant apsisaugoti nuo kibernetinių grėsmių labai svarbu, kad asmenys, bendruomenės ir valstybės pirmenybę teiktų kibernetinio saugumo supratimui, švietimui ir aktyvioms priemonėms.

Todėl labai svarbu skatinti švietimą, informuotumą ir raštingumą kibernetinio saugumo srityje, kad žmonės geriau suprastų riziką ir geriausią praktiką, susijusią su jų skaitmeninio gyvenimo apsauga.

4.3. Ekspertinio interviu kokybinio turinio analizė ir interpretavimas

Dalyvauti tyrime buvo pakvieti 11 ekspertų, kurie susiję su kibernetinio saugumo vykdomomis programomis ir darbuotojų kvalifikacijos kėlimu kibernetinio saugumo srityje. Iš visų pakviestų ekspertų susidomėjimą dalyvauti tyrime pareiškė 7 ekspertai. Kvietimai į interviu atrinktiems specialistams buvo išsiuntinėti elektroniniu paštu bei pakviesta asmeniškai. Interviu vyko gruodžio 5 – sausio 09 dienomis.

Kvietime buvo pateikta trumpa tyrimo santrauka, kurioje paaiškintas tyrimo tikslas. Nors pirminiu kvietimų 7 ekspertai – tyrimo dalyviai pareiškė susidomėjimą, tačiau tik 4 iš jų galėjo dalyvauti interviu per nustatytą laiką.

Siekiant užtikrinti reikalingų duomenų gavimą iš ekspertų buvo paruoštas interviu *vienlapis*, kad būtų užtikrintas nuoseklumas pagal tyrimo klausimą.

Interviu sudarė dvi siužetinės linijos ir pusiau struktūruoti klausimai, kurias buvo siekiam išsiaiškinti kokie procesai yra vykdomi siekiant vystyti kibernetinę saugumo kultūrą bei stiprinant

tarpusavio darbuotojų sąveiką stiprinat kibernetinį saugumą viešajame sektoriuje, su kokiomis problemomis yra susiduriama.

Klausimai tyrimo dalyviams buvo išsiųsti prieš interviu, o pats interviu truko vidutiniškai 33 minutes (min. – 25 min., maks.- 42 min.). Dalyviai sutiko, kad pokalbiai būtų įrašinėjami. Siekiant laikytis anonimiškumo visi asmens duomenis buvo pašalinti arba nuasmeninti, interviu dalyviams buvo priskirti kodai - I1, I2, I3 ir I4. Interviu klausimai atspindi iškeltus **kriterijus:** *Informuotumo apie kibernetinį saugumą identifikavimas; Kibernetinio saugumo vertinimas organizacijoje bei kibernetinio saugumo skatinimas organizacijoje ir darbuotojų įsitraukimo raiška; Kibernetinio saugumo atsakomybių pasiskirstymas.*

Ekspertinis interviu sudarė dvi siužetines linijas:

Pirmoji siužetinė linija susijusi su informuotumu apie kibernetinį saugumą, remiantis **tyrimo kriterijumi** - *informuotumo apie kibernetinį saugumą identifikavimas*. Pirmai siužetinei linijai priskiriami 1 – 2 klausimai (žr. 2 priedą).

Antroji siužetinė linija susijusi su kibernetinio saugumo skatinimu ir darbuotojų įsitraukimu į kibernetinio saugumo veiklas organizacijoje bei kibernetinio saugumo atsakomybių pasiskirstymu, remiantis **tyrimo kriterijais** - *kibernetinio saugumo vertinimas organizacijoje bei kibernetinio saugumo skatinimas organizacijoje ir darbuotojų įsitraukimo raiška*; *kibernetinio saugumo atsakomybių pasiskirstymas*. Antrai siužetinei linijai priskiriami 3 – 6 klausimai (žr. 2 priedą).

Ekspertiniam interviu buvo taikomas kokybinis turinio (angl. *Content*) analizės metodas.

Pokalbis prasidėjo nuo prisistatymo ir tyrimo pristatymo bei dalyvių sutikimo įrašyti interviu. Toliau buvo naudojamasi parengtu interviu klausimynu užduodant atitinkamus tiriamuosius klausimus. Įrašyti atsakymai buvo transkribuoti ir parengta analizė (4 lentelė).

4 lentelė. Ekspertinio interviu kokybinio turinio (angl. *Content*) analizė

Tyrimo kriterijus	**Interviu klausimai, atitinkantys tyrimo kriterijų.**	**Iliustruojantys teiginiai (tyrimo dalyvių atsakymų tekstas)**
Informuotumo apie kibernetinį saugumą identifikavimas	1. Koks šiandien dienai yra viešojo sektoriaus darbuotojų informuotumas apie kibernetinį saugumą?	I1 „<...iš tikrųjų didėjant atakų mastams didėja ir žmonių supratimas bei gebėjimas atpažinti, kad juos kažkas vyksta negerai...>“ I2 <...pakankamai nepakankamas...> ; <...mano nuomone neatitinkantis

		kibernetinio pavojaus <...> viešojo sektoriaus darbuotojai informuojami apie kibernetines grėsmes nepakankamai...>“ I3 „<...trumpai tariant situacija viešajame sektoriuje tūrėtų būti geresnė...>“ I4 „<...darbuotojus daugiau ar mažiau supažindina, taigi jie tikrai žino kas yra kibernetinis saugumas <....> žinių lygis skirtingas ...>“
	2. Ar pasikeitė viešojo sektoriaus suvokimas apie kibernetinį saugumą, Rusijos išpuolio prieš Ukrainą kontekste?	I1 „<...suvokimas pasikeitė, bet vis dar laukiama stiprių rezultatų ...>“ I2 „<...kalbų lygyje , taip, tikrai šnekama apie tai daugiau <...> tik kalbėdami apie tai dažniau, bet nesiimdami skubių veiksmų <...> taisyti spragų <...> naudos nepakankamai. I3 „<...apie kibernetinį saugumą ir grėsmes, diskusijos suaktyvėjo ...>“ I4 „<...visada kai ištinka bėda apie tai šnekama daugiau, atsiranda susirūpinimas ir dėl savo valdomo skaitmeninio turto ...>“
Kibernetinio saugumo vertinimas organizacijoje bei kibernetinio saugumo skatinimas	3. Kaip viešajame sektoriuje vertinamas kibernetinio saugumo lygis ir kaip taikomos kibernetinio saugumo strategijos ar politika?	I1 „<...iš esmės gerėja kibernetinio saugumo lygis <...> iš žmogiškosios pusės esminė problema, kad ne visi darbuotojai linkę laikytis kibernetinio saugumo politikos ...>“ I2 „<...dedamos didelės pastangos gerinant viešojo sektoriaus

