MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

INGA ŠIMONIENĖ

KIBERNETINIO SAUGUMO KULTŪROS VERTINIMAS LIETUVOS LIGONINĖSE

Magistro baigiamasis darbas

Vadovas
prof. dr. M. Laurinaitis

Vilnius, 2024

MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

INGA ŠIMONIENĖ

KIBERNETINIO SAUGUMO KULTŪROS VERTINIMAS LIETUVOS LIGONINĖSE

Kibernetinio saugumo valdymo magistro baigiamasis darbas

Studijų programa 6211LX066

Vadovas
prof. dr. M. Laurinaitis
2024-05-02

Atliko
KSVvmis22-1 gr. stud.
I. Šimonienė
2024-05-02

Vilnius, 2024

Turinys

LENTELĖS

PAVEIKSLAI

SANTRUMPOS

ENISA – Europos Sąjungos kibernetinio saugumo agentūra

COVID – koronaviruso infekcija

ES – Europos sąjunga

LR SAM – Lietuvos Respublikos Sveikatos apsaugos ministerija

BDAR – Bendrasis duomenų apsaugos reglamentas

TIS2 – Tinklų ir informacinių sistemų direktyva

NATO – Šiaurės Atlanto sutarties organizacija

APT – išplėstinė nuolatinė grėsmė

Ddos – paskirstyta paslaugos trikdymo ataka

MitM – „Man in the middle“ ataka

HIMSS – Sveikatos priežiūros informacijos ir valdymo sistemų draugija

IT – informacinės technologijos

IRT – informacinių ir ryšių technologijos

KVTC – Kertinis valstybės telekomunikacijų centras

NKSC – Nacionalinis kibernetinio saugumo centras

ĮVADAS

Temos aktualumas. Įvairios technologijos ir skaitmeninės inovacijos sėkmingai įsiveržė į sveikatos sektorių. Informacinės sistemos leidžia operatyviai keistis informacija bei sistemingai kaupti duomenis. E. sveikatos atsiradimas palengvino specialistų darbą, užtikrino patogesnį, greitesnį ir kokybiškesnį paslaugų gavimą pacientams. Sveikatos priežiūros įstaigoms informacijos saugumas visada buvo svarbus, bet didžiąją dalį duomenų suskaitmeninus ir perkėlus į elektroninę erdvę, sparčiai didėjant išmanių įrenginių naudojimui sektoriuje, informacijos saugumas peraugo į kibernetinį saugumą ir čia iškilo naujų iššūkių. Remiantis ENISA (2022) sveikatos priežiūros sektoriuje pagrindinės žiniatinklio programų atakos, įvairios klaidos ir įsibrovimai į sistemą sudarė 76 % pažeidimų, 39% vidinės grėsmės taip pat su COVID susijusi dezinformacija padidino atakas prieš sveikatos sektorių. Pirmojoje ataskaitoje skirtoje ES sveikatos sektoriui ENISA (2023) rašė, kad 2021 m. sausio mėn.- 2023 m. kovo mėn. laikotarpyje įvykusių kibernetinių incidentų net 53 % buvo nukreipti prieš ES sveikatos priežiūros teikėjus iš kurių 42 % prieš ligonines. *Kibernetinis saugumas sveikatos priežiūros srityje apima visus bendruosius veiksmus, taikomus tiek vartotojų, tiek darbo sektoriuose (tinklo saugumas, taikomųjų programų sauga, informacijos sauga, veikimo saugumas, atkūrimas ir veiklos tęstinumas, galutinio vartotojo mokymas), pritaikytus ir specializuotus sveikatos priežiūros sektoriui. Todėl teisingas ir veiksmingas kibernetinio saugumo įgyvendinimas yra labai svarbus, nes sveikatos priežiūros sistemų kritiškumas yra aukščiausio lygio, o jos veikla susijusi su žmonių sveikata.* (Giansanti, 2021)

Coventry ir Branley (2018) išskiria dvi pagrindines priežastis, kodėl sveikatos priežiūra yra patrauklus taikinys kibernetiniams nusikaltimams: vertingi duomenys, o jos gynyba yra silpna. Autoriai teigia, kad pažeidimai gali sumažinti pacientų pasitikėjimą, sugadinti sveikatos priežiūros sistemas bei kelti grėsmę žmonių gyvybei, todėl kibernetinis saugumas turi tapti būtina pacientų saugos dalimi.

Temos ištirtumas ir naujumas. ENISA (2017) skelbė, kad nepaisant padidėjusio įmonių ir asmenų investavimo į technologijų ir programinės įrangos naujoves, kuriomis siekiama sumažinti kibernetinių incidentų skaičių, duomenų saugumo pažeidimų skaičius toliau auga. Žmonės tebėra silpniausia saugumo grandinės grandis ir tik kibernetinio saugumo kultūros plėtojimas ir stiprinimas gali sumažinti žmogiškąjį faktorių. Kibernetinio saugumo tema pastarąjį dešimtmetį plačiai nagrinėjama, o COVID pandemija dar labiau išryškino šios temos svarbą, ypatingai sveikatos sektoriuje. 2022 metais buvo atliktas didelis tyrimas trijose skirtingose sveikatos priežiūros organizacijose, skirtingose šalyse: Graikija, Rumunija, Portugalija. Juo buvo siekiama užfiksuoti

organizacijų kibernetinio saugumo sąmoningumo lygį. (Gioulekas, Stamatiadis, Tzikas, Gounaris, Georgiadou, Michalistsi-Psarrou, Doukas, Kontoulis, Nikoloudakis, Marin, Cabecinha ir Ntanos, 2022) Lietuvoje kibernetinio saugumo kultūra, ypač sveikatos sektoriuje, nėra pakankamai išnagrinėta.

2022 metais vyko tarptautinės kibernetinio saugumo ir krizių valdymo pratybos „Cyber Europe 2022“. Jomis buvo siekama patikrinti, kaip reaguojama į išpuolius prieš ES sveikatos priežiūros infrastruktūrą. LR Sveikatos apsaugos ministerijos (2022) puslapyje buvo skelbta, kad aštuonios Lietuvos sveikatos priežiūros įstaigos dalyvavo pratybose. Remiantis higienos instituto statistikos duomenimis 2021 metais Lietuvoje veikė 235 asmens sveikatos priežiūros įstaigos, pavaldžios LR SAM ir savivaldybėms bei 15 privačių ligoninių ir 189 privačios pirminės sveikatos priežiūros įstaigos. Aišku, kad aktyvumas nėra pakankamas. Todėl atliktas tiriamasis darbas, siekiant įvertinti kibernetinio saugumo kultūrą Lietuvos ligoninėse, pavaldžiose LR SAM ir savivaldybėms. Tai leidžia išsikelti darbo problemą, kuri gali būti formuluojama tokiu klausimu:

Tyrimo problema: Kaip stiprinti kibernetinio saugumo kultūrą Lietuvos ligoninėse?

Tyrimo objektas – kibernetinio saugumo kultūra Lietuvos ligoninėse

Tyrimo tikslas – įvertinti kibernetinio saugumo kultūrą Lietuvos ligoninėse.

Tyrimo uždaviniai:

1. Išnagrinėti kibernetinio saugumo kultūros teorinius aspektus.
2. Apžvelgti pagrindines kibernetines grėsmes sveikatos sektoriuje.
3. Atlikti tyrimą, siekiant įvertinti Lietuvos ligoninių darbuotojų ir jų vadovų supratimą apie kibernetinio saugumo kultūrą.

Tyrimo metodai:

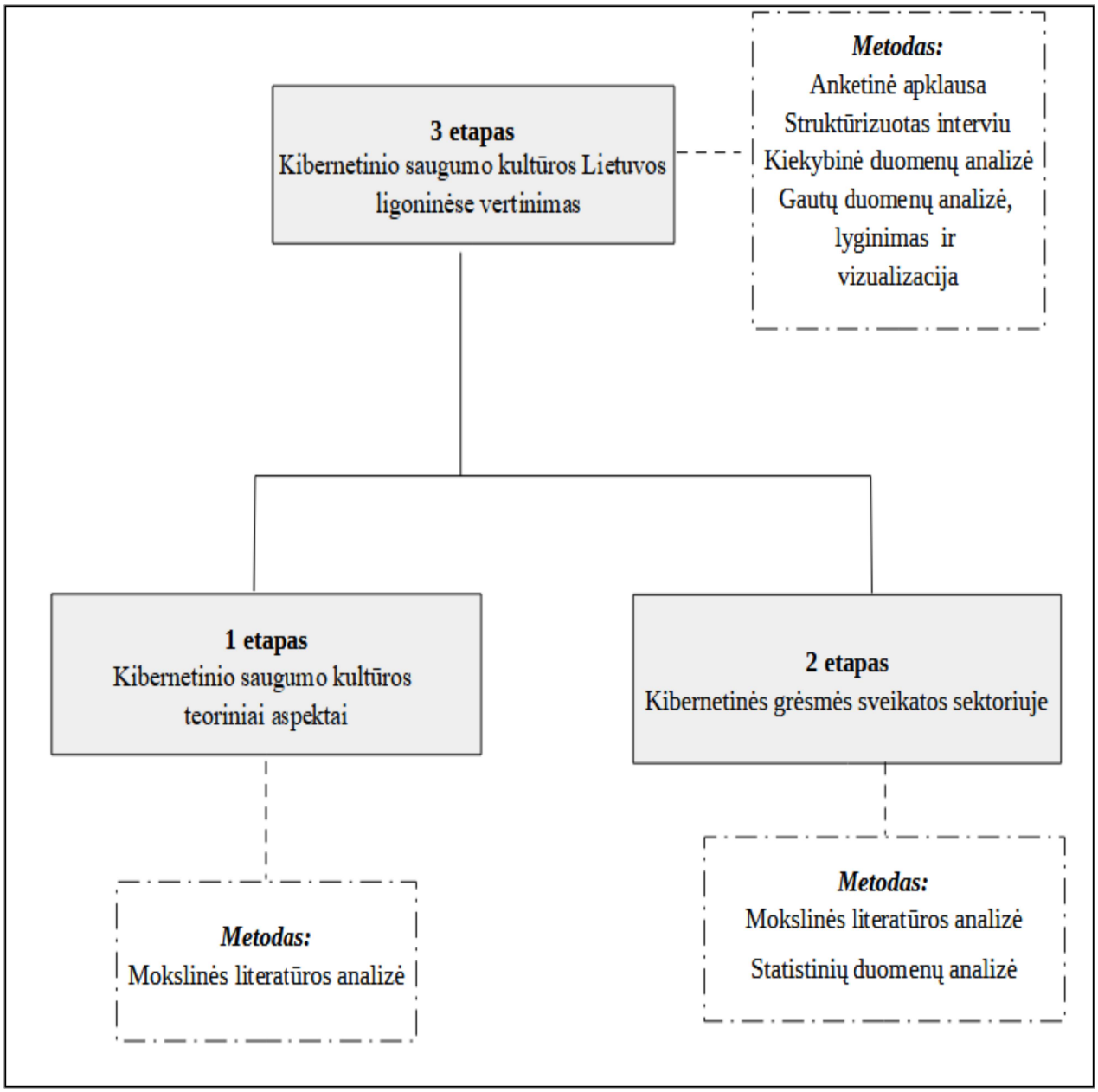
1. Mokslinės literatūros analizės metodas bus naudojamas atliekant literatūros analizę ir siekiant išnagrinėti kibernetinio saugumo kultūros teorinius aspektus bei apibūdinti pagrindines kibernetines grėsmes sveikatos sektoriuje.
2. Antrinių statistinių duomenų analizės metodas taikytas, apžvelgiant pagrindines kibernetines grėsmes sveikatos sektoriuje.
3. Duomenų vizualizacijos metodas naudojamas pateikiant schemas, lenteles.
4. Kokybinis tyrimas - pusiau struktūrizuotas interviu, siekiant surinkti informaciją iš ligoninių vadovų, kurie turėtų būti atsakingi už kibernetinio saugumo kultūros skatinimą ir plėtrą.
5. Kiekybinis tyrimas – apklausa internetu (CAWI). Šis metodas pasirinktas, siekiant įvertinti Lietuvos ligoninių darbuotojų supratimą apie kibernetinio saugumo kultūrą. Kadangi tai geografiškai plati vieta, apimanti visą Lietuvą, šis metodas buvo priimtiniausias.