organizacijoje ir darbuotojų įsitraukimo raiška		kibernetinį saugumą <...> trūkumas kad, skyrių ar komandų vadovai (nesusijusiu su kibernetiniu saugumu) į kibernetinį saugumą žiūri kaip į primestines funkcijas <...> prie kiekvieno saugos specialisto *nepastatysi* ...>“ I3 „<...pajėgumai turėti aukšta kibernetinio saugumo lygį yra <...> vadovybė rodo blogą pavyzdį ...>“ I4 „<...kaip sakoma „žuvis pūva nuo galvos“ kol mūsų pareigūnai nesupras, kad kibernetinio saugumo politika taikoma ir jiems jokio pagerėjimo nebus ...>“
	4. Kodėl saugumui užtikrinti svarbu sutelkti dėmesį į žmones (darbuotojus)?	I1 „<... žmogiškasis faktorius ir čia neužprogramuosi, kad jis neklystų ir darbą darytų pagal algoritmus <...> Žmogus tai visada rizika ...>“ I2 „<...būtent žmogus jiems (įsilaužėliams) padės apeiti technologines apsaugos priemones ...> taigi todėl labai svarbu stiprinti žmogiškąjį saugumo sluoksnį.“ I3 „<... darbuotojai yra esminiai organizacijos saugumo grandinės jungtys <...>žmogus yra potencialus saugumo pažeidimo šaltinis, nes gali atlikti na arba neatlikti tam tikrus veiksmus ...>“

		I4 „Darbuotojai atlieka labai svarbų vaidmenį užtikrinant kibernetinį saugumą ...>“
	5. Kokie galėtų būti svarbiausi aspektai siekiant subalansuoto kibernetinio saugumo viešajame sektoriuje?	I1 “<… vadovybė privalo užtikrinti, kad kibernetinis saugumas taptų organizacijos prioritetu ...>“ I2 “<…vien techninių - technologinių sprendimų nepakaks <...> dėmesys žmogiškajai pusei <...> mokymai, - turi vykti nuolatinis procesas ...>“ I3“<…kad būtų laikomasi nustatytos saugumo politikos ir procedūrų <...> kad būtų pranešama apie bet kokius saugumo incidentus ...>“. I4 “<… kibernetinio saugumo priemonių diegimas <…> visi darbuotojai turi būti atsakingais kibernetinės erdvės valdytojais …>”.
Kibernetinio saugumo atsakomybių pasiskirstymas	6. Jūsų nuomone, už kibernetinį saugumą atsakinga vyriausybė, organizacijos ar kiekvienas asmeniškai? Kieno atsakomybė yra kibernetinis saugumas?	I1 „Mano nuomone kibernetinis saugumas yra per didelis darbas kažkam vienam susitvarkyti<…> kiekvienas iš paminėtų yra atsakingas, ne tik tie, kurie žino, todėl atsakomybė iš tikrųjų tenka mums visiems.“ I2 „Kibernetinis saugumas yra bendra atsakomybė ...>“ I3 „<...iš esmės tai bendra atsakomybė.“

		I4 "<...*užkrauti* tik konkrečius skyrius ar aukštesnę vadovybę paprasčiausiai nepakanka, kad užtikrintumėte kibernetinį saugumą <...> esame savo organizacijos akys, todėl turite užtikrinti, kad organizacijos durys visada būtų užrakintos ir apsaugotos nuo kibernetinių nusikaltėlių<...>Trumpai tariant, kibernetinis saugumas yra bendra atsakomybė...>"

Pirmoji siužetinė linija susijusi su informuotumu apie kibernetinį saugumą, remiantis **tyrimo kriterijumi** - *informuotumo apie kibernetinį saugumą identifikavimas* išryškėjo, kad viešojo sektoriaus darbuotojai iš esmės nepakankami informuojami apie kibernetines grėsmes. I2 pažymėjo, kad viešojo sektoriaus darbuotojų informuotumas ir pasiruošimas atpažinti kibernetines grėsmes yra neatitinkantis šių dienų grėsmių – apibūdindamas viešojo sektoriaus informuotumą kaip <...pakankamai nepakankamas...>. Bet I1 teigimu, kad išaugusių sėkmingų atakų skaičiaus kontekste ir darbuotojams praktiškai susidūrus su kibernetinėmis grėsmėmis atitinkamai didėja ir žmonių suvokimas gebėti atpažinti kibernetines grėsmes. Tačiau I3 ir I4 mano, kad darbuotojai galėtų būti skatinami labiau domėtis kibernetiniu saugu, nes jų žinių lygis yra skirtingas taigi nevisi yra vienodai stiprūs atremiant kibernetines atakas ir todėl bendras informuotumas apie kibernetines grėsmes viešajame sektoriuje nėra toks koks turėtų būti.

Vertinant viešojo sektoriaus suvokimą apie kibernetinį saugumą, Rusijos išpuolio prieš Ukrainą kontekste. Ekspertai šiuo klausimu, galima sakyti, buvo vieningi – viešojo sektoriaus suvokimas lyg ir pasikeitė, t.y. buvo sureaguota, kad tai didelė grėsmė ir kad reikia stiprinti pajėgumus, motyvuoti darbuotojus elgtis atsakingai kibernetinėje erdvėje. Tačiau vis dar laukiama apčiuopiamų rezultatų, kad kibernetinis saugumas viešajame sektoriuje tapo kartais stipresnis.

Antroji siužetinė linija susijusi su kibernetinio saugumo skatinimu ir darbuotojų įsitraukimu į kibernetinio saugumo veiklas organizacijoje bei kibernetinio saugumo atsakomybių pasiskirstymu, remiantis **tyrimo kriterijais** - *kibernetinio saugumo vertinimas organizacijoje bei kibernetinio*

saugumo skatinimas organizacijoje ir darbuotojų įsitraukimo raiška; *kibernetinio saugumo atsakomybių pasiskirstymas*. Interviu informantu (I1, I2, I3, I4) teigimu kibernetinis saugumas nors ir lėtas procesas, viešajame sektoriuje, bet iš esmės gerėjantis. Pagrindinė problema, I1 teigimu, darbuotojas – „*<... iš žmogiškosios pusės esminė problema, kad ne visi darbuotojai linkę laikytis kibernetinio saugumo politikos...>*“. Informanto I2 teigimu, vadovybė neparodo gerojo pavyzdžio kibernetinio saugumo kontekste – „*<...trūkumas kad, skyrių ar komandų vadovai (nesusijusiu su kibernetiniu saugumu) į kibernetinį saugumą žiūri kaip į primestines funkcijas...>*“. Ekspertinio interviu dalyviai I3 ir I4 taip pat pažymi, kad yra atveju kuomet komandos vadovas, pats nesilaiko visų kibernetinio saugumo reikalavimų darbo aplinkoje ir tuo pačiu rodo blogą pavyzdį savo darbuotojams. Todėl dažnu atveju kibernetinio saugumo politika yra neveiksminga. Norint turėti efektyvų kibernetinį saugumą organizacijoje ekspertinio interviu dalyviai pabrėžia, kad svarbu ugdyti veiksmingus tarpusavio darbuotojų bendradarbiavimo procesus. Darbuotojai anot kibernetinio saugumo ekspertų *„<...yra esminiai organizacijos saugumo grandinės jungtys <...> žmogus yra potencialus saugumo pažeidimo šaltinis, nes gali atlikti na arba neatlikti tam tikrus veiksmus ...>“* – I3. I1 – teigimu *„<...Žmogus tai visada rizika ...>“*, I2 *„<...būtent žmogus jiems (įsilaužėliams) padės apeiti technologines apsaugos priemones ...>*“.

Siekiant organizacijoje subalansuoto kibernetinio saugumo, tyrimo dalyviai pabrėžia, reikia ne tik techninių priemonių, bet ir susifokusuoti ties žmogiškaisiais ištekliais. Anot ekspertų subalansuotas tandemas tarp šių dviejų aspektų – techninio ir žmogiškojo padės pasiekti efektyvų kibernetinį saugumą organizacijoje. Įgalinant šiuos kibernetinio saugumo procesus svarbus vadovybės palaikymas - I1 *“<... vadovybė privalo užtikrinti, kad kibernetinis saugumas taptų organizacijos prioritetu ...>“*; I4 *„<...visi darbuotojai turi būti atsakingais kibernetinės erdvės valdytojais ...>”.*

Aptariant kibernetinio saugumo atsakomybės klausimą tyrimo dalyviai teigia, kad tai visų organizacijos darbuotojų bendra atsakomybė. Informantas I1 *„Mano nuomone kibernetinis saugumas yra per didelis darbas kažkam vienam susitvarkyti...>“*; I4 *„<...esame savo organizacijos akys, todėl turite užtikrinti, kad organizacijos durys visada būtų užrakintos ir apsaugotos nuo kibernetinių nusikaltėlių...>“*.

4.4. Kibernetinės kultūros viešajame sektoriuje tobulinimo gairės

Remiantis atliktu kombinuotu tyrimu, taikant ekspertinio interviu ir anketinės apklausos metodus bei atliekant antrinių statistinių duomenų analizę, parengtos „Kibernetinės kultūros viešajame sektoriuje tobulinimas“ garės (5 lentelė).

5 lentelė. Kibernetinės kultūros viešajame sektoriuje tobulinimo gairės

Silpnoji pusė/ vieta	Galima (-os) rekomendacija (-os)
Teisinė aplinka	✓ Kadangi darbuotojai yra linkę nesilaikyti organizacijos saugumo politikos, organizacijoms reikia **permąstyti savo informuotumo apie kibernetinį saugumą strategiją** arba ją parengti jei tokios organizacija vis dar neturi. ✓ **Stiprinti tarpinstitucinį bendradarbiavimą ir derinti metodus.** Kibernetinio saugumo taisyklės turėtų būti taikomos vienodai visose viešojo sektoriaus organizacijoje, kad būtų užtikrinta kokybiškas ir nuoseklus bendradarbiavimas. ✓ **Darbuotojų kibernetinio saugumo kompetencijų *žemėlapio* sudarymas**. Mažiausiai kasmetinis darbuotojų **testavimas kibernetinio saugumo įgūdžiams įvertinti.** Toks *kompetencijų žemėlapis* bus naudingas vertinant kibernetinio saugumo mokymų ir veiklos naudą ir atitinkamai atlikti korekcijas kibernetinio saugumo mokymų programose organizacijoje.
Vadovų pritarimo ir įsitraukimo stoka	✓ Visi organizacijos darbuotojai atlieka bendrą vaidmenį užtikrinant organizacijos kibernetinio saugumą. Sveikai kibernetinio saugumo kultūrai vystyti reikalinga įtraukti darbuotojus visais lygiais. **Pirmame etape** – pradėti dialogą ir įtraukti vadovybę **rekomenduotina rengti kibernetinio saugumo mokymus bei veiklas grupėms** (darbuotojai, komandų vadovai, aukščiausia vadovybė ir t.t.). **Antrame etape** grupes **miksuoti** per interaktyvias kibernetinio saugumo veiklas . ✓ **Skirti daugiau** lėšų kibernetinio saugumo programoms.
Darbuotojų įsitraukimo stoka	✓ Dažnai „PowerPoint“ prezentacijos yra nuobodžios, todėl darbuotojų įsitraukimas nepakankamas. **Skatinti įsitraukimą į kibernetinio saugumo veiklas per interaktyvias veikas**. Įtraukianti patirtis sustiprins darbuotojų vaidmenį užtikrinant organizacijos kibernetinį saugumą. ✓ Taip pat rekomenduojama **rengti bendras tarpinstitucines interaktyvias kibernetinio saugumo veiklas.**
Švietimo trūkumas organizacijoje	✓ Atsižvelgiant į tai, kad kibernetinis saugumas organizacijose gali būti didelė problema, reikėtų atkreipti dėmesį į tai, kad **organizacijoje** būtų **daugiau kibernetinio saugumo specialistų**, kurie būtų **atsakingi už švietimo veiklą.** ✓ Darbuotojų **žinių stiprinimas** apie kibernetines **grėsmes su kuriomis susiduria pati organizacija, jų sistemos ir jie patys.**

	✓ **Didinti kibernetinio saugumo mokymų dažnį**, rengiant trumpalaikius kursus/praktikas , kad žmonės geriau suprastų apie riziką ir saugumą. ✓ Mokymai galėtų apimti net tik dažnai naudojamus scenarijus kaip „*fishing*“ atakos, bet ir **derinti kitus kibernetinio saugumo scenarijus**. ✓ **Akcentuoti** kibernetinio saugumo **svarbą** – kokią **naudą** duoda kibernetinis saugumas. **Paskatinti** darbuotojų **motyvaciją elgtis saugiai** ir atsakingai kibernetinėje erdvėje visais gyvenimo atvejais. ✓ **Mokymosi medžiaga** turi būti prieinama ir **lengvai suprantama** ne kibernetinio saugumo srityje dirbantiems darbuotojams.
Diskusijos dėl kibernetinio įncidento atskleidimo	✓ **Daugiau komunikuoti** su darbuotojais, **įtraukiant į diskusijas** dėl kibernetinio incidentų ✓ Darbuotojai turėtų būti **skatinami pranešti apie bet kokią įtartiną veiklą** ar incidentus, susijusius su kibernetiniu saugumu. Tai padės organizacijai nedelsiant imtis veiksmų rizikai sumažinti
Bendras KS sąmoningumo trūkumas	✓ Daugiau dėmesio reiktų skirti KS švietimui, kad darbuotojai gebėtų atskirti IT administratorius nuo KS specialistų bei identifikuoti jų atsakomybes. ✓ Skatinti darbuotojus laikytis saugios praktikos: naudoti sudėtingus slaptažodžius, naudoti daugiafaktorinį autentifikavimą, laikytis švaraus stalo politikos, būti apdariems diskutuojant apie darbo reikalus.