Duomenų analizės metodai:

1. Kokybinė duomenų analizė
2. Kiekybinė duomenų analizė
3. Gautų duomenų analizė

Darbo struktūra. Darbas sudarytas iš 3 dalių. Pirmoje dalyje nagrinėjama kibernetinio saugumo kultūros samprata. Antrojoje dalyje apžvelgiamos kibernetinės grėsmės sveikatos priežiūros sektoriuje. Trečiojoje dalyje aprašomas mišrus tyrimas. Kiekybinio tyrimo tikslas išsiaiškinti, kaip Lietuvos ligoninių darbuotojai supranta kibernetinio saugumo kultūrą. Kokybinio tyrimo metu siekiama išsiaiškinti, kaip vadovai skatina kibernetinio saugumo kultūrą ligoninėse. Darbo struktūros loginė schema pavaizduota 1 paveiksle.

Praktinis taikomumas. Įvertinus esamą kibernetinio saugumo kultūros padėtį sveikatos priežiūros įstaigose galima pateikti išvadas ir pasiūlyti rekomendacijas Lietuvos ligoninių vadovams ir LR sveikatos apsaugos ministerijai, kaip skatinti kibernetinio saugumo kultūros plėtrą ir stiprinimą sveikatos sektoriuje.



1 pav. Darbo struktūros loginė schema

1. Kibernetinio saugumo kultūros teoriniai aspektai

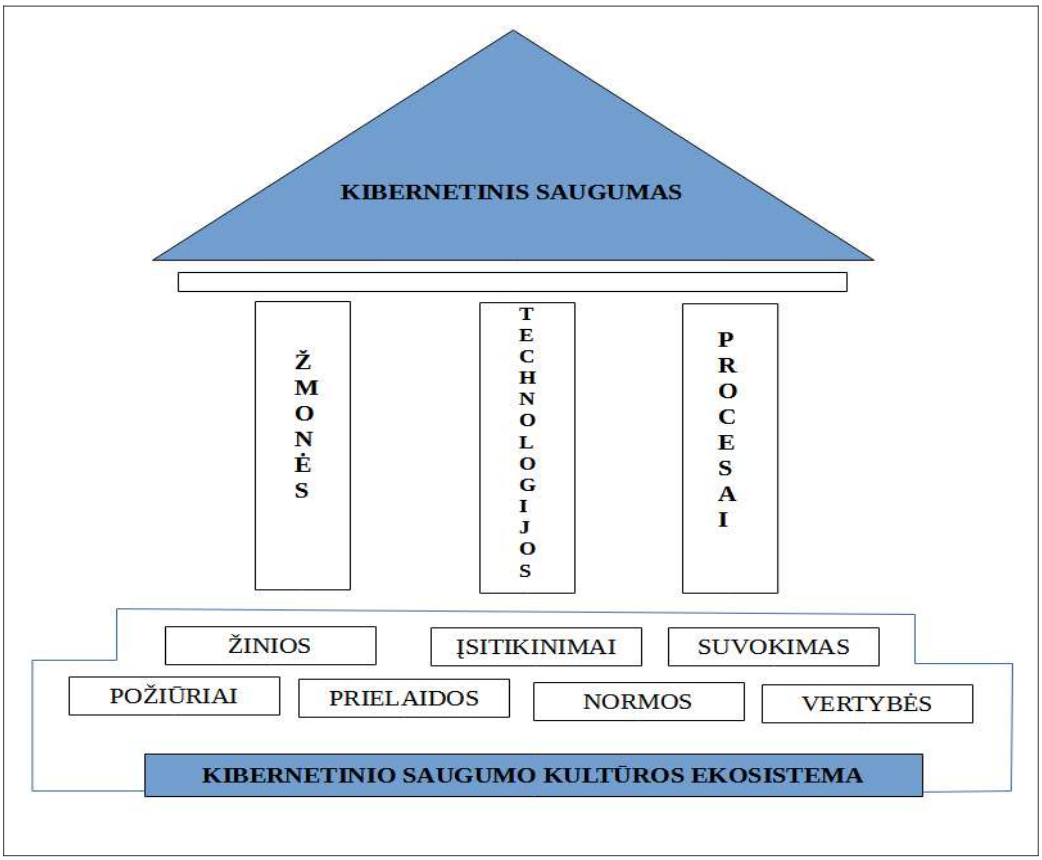
Šiais laikais vis dažniau pripažįstama, kad kibernetinio saugumo užtikrinimui vien technologinių priemonių nepakanka. Autoriai Alvarez-Dionisi ir Urrego-Baquero (2019) teigia, kad kibernetinio saugumo kultūra yra nuolat kintantis procesas, kuris reikalauja dėmesio, todėl kibernetinio saugumo kultūrą organizacija turi paversti nuolatine įmonės veikla. Kibernetinio saugumo kultūra tai ne tik fizinės kliūtys įėjimui į pastatą ar mažiausi teisių įgaliojimai, bet tai organizacijos žmonių mąstysena. (Frenken, 2020) Corradini (2020) savo knygoje rašė, kad kibernetinio saugumo kultūra kiekvienoje organizacijoje yra skirtinga ir unikali. Ji remiasi organizacijos skirtingomis savybėmis, technologijomis, procesais ir žmonių vertybėmis. Norint užtikrinti kibernetinio saugumo kultūros veiksmingumą, būtina skatinti žmones suprasti, kad saugumas nėra tik IT skyriaus problema, tai apima visus darbuotojus. Norėdami pasiekti teigiamų rezultatų, turime užtikrinti imlią ir sveiką aplinką, kurioje darbuotojai atlikdami savo užduotis elgiasi saugiai. Ir kaip teigia Frenken (2020), geriausia kibernetinio saugumo praktika prasideda nuo saugumo kultūros kūrimo.

Pagrindinis kibernetinio saugumo kultūros tikslas - padėti įgyvendinti ir plėtoti kibernetinio saugumo ekosistemą. (Alvarez-Dionisi ir Urrego-Baquero, 2019) Reikia sukurti organizacijos saugų požiūrį ir elgesį su informacinėmis sistemomis ir su jomis susijusiais procesais. Norint užtikrinti kibernetinio saugumo kultūros plėtrą organizacijoje, reikia suvokti, kad kibernetinio saugumo kultūra sudaryta iš įvairių skirtingų elementų, kurie plačiau nagrinėti sekančiame skyriuje.

1.1. Kibernetinio saugumo kultūros elementai

Kibernetinio saugumo kultūra sudaryta iš skirtingų elementų, kuriuos stiprinant, galima pasiekti stiprią kibernetinio saugumo kultūrą, taip sumažinant kibernetinių atakų sukeliamus nuostolius. ENISA (2017) kibernetinio saugumo kultūrą apibūdino kaip „žmonių žinias, įsitikinimus, suvokimą, požiūrį, prielaidas, normas ir vertybes, susijusias su kibernetiniu saugumu ir kaip jos pasireiškia žmonių elgesyje, naudojant informacines technologijas“.

Autoriai Alvarez-Dionisi ir Urrego-Baquero (2019) pristatė septynis blokus, suteikiančius tinkamą aplinką kibernetiniam saugumui palaikyti: žinių, įsitikinimų, suvokimo, požiūrių, prielaidų, normų ir vertybių. Šie septyni blokai sudaro integruotą požiūrį į kibernetinį saugumą, pabrėžiant ne tik techninius aspektus, bet ir žmonių elgesį, požiūrį ir vertybes. (2 pav.)



šaltinis: išversta pagal Alvarez-Dionisi ir Urrego-Baquero, 2019

2 pav. Kibernetinio saugumo kultūros ekosistema

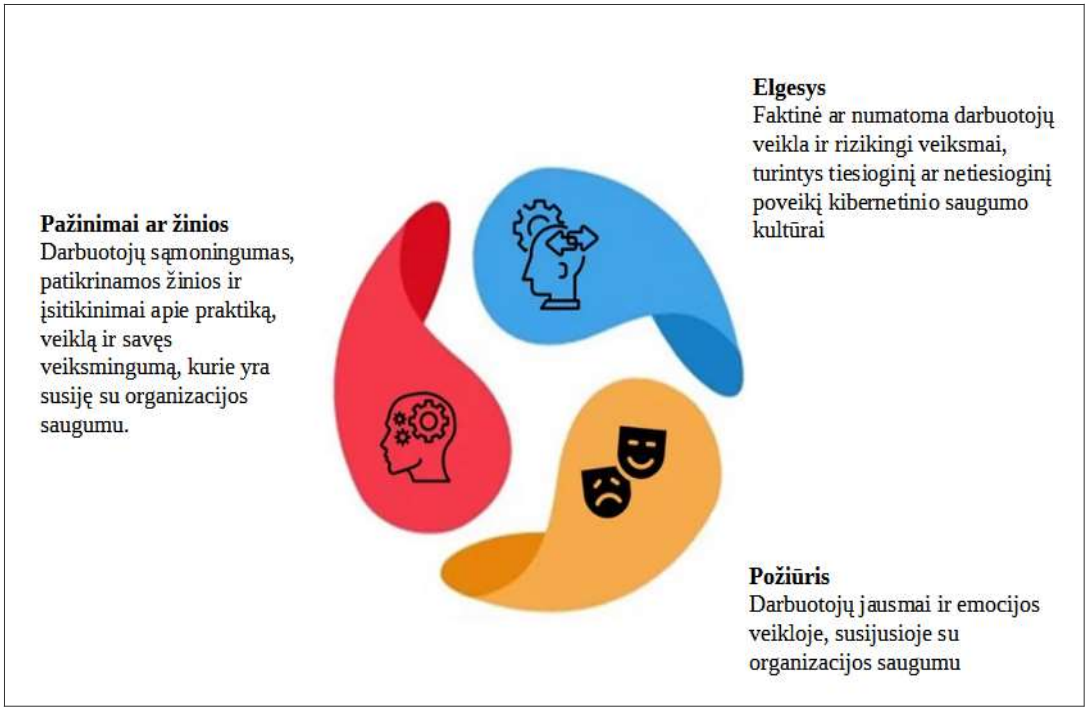
Parksas (2021) išskyrė septynis kibernetinio saugumo kultūros elementus, padedančius organizacijoms apsisaugoti nuo kibernetinių grėsmių, tai lyderystė, apimanti vyresniosios vadovybės elgesį ir finansines investicijas, daugialypės darbo grupės sukūrimas, skirtos rizikos ir galimybių nustatymui, saugumo spragų sumažinimui, saugumo priemonių parinkimui taip pat padedančios nustatyti kultūrines kliūtis, trukdančias saugiai mąstysenai ir geriausiai praktikai. Švietimas, kibernetinio saugumo procedūrų integravimas į darbuotojų kasdienes procedūras, darbo rutiną. Požiūriai ir veiksmai, kai darbuotojai jaučiasi gerai, prisidėdami prie organizacijos kibernetinio saugumo stiprinimo, o kibernetinis saugumas ne tik organizacijoje, bet ir už jos ribų, kai keičiamasi informacija tarp kolegų, suinteresuotų šalių, klientų ir tiekėjų, sudaro visą ekosistemą. Metrika, kaip dar vienas elementas, padeda stebėti mokymo efektyvumą ir bendrą vertę, galintis veiksmingai parodyti programos vertę vyresniajai vadovybei ir išlaikyti jų paramą.