IŠVADOS IR REKOMENDACIJOS

- Analizuojant mokslinę literatūrą nustatyta, kad kibernetinis saugumas tai daugialypis ir sudėtingas reiškinys, kuris neturi bendro apibrėžimo, o taip pat vieningo supratimo ar bendros vizijos. Todėl skirtingos šalys turi savitą kibernetinio saugumo sampratą. Remiantis moksline literatūra, bendrąja prasme, kibernetinio saugumo supratimas tai žmonių žinios, įsitikinimai, požiūris, normos ir vertybės, geriausios praktikos ir rizikos, susijusios su individo skaitmeninio turto, privatumo internete ir informacijos saugumo apsauga, suvokimas ir kaip tai pasireiškia žmonių elgesyje su informacinėmis technologijomis. Remiantis antriniais statistiniais duomenimis nustatyta, kad organizacijose dėl nuolatinio kibernetinio saugumo specialistų trūkumo ir dėl kitų darbuotojų kibernetinio saugumo įgūdžių stokos, informuotumas apie kibernetinį saugumą galimai nepakankamas. Tačiau organizacijos deda pastangas siekiant didinti darbuotojų informuotumo lygį apie kibernetinį saugumą ir jo grėsmes
- Moksliniuose šaltiniuose teigiama, kad organizacijos silpniausia kibernetinio saugumo grandis yra žmogus. Būtent dėl žmogiškojo faktoriaus organizacija patyria kibernetinių saugumo iššūkių. Žmogaus elgsenos kibernetiniame saugume neįmanoma užprogramuoti, taip kaip žmogus elgiasi skaitmeninėje erdvėje lemia jo įpročiai, vertybės, emocinė būsena. Nustatyta, kad kibernetinis saugumas susijęs ir su technologiniu ir su žmonių saugumu. Technologinio saugumo kontrolės priemonės orientuotos į technologijos vientisumo palaikymą, technologinio saugumo naudojimo galimybių užtikrinimą, apsaugą nuo kenkėjiškų programų ir prieigos kontrolę. Kita vertus, žmogaus saugumas yra susijęs su žmonių tarpusavio sąveika, kuriai tarpininkauja technologijos. Šiandien dėl technologinės priklausomybės kyla daugybė saugumo iššūkių, todėl svarbu suprasti kasdienę saugumo praktiką ir iššūkius, kuriuos kelia technologijų integravimas į daugelį gyvenimo ir darbo aspektų. Dauguma organizacijų rengia kibernetinio saugumo politiką, siekdamos informuoti darbuotojus apie numatomas grėsmes ir riziką bei nustatyti standartus, kaip darbuotojai turėtų elgtis kibernetinėje aplinkoje. Tačiau, nustatyta, kad darbuotojai yra linkę nesilaikyti organizacijos saugumo politikos ir laiko tai labiau rekomendacijomis. Neretai kibernetinės saugos pažeidimai sumažina organizacijų technologijomis grįstų priemonių efektyvumą. O taip yra todėl, kad organizacijoms trūksta esminio apsaugos elemento – žmogiškojo faktoriaus. Todėl kibernetinės kultūros kūrimas organizacijoje yra svarbus aspektas siekiant valdyti žmogiškojo veiksnio riziką.
- Šiuo metu viešojo sektoriaus kibernetinis saugumas Lietuvoje neatitinka dabartinio kibernetinio grėsmių lauko. Remiantis nagrinėtais dokumentais bei atlikto kombinuoto tyrimo rezultatais

išryškėjo, kad viešojo sektoriaus organizacijos nėra aktyviai dalyvaujančios kibernetinio saugumo mokymuose ar veiklose. Todėl svarbu pažymėti, kad ne visi darbuotojai gali turėti išsamų kibernetinio saugumo supratimą, nes ši sritis nuolat vystosi ir gali būti sudėtinga užtikrinti vienodą darbuotojų kibernetinio saugumo žinių lygį. Daugelis žmonių vis dar gali turėti žinių spragų arba klaidingai suvokti tam tikrus kibernetinio saugumo aspektus, todėl gali būti pažeidžiami kibernetinių grėsmių. Būtina skatinti švietimą, informuotumą ir raštingumą kibernetinio saugumo srityje, kad žmonės geriau suprastų riziką, susijusią su jų skaitmeninio gyvenimo apsauga.

Rekomendacijos:

Konceptualiai ir empiriškai pagrindus, sukonstruotos gairės, siūloma:

- Tam, kad užtikrinti efektyvų viešojo sektoriaus kibernetinį saugumą, reikia skirti daugiau dėmesio žmogiškiesiems ištekliams ugdant jų kompetencijas kibernetinio saugumo srityje. Gerindami darbuotojų supratimą apie kibernetinį saugumą darbo aplinkoje, bus efektyviau apsaugotas organizacijos skaitmeninis turtas ir sumažinta kibernetinių išpuolių rizika.
- Kad kibernetinio saugumo mokymai ir veikla būtų efektyvūs, rekomenduojama įsivertinti darbuotojų kibernetinio saugumo kompetencijas, kad pritaikyti į įgūdžių ir žinių trūkus orientuotas kibernetinio saugumo programas.
- Organizacijose rekomenduojama turėti už kibernetinį švietimą atsakingą padalinį / darbuotoją-specialistą. Skatinti įsitraukimą į kibernetinio saugumo veiklas per interaktyvias veikas. Įtraukianti patirtis sustiprins darbuotojų vaidmenį užtikrinant organizacijos kibernetinį saugumą.
- Valstybės tarnautojų darbuotojų kompetencijos turi būti ugdomos atsižvelgiant į jų darbo specifiką, jų poreikį ir turimų įgūdžių lygį.

LITERATŪROS SĄRAŠAS

1. Alahmari A.A. ir Duncan R.A. (2021). *Investigating Potential Barriers to Cybersecurity Risk Management Investment in SMEs*. Prieiga per internetą (PDF) Investigating Potential Barriers to Cybersecurity Risk Management Investment in SMEs (researchgate.net)
2. Alshaikh M. (2020). *Developing cybersecurity culture to influence employee behavior: A practice perspective*. Prieiga per internetą: Developing cybersecurity culture to influence employee behavior: A practice perspective - ScienceDirect
3. Ba School Of Business and Finance. *Professional Master's Degree in Cybersecurity Management*. Prieiga per internetą: Professional Master's Degree in Cybersecurity Management (ba.lv) [žiūrėta: 2023 04 06]
4. Bukauskas L. ir kt. (2022). *Ataskaita Lietuvos kibernetinio saugumo kompetencijų žemėlapis*. Prieiga per internetą: https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf
5. Center for Infrastructure Assurance and Security, CIAS (2023) .*The Community Cyber Security Maturity Model*. Prieiga per internetą: Our Maturity Model, the CCSMM – The UTSA CIAS
6. CERT.LV Prieiga per internetą: CERT.LV - CERT.LV lekcijas skolās un valsts un pašvaldību iestādēs 2022.
7. Chapman P. (2020). *Are your IT staff ready for the pandemic-driven insider threat?* Prieiga per internetą: Are your IT staff ready for the pandemic-driven insider threat? - ScienceDirect
8. Ekonomikos reikalų ir ryšių ministerija (2019). *Cybersecurity strategy 2019 -2022*. Prieiga per internetą: e-Estonia Programme for Cyber Security - e-Estonia
9. ENISA (2017). *Cyber Security Culture in organisations*. Prieiga per internetą: Cyber Security Culture in organisations — ENISA (europa.eu)
10. ENISA (2021). *Enisa Threat Landscape 2021*. Prieiga per internetą: ENISA Threat Landscape 2021 — ENISA (europa.eu)
11. ENISA (2021). *Raising Awareness Of Cybersecurity*. Prieiga per internetą: Raising Awareness of Cybersecurity — ENISA (europa.eu)
12. ENISA (2022). *Enisa Threat Landscape 2022*. Prieiga per internetą: ENISA Threat Landscape 2022 — ENISA (europa.eu)
13. Ertan A. ir kt. (2018). *Everyday cyber security in organisations*. Prieiga per internetą: 2004.11768.pdf (arxiv.org)

14. ES Taryba ir Europos Vadovų Taryba. *Kibernetinis saugumas: kaip ES kovoja su kibernetinėmis grėsmėmis*. Prieiga per internetą: Kibernetinis saugumas: kaip ES kovoja su kibernetinėmis grėsmėmis - Consilium (europa.eu) [žiūrėta: 2023 04 26]
15. Esidross.lv. *Saugumas Latvijos kibernetinėje erdvėje.* Prieiga per internetą: Esidrošs – vietne, kurā apkopota noderīga informācija tiem, kam rūp sava un sava datora, telefona vai citu viedierīču drošība internetā (esidross.lv)
16. Estijos informacinių sistemų tarnyba (Riigi Infosüsteemi Amet, RIA). *Cyber Security in Estonia 2021*. Prieiga per internetą: https://www.ria.ee/medial/1494/download
17. Estijos informacinių sistemų tarnyba (Riigi Infosüsteemi Amet, RIA). *Cybersecurity in Estonia 2022*. Prieiga per internetą: https://www.ria.ee/media/1490/download
18. Europos audito rūmai (2019). *Veiksmingos ES kibernetinio saugumo politikos iššūkiai.* Prieiga per internetą: Challenges to effective EU cybersecurity policy (europa.eu)
19. Giantas D. H. ir Liaropoulos A. (2019). *Cybersecurity in the EU: Threats, frameworks and future perspectives*. Prieiga per internetą: (PDF) Cybersecurity in the EU: Threats, frameworks and future perspectives (researchgate.net)
20. HM Government (2022). *Government Cyber Security Strategy 2022 – 2030*. Prieiga per internetą: Government Cyber Security Strategy: 2022 to 2030 - GOV.UK (www.gov.uk)
21. ISACA (2020). *State of Cybersecurity 2020.* Prieiga per internetą: State of Cybersecurity 2020 (isaca.org)
22. ISACA (2021). *State of Cybersecurity 2021*. Prieiga per internetą: State of Cybersecurity 2021 | ISACA
23. ISACA (2022). *State of Cybersecurity 2022*. Prieiga per internet: State of Cybersecurity 2022 | ISACA
24. KAM (2018). *Nacionalinė kibernetinio saugumo strategija*. Prieiga per internetą: nacionaline-kibernetinio-saugumo-strategija.pdf (kam.lt)
25. KAM (2021). *Nacionalinė kibernetinio saugumo būklės ataskaita 2021.* Prieiga per internet: Nacionaline-kibernetinio-saugumo-ataskaita-2021.pdf (kam.lt)
26. KAM (2022). *Svarbiausia Lietuvos kibernetinio saugumo būklės statistika ir tendencijos. 2021-2022 m. I ketv*. Prieiga per internetą: Svarbiausia-Lietuvos-kibernetinio-saugumo-bukles-statistika-ir-tendencijos-2021-2022-I-ketv.pdf (nksc.lt)
27. Kauno technologijos universitetas. *Informacijos ir informacinių technologijų sauga*. Prieiga per internetą: Informacijos ir informacinių technologijų sauga | KTU [žiūrėta: 2023 04 06]