Nurse (2023) pristatė penkis svarbiausius kibernetinio saugumo kultūros elementus: lyderystė, politika, sąmoningumas, mokymas, pokyčių valdymas. Uchendu, Nurse, Bada ir Furnell

(2021) analizuodami straipsnius kibernetinio saugumo kultūros tema išvardijo dažniausius veiksnius, laikomus svarbiais, kuriant ir palaikant kibernetinio saugumo kultūrą: aukščiausios vadovybės palaikymas, vadovavimas ir dalyvavimas buvo vienas svarbiausių elementų, kaip ir Willie (2023) nagrinėdamas organizacijos kultūros įtaką kibernetiniam saugumui teigė, kad vadovavimas yra pagrindas, formuojant kibernetinio saugumo kultūrą, taip pat mąstė ir autoriai Parksas (2021) ir Nurse (2023), kurie išskyrė vadovybės svarbą, nes be vadovybės palaikymo, jos rodomo pavyzdžio, kibernetinio saugumo kultūra nepasieks maksimalaus efektyvumo. Jei vadovybė nesupras kultūros svarbos, ji nebus suinteresuota finansiškai remti programas, skatinančias kibernetinio saugumo kultūros stiprinimą. Uchendu ir kt. (2021) pabrėžė, kad svarbu turėti aiškią politiką ir procedūras. Autoriai Parksas (2021), Nurse (2023), Willie (2023), Uchendu ir kt. (2021) sutinka, kad mokymai, žinios ir darbuotojų sąmoningumas yra kertiniai elementai, padėsiantys kibernetinio saugumo kultūros kūrimui.

Ashik (2023) rašė, kad kibernetinio saugumo kultūra susideda iš darbuotojų elgesio, požiūrio ir žinių susijungimo ir bandė kibernetinio saugumo kultūrą atvaizduoti matematiškai:

kibernetinio saugumo kultūra = požiūris*elgsena*pažinimas (3 pav.)



Šaltinis: išversta pagal Ashik (2023)

3 pav. Kibernetinio saugumo kultūra

Mokymai ir švietimas ne tik suteikia galimybę plėsti žinias kibernetinio saugumo klausimais, bet ir keičia žmonių mąstyseną, požiūrį ir elgesį. Aiškios politikos ir procedūros

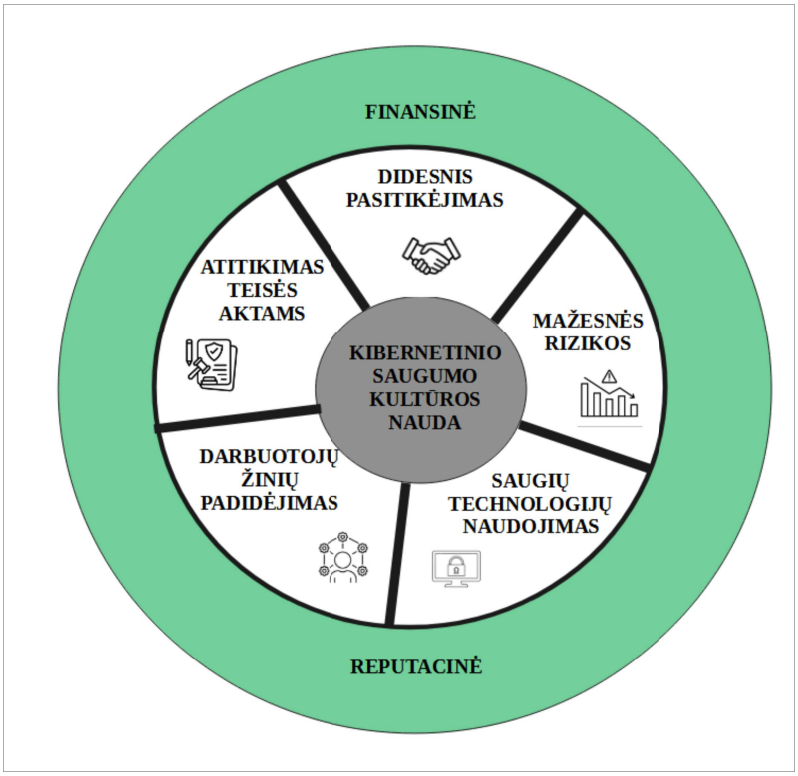
sustiprintų žinių įsisavinimą. Vadovai paskirstydami išteklius, nustatydami suprantamą politiką ir būdami pavyzdžiu, laikantis kibernetinio saugumo praktikų, parodytų aiškų įsipareigojimą kibernetiniam saugumui. Visi šie elementai padeda kurti stiprią kibernetinio saugumo kultūrą organizacijose.

1.2. Kibernetinio saugumo kultūros nauda organizacijai

Frenken (2020) teigia, kad stipri kibernetinio saugumo kultūra padeda apsaugoti svarbiausią įmonės turtą – jos duomenis, nes fizinis turtas gali būti pakeistas, o daugelį metų kaupti duomenų ištekliai, sunkiai pakeičiami. Be duomenų saugos svarbumo, organizacijoms ne ką mažiau aktualu apsaugoti ir teikiamas paslaugas, jų prieinamumą. Kibernetinio saugumo kultūra gali apsaugoti ne tik nuo didelės finansinės, bet ir reputacinės žalos, nes išlaikyti gerą įmonės reputaciją yra taip pat svarbu kaip ir apsaugoti savo duomenis. „Veiksminga kibernetinio saugumo kultūra gali būti diferencijuojantis veiksnys, pabrėžiantis organizacijos įsipareigojimą saugoti savo turtą ir išlaikyti ypatingos svarbos informacijos konfidencialumą, vientisumą ir prieinamumą.“ Nas (2023) Įgyvendindami stiprią kibernetinio saugumo kultūrą organizacijos gali parodyti savo partneriams ir klientams, kad į duomenų saugumą žiūrima rimtai, taip išsaugodami klientų pasitikėjimą. Nas (2023) straipsnyje „Kokia yra veiksmingos saugumo kultūros nauda?“ įvardijo penkias pagrindines naudas: didesnis saugumo suvokimas, patobulintas reagavimas į incidentus, geresnis rizikos valdymas, klientų pasitikėjimas ir reputacija, reguliavimo reikalavimų laikymasis. Autorius teigė, kad vienas iš pagrindinių privalumų yra padidėjęs drabuotojų informuotumas apie saugumą. Darbuotojai būna sąmoningesni ir aktyviau prisiima atsakomybę už saugų elgesį internete yra labiau linkę aktyviau imtis atsargumo priemonių, sumažindami sėkmingų atakų riziką. Įsišaknijusi kibernetinio saugumo kultūra gali padėti skatinti atvirą darbuotojų bendravimą ir skatina pranešti apie įtartiną veiklą, galimus pažeidimus ar saugumo incidentus. Kibernetinio saugumo kultūra skatina atskaitomybės kultūrą, o tai gali padidinti našumą ir efektyvumą. Efektyvus rizikos valdymas sumažina incidentų skaičių ir tai reiškia, kad sumažėja rimtų teisinių ir finansinių pasekmių, organizacija sutaupo laiko ir pinigų. Galima išskirti šias pagrindines naudas organizacijai (4 pav.):

- **Mažesnės rizikos**, tai kai kibernetinio saugumo kultūra padeda organizacijoms išvengti kibernetinių atakų, susidurus su jomis greičiau jas identifikuoti, duoti atsaką ir greičiau atsistatyti po kibernetinio incidento.

- **Didesnis pasitikėjimas** organizacija - verslo partneriai, klientai labiau linkę pasitikėti organizacija, kuri rūpinasi kibernetiniu saugumu.
- **Atitikimas teisės aktams**, kai organizacijoje, kurioje kibernetinio saugumo kultūra yra svarbi, laikosi teisės aktų ir reglamentų reikalavimų, taip išvengdami baudų ir teisinių problemų.
- **Darbuotojų žinių ir įgūdžių padidėjimas**, nes organizacijos vykdydamos nuolatinius saugumo mokymus, skatina darbuotojų suvokimą apie kibernetinio saugumo grėsmes, taip keldami darbuotojų kvalifikaciją ir formuodami naujus įgūdžius.
- **Saugių technologijų naudojimas** pasireiškia tada, kai organizacija, kurioje kibernetinio saugumo kultūra yra puikiai išvystyta, investuoja į saugias ir pažangias informacines technologijas.



4 pav. Kibernetinio saugumo kultūros nauda organizacijai

Įgyvendinusios kibernetinio saugumo kultūrą organizacijos apsisaugo ne tik nuo finansinių nuostolių ir išsaugo reputaciją, bet ir padidina saugumą bei gebėjimą atitikti teisės aktus ir apsaugoti savo duomenis nuo neteisėtos prieigos. Užtikrinamas organizacijos veikimo ilgaamžiškumas ir jos veiklos tęstinumas. Norėdami gauti naudos iš kibernetinio saugumo kultūros plėtros, turime užtikrinti, kad stiprios kibernetinio saugumo kultūros bruožai atsispindėtų ir organizacijos procesuose. Kokie tie bruožai, plačiau aptarta kitame skyriuje.

1.3. Stiprios kibernetinio saugumo kultūros bruožai

Kibernetinio saugumo kultūros ekspertas Everard (2023) teigė, kad pagrindas efektyvios kibernetinio saugumo kultūros yra pripažinimas, kad saugią organizaciją daro žmonės, o ne technologijos. Reikia puoselėti aplinką, kurioje darbuotojai žinotų ir sugebėtų saugotis nuo kibernetinių grėsmių. ENISA (2017) pateikė gerosios praktikos pavyzdžius, kai kibernetinio saugumo klausimai tampa nuolatiniais valdybos posėdžių darbotvarkės klausimais, kai rengiamos ataskaitos apie kibernetinio saugumo kultūros būklę organizacijoje bei priemones ir išteklius skirtus kultūros palaikymui ir formavimui. Vadovybė yra dalis kibernetinio saugumo kultūros, ji dalyvauja mokymuose, laikosi bendrų saugumo taisyklių. Visi organizacijos darbuotojai įsitraukę į kibernetinio saugumo kultūros įgyvendinimą, noriai dalyvauja mokymuose, nebijo išsakyti, kokie kibernetinio saugumo sprendimai trukdo jų darbui ir nebijo pranešti, kas nesilaiko saugumo procedūrų. Visa tai sukuria stiprią kibernetinio saugumo kultūrą.

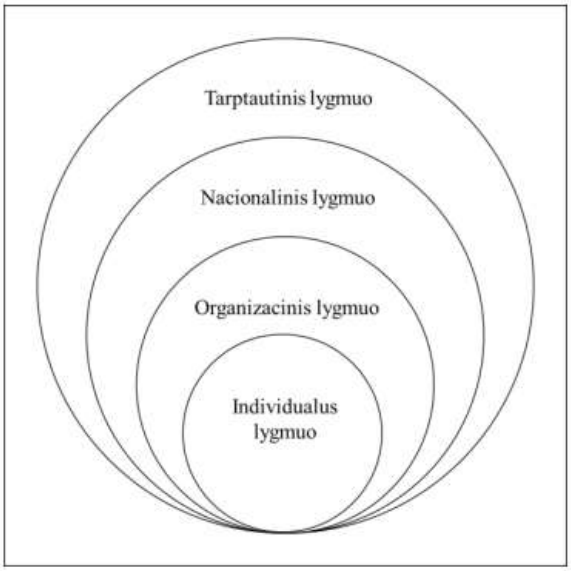
Wilie (2023) teigė, kad kai kibernetinis saugumas yra giliai įsišaknijęs organizacijoje, darbuotojai supranta, kad saugumo laikymasis nėra privalomas, bet būtinas, norint apsaugoti organizacijos neskelbtiną informaciją. Galima išskirti šiuos pagrindinius bruožus, būdingus stipriai kibernetinio saugumo kultūrai:

- **Vadovybės įsitraukimas**, kai vadovai investuoja į kibernetinio saugumo kultūros stiprinimą, aktyviai skatina jos plėtrą, rodo teigiamą pavyzdį darbuotojams kibernetinio saugumo klausimais.
- **Nuolatinis mokymasis**, pratybos ar seminarai, padeda darbuotojams gilinti ir tobulinti savo saugumo žinias. Formuoja naujus įgūdžius.
- **Tarpusavio bendradarbiavimas** kai darbuotojai, skyriai nebijo dalytis naujausia informacija, žiniomis ir praktikomis, užtikrinant saugumo reikalavimus. Tai padeda efektyviau atpažinti, pranešti ir reaguoti į incidentus.
- **Nuolatinė kibernetinio saugumo kultūros būklės analizė** pasireiškia tada, kai reguliariai vykdoma kultūros analizė, kurios proceso metu įvertinamas organizacijos gebėjimas užtikrinti duomenų, informacijos ir sistemų saugumą. Reguliari analizė padeda organizacijoms prisitaikyti prie nuolatos kintančių grėsmių.

Stipriai kibernetinio saugumo kultūrai reikia aktyvaus visos organizacijos įsitraukimo ir noro prisitaikyti prie besikeičiančio grėsmių kraštovaizdžio. Tai nuolatinis įsipareigojimas, o ne vienkartinės pastangos. Stipri kibernetinio saugumo kultūra organizacijoje padeda užtikrinti, kad kibernetinės grėsmės būtų nuolat atpažįstamos ir mažinamos, o organizacijos duomenys ir verslo tęstinumas išliktų apsaugoti.

1.4. Kibernetinio saugumo kultūros lygmenys ir jų įtaka

Kibernetinė saugumo kultūra yra daugialypė ir apimanti ne tik individualius įgūdžius ir žinias, bet ir tarptautinius standartus, bendradarbiavimo iniciatyvas ar bendrus tinklo saugos susitarimus. Da Veiga (2016) į kibernetinio saugumo kultūrą pažvelgė keturiais lygiais, pradedant nuo tarptautinės kibernetinio saugumo kultūros ir baigiant individualiu lygmeniu. (4 pav)



Šaltinis: išversta pagal Da Veiga (2016)

5 pav. Kibernetinio saugumo kultūros lygmenys

Ne išimtis ir sveikatos sektorius, kur tarptautinės kibernetinio saugumo kultūros įtaka yra didelė. Europos parlamentas ir taryba (2016) išleido reglamentą, dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. Norint tinkamai taikyti Bendrąjį duomenų apsaugos reglamentą, Lietuvos seimas patvirtino naują Asmens duomenų teisinės apsaugos įstatymo redakciją, kadangi sveikatos priežiūros sektorius tvarko daug ir labai jautrių duomenų privalėjo įgyvendinti BDAR ir Asmens duomenų teisinės apsaugos įstatymo reikalavimus, paskyrė Duomenų apsaugos pareigūnus, nustatė asmens duomenų tvarkymo tikslus, teisinį jų tvarkymo pagrindą ir kitus šių dokumentų reikalavimus. Su šių dokumentų reikalavimais turėjo keistis ir darbuotojų elgesys, organizacijų darbo tvarka. ES (2022) išleido teisinį dokumentą, TIS2 direktyvą, kurios nuostatose sveikatos sektorius priskiriamas esminiams subjektams, o medicinos prietaisų gamyba – svarbiems. Direktyvos nuostatos turi būti perkeltos į nacionalinius teisės aktus. Dokumento reikalavimai yra imtis tinkamų priemonių kibernetinio saugumo rizikų valdymui ir pareigą pranešti atsakingoms institucijoms apie incidentus.

Tarptautinė kibernetinio saugumo kultūra reikalauja bendradarbiavimo tarp valstybių, siekiant sudaryti bendrą supratimą apie kibernetinio saugumo iššūkius ir bendradarbiavimą, sprendžiant tarptautines grėsmes. Paziuk ir Mitsik (2019) analizuodami pasaulinės kibernetinio saugumo kultūros raidos tendencijas tarptautiniame diskurse teigė, kad norint kurti tarptautinę kibernetinio saugumo kultūrą, reikia sukurti tarptautinį teisinį pagrindą. Tarptautiniai standartai tampa orientyrais kibernetinio saugumo srityje. Šiaurės Atlanto sutarties organizacija (NATO) ir Europos Sąjunga (ES) yra svarbios tarptautinės organizacijos, kurioms priklauso Lietuva, ir šių organizacijų priimtos procedūros, strategijos ar politikos daro tiesioginę įtaką kibernetinio saugumo įgyvendinimui Lietuvoje. Valstybės narės keičiasi informacija apie kibernetines grėsmes, geriausias praktikas ir bendradarbiauja kovojant su kibernetinėmis grėsmėmis. Tarptautinė kibernetinio saugumo kultūra persipina su nacionaline ir toliau yra plėtojama ir skatinama per nacionalinius įstatymus ir nacionalines kibernetinio saugumo strategijas. Nacionalinės kibernetinio saugumo strategijos nustato valstybės prioritetus, tikslus ir politiką kibernetinio saugumo srityje.

LR Sveikatos ministras 2021 metais priėmė įsakymą „Dėl sveikatos priežiūros įstaigos informacinės sistemos pavyzdinių saugaus elektroninės informacijos tvarkymo taisyklių, sveikatos priežiūros įstaigos informacinės sistemos pavyzdinių naudotojų administravimo taisyklių ir sveikatos priežiūros įstaigos informacinės sistemos pavyzdinio veiklos tęstinumo valdymo plano patvirtinimo“, kuriame sveikatos priežiūros įstaigoms rekomenduoja juo vadovautis. Dokumento taisyklių laikymasis padeda užtikrinti informacijos saugumą, veiklos tęstinumą ir veiksmingas tada, kai taisyklės ir reikalavimai ne tik nugula dokumentų puslapiuose, bet tiesiogiai įtakoja organizacijų procesus ir čia galima teigti, kad kibernetinio saugumo kultūra pereina į organizacinį lygmenį, šią temą detaliau analizavo Wilie (2023), kuris nagrinėjo organizacijos vaidmenį kibernetinio saugumo srityje. Autorius pabrėžė, kad organizacijos kultūra daro didelę įtaką darbuotojų požiūriui ir supratimui apie kibernetinę saugą, vadovų aktyvus dalyvavimas saugumo iniciatyvose, kaip pagrindinis veiksnys formuojant kibernetinio saugumo kultūrą. Wilie (2023) pateikė išvadas, kad organizacijos, suprasdamos ir panaudodamos organizacijos kultūros vaidmenį, gali sukurti tvirtą kibernetinio saugumo kultūrą. Remiantis autoriumi, organizacijos kultūra įtakoja ir individualią kibernetinio saugumo kultūrą. Individualus lygmuo apima asmenines žinias ir įgūdžius dėl kibernetinio saugumo. Organizacija laikydamasi nacionalinių teisės aktų, įstatymų, kuria darbo procesus, vidines darbo tvarkas, o darbuotojai privalo jų laikytis. Palaipsniui diegiant kibernetinio saugumo kultūrą, rodant tinkamą pavyzdį, kuriant saugumo politikas ir tvarkas, vykdant nuolatinį švietimą kibernetinio saugumo tema, po truputį keičiamas darbuotojų elgesys, jų požiūris.

Tarptautinės ir nacionalinės kibernetinio saugumo kultūros tarpusavio sąveika padeda sukurti veiksmingą kibernetinio saugumo ekosistemą. Nacionaliniai teisės aktai ir įstatymai nurodo

pagrindines taisykles ir reikalavimus, kurių turi laikytis organizacijos. Organizacijos įgyvendindamos įstatymų reikalavimus, kuria aplinką, kurioje darbuotojai jaučia atsakomybę kibernetinio saugumo srityje ir supranta savo vaidmenį, užtikrinant informacijos saugumą. Vienas kibernetinio saugumo kultūros lygis įtakoja kitą, tai būdinga visiems sektoriams.