28. Latvijos gynybos ministerija (2019). *Cybersecurity Strategy of Latvia 2019-2022*. Prieiga per internetą: Informatīvais ziņojums "Latvijas kiberdrošības stratēģija 2019.-2022.gadam" (mod.gov.lv)
29. LCC tarptautinis universitetas. *Cybersecurity bootcamp*. Prieiga per internetą: *Cybint Cybersecurity Bootcamp lithuanian (lcc.lt)* [žiūrėta: 2023 04 06]
30. LR RRT projektas. *Būk saugus elektroninėje erdvėje*. Prieiga per internetą: https://www.esaugumas.lt/duk [žiūrėta: 2023 04 25]
31. LR VSD ir Antrasis operatyvių tarnybų departamentas prie KAM „Grėsmių nacionaliniam saugumui vertinimas“ 2023 m.
32. LRV *Nutarimas dėl Lietuvos Respublikos Kibernetinio saugumo įstatymo įgyvendinimo, 2018 m. rugpjūčio 13 d. Nr. 818 (Galiojanti suvestin4 redakcija nuo 2021-01-01.* Prieiga per internetą: 818 Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo (lrs.lt)
33. LSM.lv *Latvian government agrees cyber-security strategy until 2026*. Prieiga per internetą: Latvian government agrees cyber-security strategy until 2026 / Article (lsm.lv)
34. Mana.Latvija.lv. *Saugumas internete (Drošība internetā)*. Prieiga per internetą: Drošība internetā - Mana Latvija.lv
35. Mykolo Romerio universitetas. *Kibernetinio saugumo valdymas*. Prieiga per internetą: Kibernetinio saugumo vadyba | Studijos Lietuvoje | MRU (mruni.eu) [žiūrėta: 2023 04 06]
36. Moti Zwilling ir kt. „Cyber Security Awareness, Knowledge and Behavior: A Comparative Study“ 2022 m. Prieiga per internetą (PDF) Cyber Security Awareness, Knowledge and Behavior: A Comparative Study (researchgate.net)
37. National Cybersecurity Preparedness Consortium, NCPC (2023). *The Community Cyber Security Maturity Model*. Prieiga per internetą: NCPC | CCSMM (nationalcpc.org)
38. NCSI (2023). *National vybr security index*. Prieiga per internetą: NCSI :: Ranking (ega.ee)
39. Nic.lv. *Cybersecurity Basics*. Prieiga per internetą: Free online course “Cybersecurity Basics” (nic.lv)
40. NKSC ir kt. (2020). *Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas*. Prieiga per internetą: Kibernetinio_saugumo_vadovas_verslui_2020.pdf (nksc.lt)
41. NKSC prie KAM (2022). *Nacionalinės kibernetinio saugumo pratybos "Kibernetinis skydas 2022" ataskaita*. Prieiga per internetą: Aktuali informacija, reglamentavimas, statistika | NKSC

42. Nobles C. (2018). *Botching Human Factors in Cybersecurity in Business Organizations* Prieiga per internetą: (PDF) Botching Human Factors in Cybersecurity in Business Organizations (researchgate.net)
43. Pawlicka A. ir kt, (2021). A $10 million question and othercybersecurity-related ethical dilemmas amid the COVID-19 pandemic. *Business Horizons (2021) 64, 729-734.* Prieiga per internetą: A $10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic | Elsevier Enhanced Reader
44. Piest J. P. S. ir kt. (2023). *Digital Architectures Under Society 5.0: An Enterprise Architecture Perspective*. Prieiga per internetą: Digital Architectures Under Society 5.0: An Enterprise Architecture Perspective | Request PDF (researchgate.net)
45. Reegard K. ir kt. (2019). *The Concept of Cybersecurity Culture*. Prieiga per internetą (PDF) The Concept of Cybersecurity Culture (researchgate.net)
46. RISCS (2021). *Remote Working and Cyber Security*. Prieiga per internetą: (PDF) Remote Working and Cyber Security Literature Review (researchgate.net)
47. Riga technical university. *Cybersecurity Engineering.* Prieiga per internetą: Cybersecurity Engineering - RTU International Coorperation and Foreign Students Department [žiūrėta: 2023 04 06]
48. Robert S. Gutzwiller ir kt. „Panel: Research Sponsors for Cybersecurity Research and the Human Factor“ 2019 m. Prieiga per internetą Panel: Research Sponsors for Cybersecurity Research and the Human Factor (sagepub.com)
49. Saugesnio interneto projektas. *Draugiškas internetas.* Prieiga per internetą: Apie programą - Draugiškas internetas (draugiskasinternetas.lt) [žiūrėta: 2023 04 25]
50. Skaitmeninė ekonomika ir visuomenė Lietuvoje (2022 m. leidimas) [žiūrėta 2023-04-03]. Prieiga per internetą https://osp.stat.gov.lt/skaitmenine-ekonomika-ir-visuomene-lietuvoje-2022/skaitmenine-visuomene-ir-verslas/gyvenimas-internete
51. Skaržauskienė A. ir kt. (2020). *The Digital Media in Lithuania: Combating Disinformation and Fake News*. Prieiga per internetą: (PDF) The Digital Media in Lithuania: Combating Disinformation and Fake News (researchgate.net)
52. Sosafe (2022). *Human Risk Review 2022*. Prieiga per internetą Human Risk Review 2022 | SoSafe (sosafe-awareness.com)

53. Šarpienė J. ir kt. (2019). *Skaitmeninių įgūdžių viešajame sektoriuje esamos situacijos analizė*. Prieiga per internetą: skaitmeniniu-igudziu-viesajame-sektoriuje-esamos-situacijos-analize.pdf (kurklt.lt)
54. Tallinn University of Technology. *MSC in Cybersecurity*. Prieiga per internetą: Cybersecurity (MSc) (taltech.ee) [žiūrėta: 2023 04 06]
55. Tallinn University of Technology. *Cyberus Erasmus Mundus Master in Cybersecurity*. Prieiga per internet: NEW International Master in Cybersecurity: CYBERUS (linkedin.com)
56. The NATO Cooperative Cyber Defence Centre of Excellence. *Cyber Defence Awareness*. Prieigaper internetą: CCDCOE
57. Valstybės kontrolė (2022). *Kibernetinio saugumo užtikrinimas*. Prieiga per internetą: Produktas | Lietuvos Respublikos valstybės kontrolė (valstybeskontrole.lt)
58. Valstybės policija (Valsts policija). *Valstybės policijos superherojai*. Prieiga per internetą: Valstybės policijos superherojai | Valstybės policija (vp.gov.lv)
59. Vilniaus Gedimino technikos universitetas. *Informacijos ir Informacinių technologijų sauga*. Prieiga per internetą: Prioritetinės mokslinių tyrimų kryptys ir tematikos | VILNIUS TECH [žiūrėta: 2023 04 06]
60. Vilniaus universitetas. *Kompiuterinis modeliavimas*. Prieiga per internetą: Kompiuterinis modeliavimas (vu.lt) [žiūrėta: 2023 04 06]
61. Vidzeme University of Applied Sciences. *Cybersecurity Engineering*. Prieiga per internetą: Cybersecurity Engineering | Vidzeme University (va.lv) [žiūrėta 2023 04 06]
62. Zemgale region human resource and competences development centre. *Cybersecurity, computer systems and software*. Prieiga per internetą: Zemgale Region Human Resource and Competences Development Centre (zrkac.lv)

Šakėnienė I. (2023). *Organizacijų vaidmuo užtikrinant kibernetinį saugumą: individo ir institucijos sąveika*. Vilnius: Mykolo Romerio Universitetas