2. Kibernetinės grėsmės sveikatos sektoriuje

Sveikatos priežiūros srityje kiekvienas kibernetinis incidentas gali ne tik paveikti organizacijos reputaciją ir turėti finansinių nuostolių, bet šis poveikis padidėja, nes incidentas gali fiziškai pakenkti žmonėms, kaip tai įvyko 2020 metais Vokietijoje Diuseldorfo ligoninėje, po to kai išpirkos programinė įranga užšifravo ligoninės duomenis ir ši negalėjo priimti pacientų ir dėl pervežimo į kitą ligoninę, pacientas mirė. (Silomon, 2020) Po išpirkos programinės įrangų atakų padidėja medicininės komplikacijos ir mirtingumas. Neturėdami prieigos prie paciento duomenų ar IT sistemų atšaukiami apsilankymai, vėluojama diagnozuoti ir gydyti. (Alder, 2024) Sveikatos priežiūros sektoriui būtina ypač rimtai žiūrėti į kibernetines grėsmes. Kibernetinių grėsmių nagrinėjimas, jų žinojimas yra pagrindinis elementas, padedantis organizacijoms apsisaugoti nuo kibernetinių atakų, sumažina galimas rizikas ir kartu stiprina kibernetinio saugumo kultūrą organizacijoje. ENISA (2016) išleido leidinį, kuriame pasiūlė „išmaniųjų ligoninių“ apibrėžimą: „Išmanioji ligoninė, tai ligoninė, kuri remiasi optimizuotais ir automatizuotais procesais, paremtais tarpusavyje sujungtų išteklių IRT aplinka, ypač pagrįsta daiktų internetu, siekiant pagerinti esamas pacientų priežiūros procedūras ir įdiegti naujas galimybes.“ Taip pat teigė, kad pagrindinė išmaniųjų ligoninių problema yra informacijos saugumas, nes ligoninės neturi aiškių ribų, dėl didelio suinteresuotų šalių bendradarbiavimo, daugybės tarpusavyje susijusių išteklių ir ligoninių veiklos sudėtingumo. Razaque, Amsaad, Khan, Hariri, Chen, Siting ir Xingchen Ji (2019) aprašė sveikatos priežiūros sektoriaus duomenų srauto modelį, teigdami, kad keitimosi informacija procesas yra būtinas teikiant sveikatos priežiūros paslaugas, todėl būtina apsaugoti šiuos duomenis nuo sugadinimo, sunaikinimo, ar pakeitimo, kuris gali turėti įtakos gydytojų sprendimams dėl gydymo. Jų pristatytas sveikatos priežiūros sektoriaus duomenų srauto modelis susideda iš keturių etapų: paciento registracija, duomenų rinkimas, duomenų saugojimas ir medicininių duomenų taikymas. Visi etapai pereina skirtingus įrenginius ir tinklus, kur kiekviename žingsnyje gali įvykti įsilaužimas. Tarpusavyje sujungtos informacinės sistemos ir tinkle sujungti medicininiai prietaisai sudaro platesnį kibernetinių atakų paviršių. Ši sąveika gali padidinti organizacijų pažeidžiamumą ir kelti grėsmę pacientų saugumui, todėl būtina stiprinti kibernetinį saugumą sveikatos sektoriuje.

2.1. Kibernetinių grėsmių samprata ir esminiai bruožai

Pasauliui vis labiau persikeliant į elektroninę erdvę ir vis labiau pasitikint internetu ir informacinėmis technologijomis, auga duomenų pažeidimų, sukčiavimo ar tapatybės vagysčių skaičius. Organizacijos supranta kibernetinio saugumo svarbą, tačiau ne visada aktyviai dalyvauja, kuriant kibernetinio saugumo politiką. Vienas iš etapų, norint apsisaugoti, reikia žinoti nuo ko saugotis. 1 lentelėje pateikti kibernetinės grėsmės sąvokų apibrėžimai.

1 lentelė. Kibernetinės grėsmės sąvokos apibrėžimai

Eil. Nr.	Sąvoka	Autorius
1.	Kibernetinė grėsmė - kenkėjiškas veiksmas, kuriuo siekiama pavogti ar sugadinti duomenis arba sutrikdyti įmonės skaitmeninę gerovę ir stabilumą.	Roy, 2021
2.	Kibernetinė grėsmė - aplinkybė ar įvykis, galintis neigiamai paveikti organizacines operacijas (įskaitant misiją, funkcijas, įvaizdį ar reputaciją), organizacinį turtą ar asmenis per informacinę sistemą ir neteisėtą prieigą, sunaikinimą, atskleidimą, informacijos keitimą ir (arba) atsisakymą teikti paslaugas. Be to, grėsmės šaltinio galimybė sėkmingai išnaudoti tam tikrą informacinės sistemos pažeidžiamumą.	JAV Nacionalinis standartų ir technologijų instituto, kompiuterinių išteklių saugos centro žodynėlis
3.	Kibernetinė grėsmė - galima aplinkybė, įvykis arba veiksmas, kuris galėtų pažeisti, sutrikdyti arba kitaip neigiamai paveikti tinklų ir informacines sistemas, tokių sistemų naudotojus ir kitus asmenis.	Europos parlamento ir tarybos reglamentas (ES) 2019/881 (2019)
4.	Kibernetinė grėsmė – tai veikla, kuria siekiama pakenkti informacinės sistemos saugumui, pakeičiant sistemos ar joje esančios informacijos prieinamumą, vientisumą ar konfidencialumą, arba apskritai sutrikdyti skaitmeninį gyvenimą.	Kanados kibernetinio saugumo centras, 2022

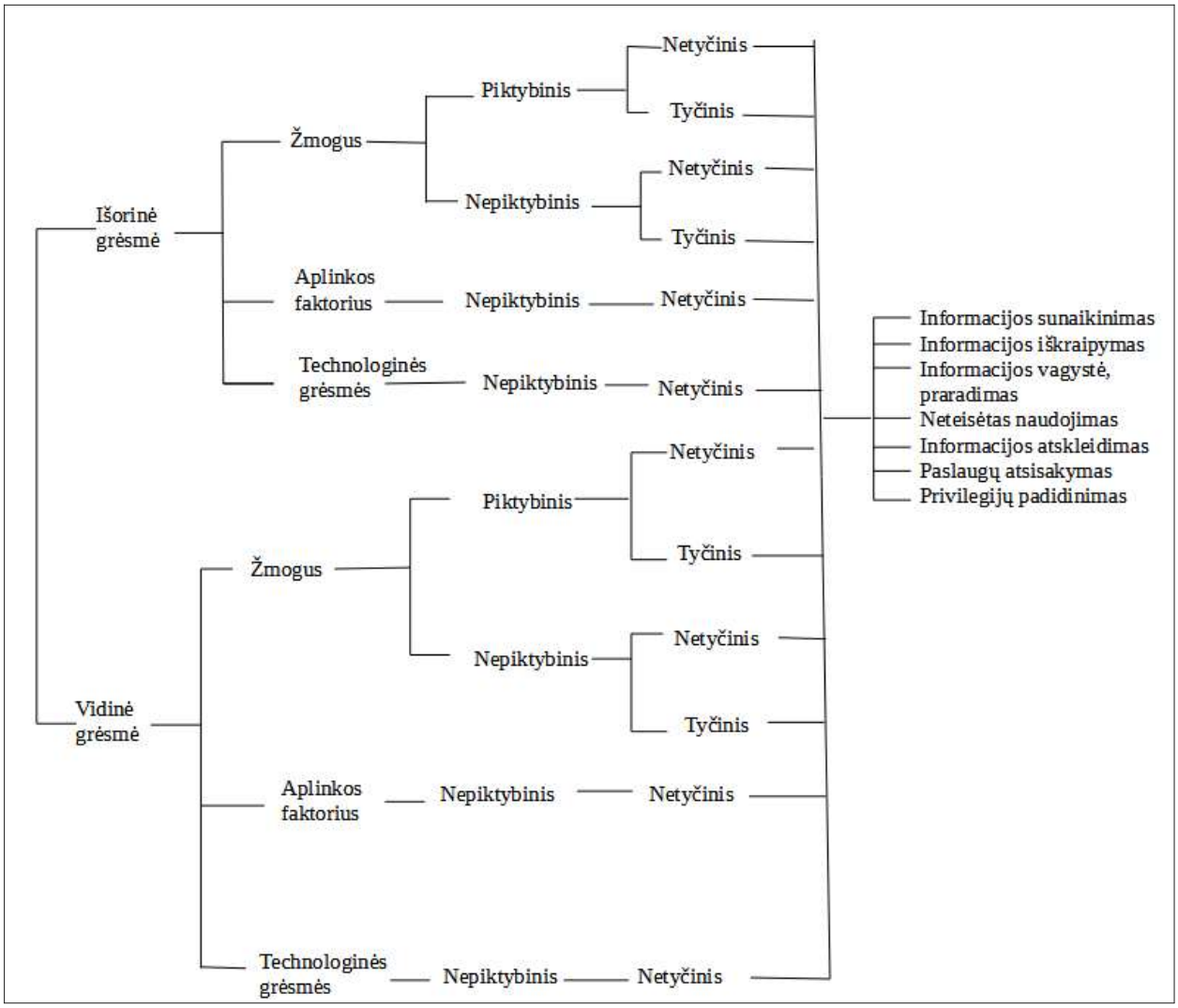
1 lentelės tęsinys kitame puslapyje

1 lentelės tęsinys

Eil. Nr.	Sąvoka	Autorius
5.	Kibernetinė grėsmė – galimas piktybinis veiksmas, kuriuo siekiama sabotuoti visuomenės gebėjimą palaikyti vidinę ar išorinę tvarką.	Malik, Abid, Farooq, Abidas, Navaz ir Ishaq, 2022

Išanalizavus pateiktus apibrėžimus, galima šią sąvoką apibrėžti, kaip neigiamą įvykį, turintį neigiamo poveikio ne tik informacinėms sistemoms, tinklams, bet ir jų naudotojams.

„Kibernetinis saugumas ir verslas“ vadove (2020) teigiama, kad kiekviena įmonė turi įvertinti naudojamų sistemų ir duomenų svarbą, kad galėtų pereiti prie galimų grėsmių įmonės veiklai nustatymo. Vadove rašoma, kad grėsmės nebūtinai gali būti piktybinės. Pažeidimas gali įvykti darbuotojui atidarius užkrėstą dokumentą, ištrynus ar redagavus svarbius įmonės duomenis, todėl labai svarbu dirbti drauge su savo darbuotojais. Grėsmės saugumui gali kilti iš išorės ir iš vidaus. Tad dažnai kibernetinės grėsmės yra skirstomos į vidines ir išorines. Vidinė grėsmė reiškia riziką, kad kažkas iš įmonės vidaus gali išnaudoti sistemą taip, kad padarytų žalos ar pavogtų duomenis. Išorinė grėsmė tai grėsmė iš išorės, kuri bandys išnaudoti sistemos pažeidžiamumus, naudodamas kenkėjišką programinę įrangą, įsilaužimą ar socialinę inžineriją. (Mazzarado ir Jurcut, 2019) Autoriai Jouini, Rabaia ir Aissa (2014) pasiūlė hibridinį grėsmių klasifikavimo modelį, kuriame grėsmes skirstė pagal kilmę, grėsmės veikėjus, motyvaciją ir poveikį. (5 pav.)



Šaltinis: adaptuota pagal Jouini ir kt., 2014

6 pav. Hibridinis grėsmių klasifikavimo modelis

Roy (2021) teigia, kad kibernetinės grėsmės apima platų atakų spektrą, tai ir duomenų pažeidimai ir kompiuteriniai virusai, bei paslaugų atsisakymo ir daugybė kitų atakų vektorių. Autoriai Malik ir kt. (2022) kibernetines grėsmes apibrėžė kaip veiklą, kuri gali pakenkti visuomenės gebėjimui palaikyti vidinę ar išorinę tvarką, naudojant informacines technologijas ir suskirstė į tris plačias kategorijas:

Kibernetinius nusikaltimus autoriai apibūdino, kaip nusikalstamą veiklą, kurios vykdymui naudojami kompiuteriai, skaitmeniniai įrenginiai ir tinklai, elektroninėje erdvėje. LR Baudžiamajame kodekse dauguma veikų – elektroninių nusikaltimų yra kriminalizuotos. Autoriai pristatė šiuos nusikaltimų tipus: sukčiavimas, tapatybės vagystės, privatumo pažeidimai, kibernetinis persekiojimas, socialinė inžinerija ir kt. Kibernetinių nusikaltimų motyvai yra pinigai ir

informacija. Kibernetiniai nusikaltėliai visada naudojasi vartotojų pažeidžiamumu ir aplaidumu, dėl vartotojų nesąmoningumo saugumo klausimais.

Kibernetinis terorizmas. Kibernetinio terorizmo išpuolius vykdo politiškai ar ideologiškai motyvuoti nevalstybiniai veikėjai. Pagrindinis šių išpuolių tikslas – sugriauti infrastruktūrą ir sutrikdyti visuomenės veiklą.

Kibernetinis karas. Kibernetinis karas paprastai reiškia vienos ar kelių nacionalinių valstybių vykdomas kibernetines atakas prieš kitą. Pagal autorius kibernetinio karo atakos gali būti suskirstytos į tris kategorijas: naikinimas, trikdymas ir dezinformacija.

Cassetto (2023) išskyrė septynias pagrindines kibernetinio saugumo grėsmių rūšis: kenkėjiškų programų ir socialinės inžinerijos atakos, programinės įrangos tiekimo grandinės, išplėstinės nuolatinės grėsmės atakos (APT), paskirstyta paslaugos trikdymo ataka (DdoS), "Man-in-the-middle" ataka (MitM) ir slaptažodžių ataka. ENISA (2022) Grėsmių kraštovaizdžio atsakaitoje pristatytos aštuonios: išpirkos reikalaujančios kenkėjiškos programos, kenkėjiškos programos, socialinės inžinerijos grėsmės, grėsmės duomenų saugumui, grėsmės prieinamumui: paslaugų atsisakymas, grėsmės prieinamumui: interneto grėsmės, dezinformacija ir teikimo grandinės atakos.

Kibernetinių grėsmių klasifikavimas yra sudėtingas dėl pačių atakų sudėtingumo ir tarpusavio persipynimo, todėl skirtinguose literatūros šaltiniuose naudojamos skirtingos klasifikavimo sistemos, pasigendama vieningos sistemos. Remiantis įvairiais literatūros šaltiniais, autoriaus sudaryta kibernetinių grėsmių apibūdinimo ir poveikio lentelė. (2 lentelė)

2 lentelė. Kibernetinių grėsmių apibūdinimas ir poveikis

Grėsmės tipas	Apibūdinimas	Poveikis
Kenkėjiškos programos	Bet kokio tipo programinė įranga ar kodas sukurtas, siekiant pakenkti kitai programinei ar aparatinei įrangai arba ją išnaudoti.	Duomenų praradimas Finansiniai nuostoliai Reputacinė žala
Paskirstyta paslaugos trikdymo ataka	Kenkėjiška, tikslinė ataka, kuri užtvindo tinklą klaidingomis užklausomis, kad sutrikdytų veiklą.	Duomenų prieinamumui Finansiniai nuostoliai Reputacinė žala
„Man-in-the-middle“ ataka	Užpuolikas slapta perima dviejų šalių ryšį, kad pavogtų slaptus kredencialus, sugadintų duomenis arba šnipinėtų aukas.	Neskelbtinos informacijos vagystė Finansiniai nuostoliai
Slaptažodžių atakos	Įsilaužėlis, atsitiktinai arba sistemingai bando atspėti slaptažodį arba gauti prieigą prie slaptažodžių duomenų bazės.	Duomenų vagystė Paslaugų nepasiekiamumas naudotojui

2 lentelės tęsinys kitame puslapyje

2 lentelės tęsinys

Grėsmės tipas	Apibūdinimas	Poveikis
Socialinės inžinerijos grėsmės	Kenkėjiška veikla, naudojanti psichologinį manipuliavimą, kad apgautų vartotojus ir išviliotų neskelbtiną informaciją.	Asmeninės informacijos paviešinimas Duomenų praradimas Reputacinė žala Finansiniai nuostoliai
SQL injekcijos	Tai technika, kai užpuolikas išnaudoja trūkumus programos kode ir įterpiamas specialus SQL kodas.	Duomenų nutekėjimas Reputacinė žala Finansiniai nuostoliai Sistemos kontroliavimas
Išplėstinės nuolatinės grėsmės	Ilgalaikė ir tikslinė kibernetinė ataka, kurios metu gaunama prieiga prie tinklo ir ilgą laiką lieka nepastebėta.	Duomenų nutekėjimas Paslaugų sutrikimas Reputacinė žala
Tiekimo grandinės atakos	Atakos metu bandoma paveikti tiekimo grandinės dalyvius (subrangovai, paslaugų teikėjai).	Duomenų nutekėjimas Paslaugų sutrikimas Reputacinė žala Finansiniai nuostoliai
Vidinės grėsmės	Tai esamų ar buvusių darbuotojų keliamas pavojus organizacijai, dėl jų tiesioginės prieigos prie tinklo.	Duomenų nutekėjimas Finansiniai nuostoliai Reputacinė žala
IoT grėsmės	Ataka nukreipta į daiktų interneto įrenginį ar tinklą.	Duomenų nutekėjimas Duomenų praradimas Finansiniai nuostoliai

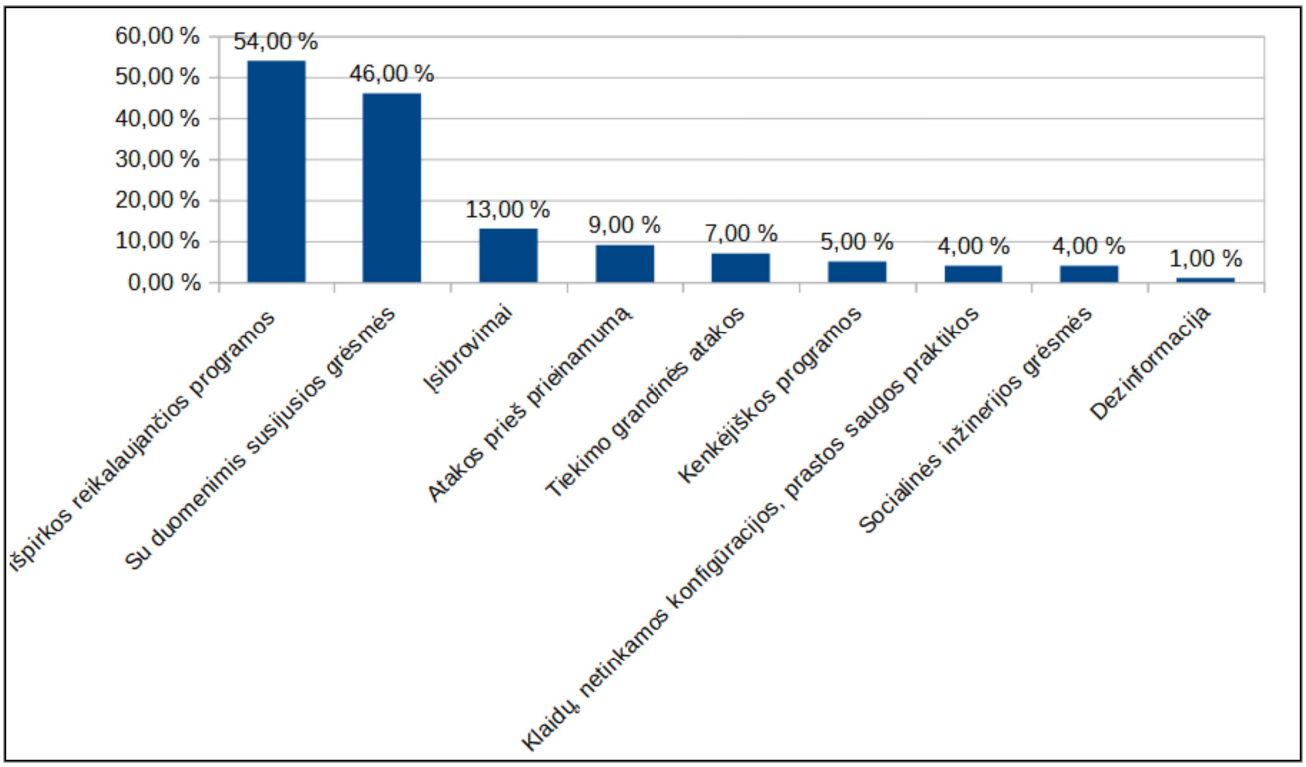
Kibernetinės grėsmės gali pasireikšti įvairiomis formomis ir turėti skirtingus bruožus. Kiekviena ataka siekia pavogti ar sugadinti duomenis arba sutrikdyti organizacijos skaitmeninę gerovę ir stabilumą. Pagrindinės kibernetinės grėsmės, būdingos sveikatos sektoriui, apžvelgtos kitame skyriuje.

2.2. Pagrindinės kibernetinės grėsmės sveikatos sektoriuje

Sveikatos priežiūros sektorius per mažai savo biudžeto skiria informacinėms sistemoms ar tinklams apsaugoti, naudojama pasenusi programinė įranga ir sena operacinių sistemų versija. Pasenusioje programinėje įrangoje yra klaidų ir tai yra didžiausia sveikatos priežiūros sektoriaus problema. (Ahmed ir kt., 2020) Ting (2022) rašė, kad pastebimas dramatiškas kibernetinių atakų skaičiaus padidėjimas sveikatos sektoriuje, kartu su juo išaugusios išlaidos atsigavimui po duomenų pažeidimo. Autorius teigė, kad 2021 metais Amerikoje 66% sveikatos priežiūros organizacijų patyrė išpirkos reikalaujančių programų atakas ir tai yra 34% daugiau nei 2020 metais. 91% įsilaužimų turėjo finansinį motyvą, vienos išpirkos reikalaujančių programų atakos ištaisymo išlaidos yra 1,27

mln. dolerių. Per COVID-19 pandemiją sukčiavimo išpuolių prieš sveikatos priežiūros organizacijas padaugėjo 220 proc. Visame pasaulyje sveikatos sektoriuje kibernetinio saugumo išlaidos tik didės. (Ting, 2022)

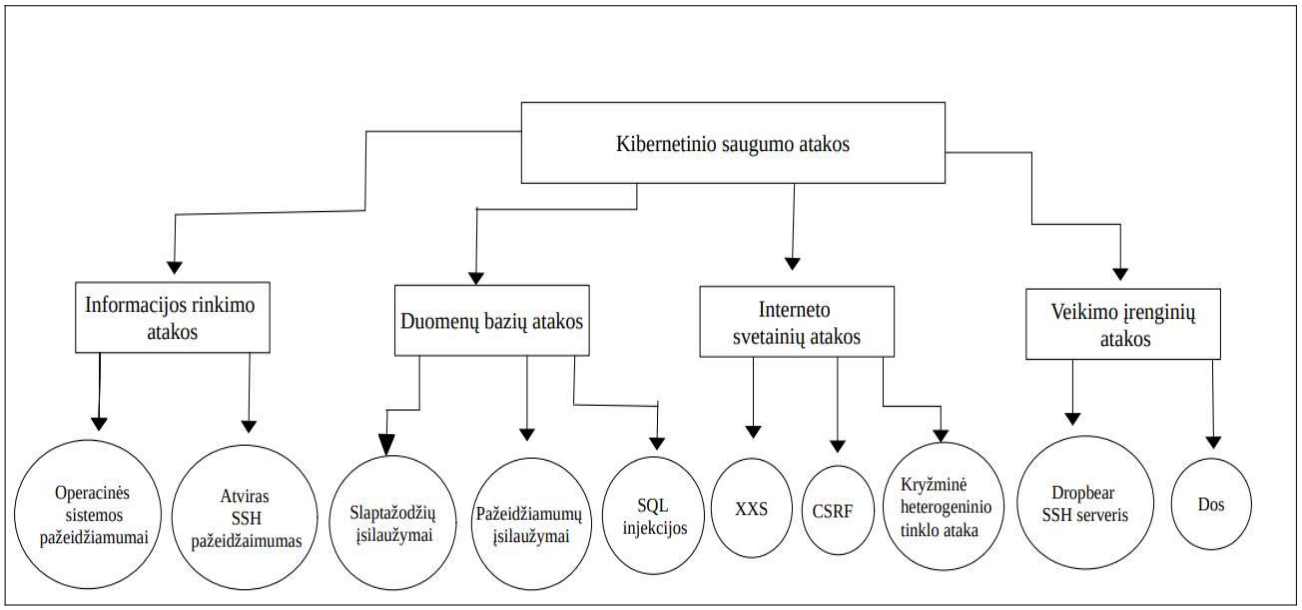
ENISA (2023) grėsmių kraštovaizdžio sveikatos sektoriuje ataskaitoje rašė, kad 2021 m. sausio mėn. - 2023 m. kovo mėn. laikotarpiu 54 % visų incidentų sudarė išpirkos reikalaujančios programos, išpuoliai prieš sveikatos priežiūros tiekimo grandinę ir paslaugų teikėjus sudarė 7 %, Ddos atakos prieš ligonines ir sveikatos priežiūros institucijas – 9 %. (6 pav.)