ANOTACIJA

Magistro baigiamajame darbe išanalizuota esamą kibernetinio saugumo situaciją viešajame sektoriuje bei įvertinta organizacijos ir individo sąveiką, užtikrinant kibernetinį saugumą. Pirmame skyriuje analizuojami kibernetinės saugumo sampratos ir kibernetinės kultūros organizacijoje teoriniai aspektai ir problematika. Apibrėžiami kibernetinio saugumo iššūkiai ir jų poveikis užtikrinant kibernetinį saugumą viešajame sektoriuje. Pateikiami organizacijos kibernetinio saugumo kultūros vystymo aspektai. Antrame skyriuje pateikiama kibernetinio saugumo raiška individo lygmenyje aptariant kibernetinį saugumą viešajame sektoriuje. Aprašomi kibernetinio saugumo viešajame sektoriuje užtikrinimo būdai ir šalių praktika bei aptariama Lietuvos kibernetinio saugumo padėtis viešajame sektoriuje. Trečiame skyriuje pateikiama tyrimo metodologija. Kombinuotu tyrimu analizuojami anketinės apklausos viešojo sektoriaus ir KS ekspertinis požiūris į kibernetinį saugumą viešajame sektoriuje ir gerinimo galimybes. Ketvirtame skyriuje analizuojami tyrimo metu surinkti duomenys siekiant tobulinti ir stiprinti kibernetinį atsparumą organizacijoje stiprinat tarpusavio bendradarbiavimą skatinant kibernetinio saugumo kultūrą. Darbo pabaigoje pateikiamos tyrimo rezultatus apibendrinančios išvados ir parengtos Gairės „Kibernetinės kultūros viešajame sektoriuje tobulinimas“.

Pagrindiniai žodžiai: kibernetinis saugumas viešajame sektoriuje, kibernetinis saugumas, kibernetinio saugumo kultūra organizacijoje.

Šakėnienė I. (2023). *The Role of Organisations in Cybersecurity Governance: the Interaction on Individual and Institution Level*. Vilnius: Mykolas Romeris University

ANNOTATION

The Master thesis analysed the current cybersecurity situation in the public sector and assesses the interaction between the organisation and the individual in ensuring cybersecurity. The first chapter analyses the theoretical aspects and issues related to the concept of cyber security and cyber culture in an organisation. It outlines the challenges and implications of cyber security in the public sector. Aspects of developing an organisational cyber security culture are presented. The second chapter presents the expression of cyber security at the individual level in the context of cyber security in the public sector. It describes the methods and practices of cybersecurity in the public sector and discusses the state of cybersecurity in the public sector in Lithuania. Chapter 3 presents the research methodology. The combined study analyses the public sector and CS expert views on cybersecurity in the public sector and the opportunities for improvement through a questionnaire survey. Chapter 4 analyses the findings of the study with a view to improving and strengthening cyber resilience in the organisation by enhancing mutual cooperation in promoting a culture of cyber security. The thesis concludes with a summary of the findings of the study and develops a set of Guidelines for "Improving Cyber Culture in the Public Sector".

Key words: cybersecurity in the public sector, cybersecurity, cybersecurity culture in the organisations.

Šakėnienė I. (2023). *Organizacijų vaidmuo užtikrinant kibernetinį saugumą: individo ir institucijos sąveika*. Vilnius: Mykolo Romerio Universitetas

SANTRAUKA

Magistro baigiamajame darbe nagrinėjama tema aptariant kibernetinį saugumą viešojo sektoriaus organizacijose. Kibernetinis saugumas viešojo sektoriaus organizacijose vis dar sukelia nemenkus iššūkius. Šio darbo tikslas buvo išanalizuoti esamą kibernetinio saugumo situaciją viešajame sektoriuje bei įvertinti organizacijos ir individo sąveiką, užtikrinant kibernetinį saugumą. Darbe buvo keliamas mokslinės problemos klausimas – *kaip organizacija įgalina kibernetinio saugumo valdymo modelius, strategijas, taiko užkardymo instrumentus, įgalinančius užtikrinti kibernetinį saugumą?* Darbo uždaviniai: Pristatyti kibernetinio saugumo organizacijose teorinius aspektus, aptariant kibernetinio saugumo valdymo modelius bei strategijas; Atskleisti, Baltijos šalių, kibernetinio saugumo organizacijose vystymo prioritetus nacionaliniuose dokumentuose; Nustatyti veiksnius, turinčius įtakos organizacijos gebėjimui užkirsti kelią kibernetinio saugumo incidentams; Pagrįsti organizacijos ir individo sąveiką viešajame sektoriuje, užtikrinant kibernetinį saugumą, parengiant Gaires „Kibernetinės kultūros viešajame sektoriuje tobulinimas“. Darbo metodai: mokslinės literatūros analizė, juridinių ir strateginių dokumentų analizė, antrinių statistinių duomenų analizė, darbuotojų anketinė apklausa ir ekspertinis interviu.

Darbe buvo siekiama patvirtinti arba paneigti ginamuosius teiginius: Kibernetinio saugumo kultūros neišmanymas organizacijoje kelia potencialią grėsmę organizacijai; Nepakankamas individų bendradarbiavimas, užtikrinant kibernetinį saugumą organizacijoje yra kliūtis siekiant aukšto kibernetinio atsparumo lygio organizacijoje. Atlikus kombinuotą tyrimą abu šie teiginiai buvo patvirtinti. Šiuo metu viešajame sektoriuje stebimas darbuotojų vangumas kibernetinio saugumo srityje. Darbuotojai nenoriai įsitraukia į kibernetinio saugumo mokymus bei veiklas. Todėl daugelis organizacijų darbuotojų gali turėti žinių spragų apie aktualias kibernetines grėsmes arba klaidingai suvokti kibernetinio saugumo aspektus ir dėl to organizacija gali būti pažeidžiama kibernetinių grėsmių atitinkamai organizacijoje išlaikomas žemas kibernetinio saugumo lygis.

Magistro baigiamojo darbo pabaigoje pateikiamos parengtos gairės - Kibernetinės kultūros viešajame sektoriuje tobulinimas, atitinkančios darbe nustatytai problematikai bei galimiems sprendimo būdams.