Šaltinis: adaptuota pagal ENISA, 2023

7 pav. Grėsmės sveikatos sektoriui

Razaque ir kt. (2019) sutelkė dėmesį į keturias pagrindines atakas, turinčias poveikio žmonių sveikatai: informacijos rinkimo, duomenų bazių, svetainių ir veikimo įrenginių atakos. (8 Pav.)



Šaltinis: adaptuota pagal Razaque ir kt. (2019)

8 pav. Kibernetinio saugumo atakų klasifikacija

Kibernetiniai išpuoliai tampa vis sudėtingesni ir labiau paplitę, sveikatos sektorius kibernetinį saugumą turėtų laikyti prioritetu ir skirti pakankamai finansų, apsaugant savo pacientus, organizaciją ir darbuotojus nuo kibernetinių grėsmių. Kost (2023) ir autoriai Kovacs ir Besenyo (2023) išskyrė šias pagrindines kibernetines grėsmes sveikatos sektoriuje, keliančias didžiausią riziką paciento informacijos ir sveikatos priežiūros duomenų saugumui: sukčiavimas apsimetant (phishing), išpirkos reikalaujančių programų atakos (ransomware), duomenų pažeidimai, DdoS atakos ir viešai neatskleista grėsmė. Autoriai Ahmed, Sindi ir Nour (2022) pristatydami kibernetinio saugumo vertinimo modelį ligoninėse išskyrė šiuos atakų tipus: sukčiavimas el.paštu, „ransomware“, įrangos praradimas, duomenų praradimas: tyčinis, netyčinis, atsitiktinis ir išpuoliai prieš prijungtus medicinos prietaisus. Autoriai Ahmed ir kt. (2020) teigė, kad daiktų internetas tai dar viena didelė sveikatos priežiūros sektoriaus problema, nes jie atveria duris užpuolikams patekti į tinklą ir padaryti žalos. Taip pat Adegoke, Navya, Jordan, Jenifer ir Begley (2022) savo tyrime apžvelgė kibernetinio saugumo tendencijas, kuriose autoriai rašė, kad medicininės ir fizinės sistemos apima medicininį daiktų internetą, implantuojamus ir nešiojamus medicinos prietaisus, kurie kelia didelę kibernetinio saugumo riziką visai sveikatos priežiūros sistemai. Trūksta paaiškinimų dėl nuosavybės po pardavimo, programinės įrangos atnaujinimų ir saugumo reguliavimo pasauliniu mastu. ENISA (2016) pateikdama rekomendacijas išmaniosioms ligoninėms, taip pat rašė, kad priklausomybė nuo daiktų interneto auga greičiau nei galimybės užtikrinti saugumą. „Cynerio” (2022), sveikatos priežiūros daiktų interneto saugumo platforma JAV,

paskelbė ataskaitą, kurioje nagrinėjo grėsmes ir saugumo problemas, susijusias su prie tinklo prijungtu daiktu internetu bei medicinos prietaisais. Ataskaitoje teigiama, kad daugiau nei 50% prijungtų prietaisų ligoninėse yra kritinės rizikos, o daugiau nei 50 % onkologijos, farmakologijos ir laboratorinių skyrių įrenginiai veikia senose Windows versijose.

Autoriai Adegoke ir kt. (2022) debesų kompiuteriją apibūdinto kaip grėsmę duomenų ir informacijos saugumui tiek perdavimo, tiek saugojimo metu. Sveikatos taikomųjų programų (programėlių) saugos funkcijų trūkumas yra didėjanti kibernetinio saugumo rizika asmens duomenų konfidencialumui ir sveikatos priežiūros infrastruktūros vientisumui.

Autoriai Ahmed ir kt. (2020) teigė, kad kai žmonės žino apie kibernetines grėsmes ir žino, kokią žalą jos sukelia, jie yra labiau linkę imtis veiksmų, atakų užkardymui. Todėl norint apsisaugoti nuo šių grėsmių, sveikatos sektoriaus organizacijos turi skirti išteklių ir laiko kibernetinio saugumo kultūros stiprinimui ir plėtrai savo įstaigose, kurdami informacijos saugumo politikas, reguliariai atnaujindami saugumo priemones, mokydami personalą saugumo taisyklių ir aktyviai stebėdami galimus pažeidimus.

2.3. Kibernetinių grėsmių veikėjai ir jų motyvai

Už kiekvienos kibernetinės grėsmės slepiasi jos autorius – veikėjas, kuriam būdinga skirtinga taktika, metodai ir procedūros. Kibernetinių grėsmių veikėjai gali naudoti įvairius metodus savo atakoms vykdyti, tai ir sukčiavimą apsimetant ir kenkėjiškas bei išpirkos reikalaujančias programas. Jie taip pat gali pasinaudoti kompiuterinių sistemų ir tinklų pažeidžiamumu, kad gautų prieigą ir pavogtų neskelbtiną informaciją. Kiekvienas kibernetinių grėsmių veikėjas turi skirtingą išpuolių motyvą. Vienus motyvuoja finansiniai, politiniai interesai, kitus- ekonominiai ar asmeniniai.

Kibernetinių grėsmių veikėjai gali būti suskirstyti į kategorijas pagal jų motyvaciją ir pagal jų sudėtingumo laipsnį. (Kanados kibernetinio saugumo centras, 2022) Cassetto (2023) pristatė aštuonis kibernetinių grėsmių veikėjus, neišskirdamas, kuriam sektoriui jis būdingas: valstybių remiami veikėjai, pramoniniai šnipai, teroristai, organizuotos nusikalstamos grupuotės, įsilaužėliai, haktyvistai, kenkėjiškas viešai neatskleistas asmuo, kibernetinis šnipas. ENISA (2022) pabrėžė keturias kibernetinių grėsmių veikėjų kategorijas, kurios būdingos ir sveikatos sektoriui: valstybių remiami veikėjai, kibernetiniai nusikaltėliai, įsilaužėliai ir haktyvistai. JAV „Sveikatos ir žmogiškųjų paslaugų departamentas“ kartu su „Sveikatos sektoriaus kibernetinio saugumo koordinavimo centru“ (2023) išleido leidinį, kuriame pristatė kibernetinių grėsmių veikėjus, keliančius grėsmę sveikatos sektoriui: kibernetiniai nusikaltėliai, hacktyvistai, nacionalinių

valstybių veikėjai, kiberteroristai, „scenarijaus vaikai“ ir vidinės grėsmės. Vienas iš įdomesnių veikėjų, pristatytų šiame dokumente – „scenarijaus vaikai“, tai terminas naudojamas apibūdint pradedančius įsilaužėlius, kurie neturi pakankamai žinių ir naudoja visiems gerai žinomus, kitu sukurtus scenarijus ar programas ir dažniausiai jų motyvas būna linksmybės, chaoso kūrimas, kartais kerštas. Kanados kibernetinio saugumo centro išleistame dokumente (2022) rašo, valstybių remiamus veikėjus dažniausiai motyvuoja geopolitiniai tikslai. Jie siekia sutrikdyti ryšius, karinę veiklą ir kasdienį gyvenimą. Dažniausiai jų atakos yra sudėtingos ir tikslios, o nusikaltėliai turi specialius įrankius ir pažangiausią turimą programinę įrangą bei gali skirti daug laiko planavimui ir veiksmų koordinavimui lyginant su kitais grėsmių veikėjais. Teroristai vykdo kibernetinius išpuolius, kad sunaikintų, įsiskverbtų ar išnaudotų ypatingos svarbos infrastruktūrą ir sukeltų grėsmę nacionaliniam saugumui, pakenktų karinei įrangai, sutrikdytų ekonomiką ir sukeltų masines nelaimes. Pramoniniai šnipai vykdo pramoninį ar verslo šnipinėjimą, kad gautų pelno arba sutrikdytų konkurentų verslą, atakuodami kritinę infrastruktūrą, pavogdami komercines paslaptis ir gaudami prieigą. Organizuotos nusikalstamos grupuotės siekia įsiskverbti į sistemas ar tinklus, siekdamos finansinės naudos. Šios grupės naudoja sukčiavimą apsimetant, šnipinėjimo ir kenkėjiškas programas, kad įvykdytų tapatybės vagystes, sukčiavimą internete ir sistemos turto prievartavimą. Įsilaužėliai tyrinėdami įvairius kibernetinius metodus, ieško kompiuterinės sistemos ar tinklo pažeidžiamumų ir gali būti motyvuoti politinėmis ar socialinėmis priežastimis. Haktyvistai kibernetines atakas vykdo siekdami politinių priežasčių, o ne siekdami finansinės naudos, juos motyvuoja noras padaryti pareiškimą teisingumo vardu ar „ištaisyti neteisybę“ kartais tai būna tiesiog kerštas arba noras pakenkti organizacijos veiklai. Jie skirti pramonės šakoms, organizacijoms ar asmenims, kurie neatitinka jų politinių idėjų ir pažiūrų. Kenkėjiškas viešai neatskleistas asmuo apima darbuotojus, trečiųjų šalių tiekėjus, rangovus ar kitus verslo partnerius, kurie turi teisėtą prieigą prie įmonės turto, tačiau netinkamai naudojasi šia prieiga, kad pavogtų ar sunaikintų informaciją siekdami finansinės ar asmeninės naudos. Kibernetinis šnipas vagia įslaptintus arba neskelbtinus duomenis, siekiant įgyti pranašumą prieš konkurencingą įmonę ar vyriausybinį objektą.

Kokie bebūtų kibernetinių nusikaltėlių motyvai, savo nusikalstamu elgesiu kelia pavojų organizacijoms ir jų veiklai. Kibernetinių grėsmių veikėjų žinojimas ir jų motyvacijos supratimas gali būti pagrindas, kuriant tvirtas kibernetinio saugumo politikas.