Šakėnienė I. (2023). *The Role of Organisations in Cybersecurity Governance: the Interaction on Individual and Institution Level*. Vilnius: Mykolas Romeris University

SUMMARY

The Master thesis addresses the topic of cyber security in public sector organisations. Cyber security in public sector organisation still poses significant challenges. The aim of this thesis was to analyse the current cybersecurity situation in the public sector and to assess the interaction between the organisation and the individual in ensuring cybersecurity. The research question was: how does an organisation enable cybersecurity management models, strategies, and prevention tools to ensure cybersecurity? The theoretical aspects of cybersecurity in organisations, discussing cybersecurity management models and strategies; Identify the priorities for the development of cybersecurity in the Baltic States in national documents; Identify the factors affecting the ability of an organisation to prevent cybersecurity incidents; Justify the interaction between the organisation and the individual in the public sector in the context of cybersecurity, by developing the Guidelines for the "Improving the cyber culture in the public sector". Methods: analysis of scientific literature, analysis of legal and strategic documents, analysis of secondary statistical data, questionnaire survey of employees and expert interviews.

The thesis aimed to confirm or deny the following statements: ignorance of cyber security culture in the organisation is a potential threat to the organisation; insufficient cooperation between individuals in ensuring cyber security in the organisation is an obstacle to achieving a high level of cyber resilience in the organisation. The combined study confirmed both of these statements. At present, there is a lack of employee engagement in cyber security in the public sector. Employees are reluctant to engage in cybersecurity training and activities. As a result, many employees in organisations may have knowledge gaps about current cyber threats or misconceptions about cyber security, which may leave the organisation vulnerable to cyber threats and consequently maintain a low level of cyber security in the organisation.

The Master's thesis concludes with a set of guidelines - Improving Cyber Culture in the Public Sector - which are in line with the issues identified in the thesis and possible solutions.

SANTRUMPOS

3D CCSMM – 3D bendruomenės kibernetinio saugumo modelis (angl. The 3D Community Cybersecurity Model) CCSMM kubas
CCSMM – Bendruomenės kibernetinio saugumo brandos modelis (angl. Community Cyber Security Maturity Model)
CIAS – angl. The Center for Infrastructure Assurance and Security (Infrastruktūros užtikrinimo ir saugumo centras)
CSC – Kibernetinio saugumo kultūra (angl. Cybersecurity Culture)
ENISA – Europos Sąjungos tinklų ir informacijos apsaugos agentūra
ES – Europos Sąjunga
IRT – informacinės ir ryšio technologijos
IT – informacinės technologijos
ITU - International Telecommunication Union
YSII – Ypatingos svarbos informacinės infrastruktūros
JK – Jungtinė Karalystė
KS – kibernetinis saugumas
NKSC – Nacionalinis kibernetinio saugumo centras

PRIEDAI

1 priedas

Klausimynas parengtas pagal ENISA (Kibernetinio saugumo kultūra organizacijose, 2017 m.). Klausimynas Nr.1 (1 priedas) skirtas viešojo sektoriaus darbuotojams

Informuotumo kibernetinio saugumo klausimu lygio nustatymo tyrimas
(darbuotojo anketa)

1. Ar kada nors girdėjote terminą „kibernetinis saugumas“ ar „kibernetinio saugumo kultūra“
   - Taip
   - Ne

2. Kaip dažnai girdite, kad Jūsų darbovietėje būtų kalbama apie kibernetinį saugumą?
   - Dažnai
   - Kartais
   - Retai
   - Niekada

3. Ar Jūsų darbovietėje kalbama apie kibernetinio saugumo skatinimą?
   - Taip
   - Ne

4. Ar Jūsų darbovietėje yra vertinamas kibernetinio saugumo lygis?
   - Taip
   - Ne
   - Nežinau

5. Ar Jūsų darbovietėje taikoma kibernetinio saugumo politika ar strategija?
   - Taip
   - Ne
   - Nežinau

6. Ar žinote kam privalote pranešti apie kibernetinio saugumo incidentus?
   - Taip
   - Ne

7. Ar Jūsų darbovietėje rengiami kibernetinio saugumo mokymai darbuotojams?
   - Taip
   - Ne
   - Nežinau

8. Ar dalyvaujate kibernetinio saugumo mokymuose?
   - Taip

- Ne

9. Ar dalyvautumėte kibernetinio saugumo mokymuose?
   - Taip
   - Ne

10. Kaip manote, ar kibernetinis saugumas laikomas pirmiausia tos srities žmonių atsakomybe darbovietėje, ar prie kibernetinio saugumo stiprinimo turi prisidėti visi?
   - Kibernetinio saugumo srities specialistų
   - Kolektyvinis indėlis

11. Ar žinote kokios priemonės naudojamos „populiarinti“ kibernetinio saugumo kultūrą Jūsų darbovietėje?
   - Taip
   - Ne

12. Kokios tai priemonės (PAŽYMĖTI VISUS TINKANČIUS)
   - Plakatai
   - Istorijos
   - Patarimų lapai
   - Vaizdo įrašai
   - Žaidimai
   - Išorės konsultantų pristatymai
   - Mokymas
   - Kita

13. Darbovietės pavadinimas (neprivaloma)
   - ……

2 priedas

Interviu klausimai

Laba diena,

Esu Mykolo Romerio universiteto, Kibernetinio saugumo valdymo magistro studijų studentė – Ivona Šakėnienė. Mano magistrinio darbo tema – „Organizacijų vaidmuo užtikrinant kibernetinį saugumą: individo ir institucijos sąveika“ , darbe atlieku tyrimą , kuris leis nustatyti esamą kibernetinio saugumo situaciją viešajame sektoriuje bei įvertinti organizacijos ir individo sąveiką, užtikrinant kibernetinį saugumą; identifikuoti esamus trūkumus ir juos pašalinti parengiant Gaires „Kibernetinės kultūros viešajame sektoriuje tobulinimas“. Jūsų ekspertinė nuomonė ir įžvalgos labai svarbios atliekant minimą tyrimą. Anonimiškumas garantuojamas.

1. Koks šiandien dienai yra viešojo sektoriaus darbuotojų informuotumas apie kibernetinį saugumą?
2. Kaip pasikeitė viešojo sektoriaus suvokimas apie kibernetinį saugumą, Rusijos išpuolio prieš Ukrainą kontekste?
3. Kaip viešajame sektoriuje vertinamas kibernetinio saugumo lygis ir kaip taikomos kibernetinio saugumo strategijos ar politika?
4. Kodėl saugumui užtikrinti svarbu sutelkti dėmesį į žmones (darbuotojus)?
5. Kokie galėtų būti svarbiausi aspektai siekiant subalansuoto kibernetinio saugumo viešajame sektoriuje?
6. Jūsų nuomone, už kibernetinį saugumą atsakinga vyriausybė, organizacijos ar kiekvienas asmeniškai? Kieno atsakomybė yra kibernetinis saugumas?