2.4. Naujausi kibernetiniai incidentai sveikatos sektoriuje

Sveikatos priežiūros specialistai daugiausia dėmesio skiria pacientams ir medicinos praktikai, neskirdami pakankamo dėmesio klausimams, susijusiems su sveikatos IT sauga ir privatumu. Kibernetinės grėsmės veikėjai, išnaudojantys medicinos prietaisų pažeidžiamumą, neigiamai veikia sveikatos priežiūros įstaigų veiklos funkcijas, pacientų saugą, duomenų konfidencialumą ir duomenų vientisumą. LR Valstybės saugumo departamento Grėsmių nacionaliniam saugumui vertinime (2021) buvo pateikti 2020 metų kenkėjiškų veiklų pavyzdžiai: Klaipėdos jūrininkų ligoninės tarnybinių stočių, kuriose veikė buhalterinės apskaitos dokumentų valdymo ir vaistų verifikavimo sistemos, atakos metu duomenys buvo užšifruoti, taip pat užfiksuota pirma kibernetinės atakos tiesiogiai nulemta žmogaus mirtis Vokietijoje po to, kai Diuseldorfo universitetinė ligoninė patyrė išpirkos reikalaujančios programos ataką ir dėl ilgo pervežimo į tolimesnę ligoninę, pacientas mirė. Kibernetinę ataką patyrė ir Lietuvos nacionalinis visuomenės sveikatos centras. „Ransomware“ ataka paveikė visas vienos didžiausių sveikatos apsaugos paslaugų tiekėjų „Universal Health Services“ kompanijos priežiūros įstaigas ir ligonines JAV.

ENISA (2023) ataskaitoje rašė, kad 2021 m. sausio mėn. - 2023 m. kovo mėn. laikotarpiu įvykusių duomenų pažeidimų labiausiai paveiktos buvo ligoninės (27%), farmacijos įmonės (15%), sveikatos priežiūros institucijos ir agentūros (14%) ir pirminės sveikatos priežiūros įstaigos (8%). 2022 metais Škotijos psichikos sveikatos asociacija, Katalonijos sveikatos centrai „Consorci Sanitari Integral“, 2023 metais „Elsan“ klinikos Prancūzijoje ir Barselonos ligoninė patyrė duomenų pažeidimus. 2021 metais duomenų nutekėjimus patyrė Šiaurės Airijos sveikatos departamentas, koronavirusų tyrimų bendrovė „Testcoronanu“ Nyderlanduose, Tarptautinis Raudonasis kryžiaus komitetas Šveicarijoje taip pat kompanija „Dedalus Biologie“. Taip pat ENISA (2023) pateikė, kad Ddos atakas 2023 m. sausį patyrė keturios Ispanijos ligoninės ir tų pačių metų vasarį aštuonios Danijos ligoninės, incidentai nebuvo susiję su sveikatos priežiūros paslaugų teikimu, tai paveikė viešosios informacijos tinklalapius ar nereikšmingas interneto paslaugas trumpą laiką.

Mason Hayes & Curran skaitmeninės sveikatos 2022 metinėje ataskaitoje rašė, kad 2022 metais Prancūzijos ligoninė, aptarnaujanti 600 000 pacientų, ir JK Nacionalinės sveikatos tarnybos, patyrė išpirkos reikalaujančių programų atakas. 2021 metais Airijos sveikatos tarnybos vadovas (HSE) patyrė didelio masto išpirkos reikalaujančių programų ataką. 2020 metais Suomijos psichikos sveikatos įstaiga patyrė duomenų pažeidimą. 2023 metais JAV Lehigh Valley sveikatos tinklas patyrė išpirkos reikalaujančių programų ataką, kurios metu paviešino pacientų, sergančių onkologinėmis ligomis, nuotraukas ir informaciją tamsiajame internete. (Mckeon, 2023)

2023 metais „Advocate Aurora Health“ 26 ligoninių sveikatos priežiūros sistema Viskonsine ir Ilinojaus valstijoje patyrė 3 mln. vartotojų duomenų pažeidimą dėl netinkamo „Meta Pixel“ naudojimo. 2023 metų liepą „HC Healtcare“ Nešvilyje, sveikatos priežiūros paslaugų teikėjas, kurį sudaro 180 ligoninių ir 2300 ambulatorinių priežiūros vietų, pranešė apie duomenų pažeidimą. Programišiai gavo prieigą prie išorinės elektroninės saugyklos, kurią verslo partneris naudojo automatizuodamas el. laiškų formatavimą. Tą patį mėnesį pažeidimą patyrė „Medicare“ ir Floridos „Tampos bendroji ligoninė“, „United Healtcare“, „The Chattanooga Heart institute“, „Phoenician medical center“ ir daug kitų. Analizuojant straipsnyje pateiktą statistiką matyti, kad 2023 metų sausio - liepos mėnesiais Jungtinėse Amerikos Valstijose įvyko 395 duomenų pažeidimai sveikatos priežiūros srityje. (Alder, 2023)

ENISA atliktu tyrimu, 40% organizacijų neturi saugumo informavimo programų, skirtų ne IT darbuotojams ir NIS bendradarbiavimo grupėje atliktoje apklausoje 95% apklaustų sveikatos organizacijų susiduria su iššūkiais atliekant rizikos vertinimą, o 46% niekada nebuvo atlikę rizikos analizės. (ENISA, 2023) HIMSS atliktame 2022 metų sveikatos priežiūros kibernetinio saugumo tyrime teigiama, kad organizacijos kibernetinio saugumo specialistų trūkumas yra didžiulis iššūkis taip pat nepakankamas biudžeto skirimas, nereguliarūs mokymai darbuotojams ir teigė, kad žmogiškasis faktorius toliau išlieka didžiausias pažeidžiamumas, todėl daugiau dėmesio reikia skirti kibernetinio saugumo programų įgyvendinimui.

Išpirkos reikalaujančios programos yra viena iš didžiausių grėsmių sveikatos sektoriuje, taip pat pastebimas Ddos atakų skaičiaus padidėjimas ir nepataisyti pažeidžiamumai ar netinkama sistemų konfigūracija yra nauja grėsmė sveikatos sektoriui. (ENISA, 2023) Iššūkiai susiję su kibernetiniais incidentais, reikalauja nuolatinio dėmesio. Didėjant technologiniam pažangumui, didėja saugumo rizikų lygis, būtina stiprinti saugumo politikas, šviesti darbuotojais saugumo klausimais, nuolat tobulinti saugumo priemones.

3. Kibernetinio saugumo kultūros Lietuvos ligoninėse vertinimas

3.1. Tyrimo metodologija

Tyrimo metodika ir organizavimas. Siekiant įvertinti esamą kibernetinio saugumo kultūros supratimo lygį Lietuvos ligoninėse buvo atliktas mišrus tyrimas. Kiekybinio tyrimo metu siekiama išsiaiškinti Lietuvos ligoninių darbuotojų supratimą apie kibernetinio saugumo kultūrą ir jos svarbą organizacijoje. Kokybinio tyrimo metu apklausti ligoninių vadovai, norint sužinoti, kaip vadovaujamose įstaigose skatinama kibernetinio saugumo kultūra ar skiriami papildomi finansai ir kaip patys vadovai supranta kibernetinio saugumo kultūrą bei kaip ją skatina. Atlikus gautų duomenų analizę bus pateiktos išvados, galinčios padėti tobulinant kibernetinio saugumo kultūrą Lietuvos ligoninėse.

Tyrimo tikslas. Įvertinti kibernetinio saugumo kultūrą Lietuvos ligoninėse.

Tyrimo uždaviniai:

1. Atskleisti Lietuvos ligoninių darbuotojų kibernetinio saugumo kultūros suvokimą.
2. Pateikti, kaip ligoninių vadovai supranta kibernetinio saugumo kultūrą ir kaip skatina jos vystymąsi.
3. Atlikus tyrimo analizę, įvertinti kibernetinio saugumo kultūrą Lietuvos ligoninėse ir parengti rekomendacijas kibernetinio saugumo kultūros stiprinimui sveikatos sektoriuje

Tyrimo metodai.

1. Anketinė apklausa. Kiekybiniam tyrimui pasirinkta anketinė apklausa skirta Lietuvos ligoninių darbuotojams. Šis metodas pasirinktas dėl nepakankamo tiriamos problemos išanalizavimo ir aprašymo literatūros šaltiniuose.
2. Struktūrizuotas interviu. Šis metodas pasirinktas, siekiant įvertinti, kaip ligoninių vadovai supranta ir kaip skatina kibernetinio saugumo kultūrą, vadovaujamose organizacijose.
3. Gautų duomenų analizė. Šiuo metodu siekiama išsiaiškinti, kaip Lietuvos ligoninių darbuotojai supranta kibernetinio saugumo kultūrą ir jos svarbą bei kaip ligoninių vadovai skatina kibernetinio saugumo kultūrą. Atlikus analizę buvo parengtos rekomendacijos, kibernetinio saugumo kultūros tobulinimui ir stiprinimui sveikatos sektoriuje.

Tyrimo reprezentatyvumas.

Kiekybinės strategijos tyrimo imties sudarymui buvo pasirinkta tikimybinė atsitiktinė atranka. Kiekybinėje internetinėje apklausoje buvo pakviesti dalyvauti Lietuvos ligoninių,

pavaldžių SAM ir savivaldybėms, darbuotojai. Kiekybinio tyrimo atveju atranka buvo statistiškai pagrįsta. Kokybinio tyrimo imties sudarymui pasirinkta kriterinė atranka. Kokybinio struktūrizuoto ekspertinio interviu respondentai atrenkami pagal šiuos kriterijus:

1. Vadovaujamo darbo patirtis gydymo įstaigoms ne mažiau 5 metai.
2. Dabartinei ligoninei vadovauja ne mažiau kaip du metai.

Tyrimas vyko trimis etapais:

1 etape atliekamas kiekybinis tyrimas– internetinė apklausa, kurios metu siekiama nustatyti Lietuvos ligoninių darbuotojų žinias ir suvokimą kibernetinio saugumo kultūros klausimais ir kaip tai priklauso nuo ligoninių lygmens.

2 etape vyko kokybinis tyrimas – interviu el. paštu su skirtingo ligoninių lygmens vadovais, siekiant išsiaiškinti kaip vadovai supranta kibernetinio saugumo kultūrą ir kaip skatina jos vystymąsi organizacijose.

3 etape aptariami gauti rezultatai, pateikiamos išvados dėl kibernetinio saugumo kultūros Lietuvos ligoninėse vertinimo ir pasiūlomos rekomendacijos sveikatos sektoriui, kibernetinio saugumo kultūros stiprinimui.

3.2. Kiekybinio tyrimo organizavimas.

Kiekybinio tyrimo organizavimas. Tyrimui pasirinktas instrumentas – anketinė apklausa internete. Elektroninių klausimynų nuoroda buvo siunčiama potencialiems tyrimo dalyviams. Tyrimas vyko 2023-12-20-2024-02-29 dienomis.

Tyrimo etika. Atliekant tyrimą, buvo laikomasi tyrimo etikos principų. Gaižauskaitė ir Mikėnė (2014) išskyrė šiuos principus: informuotas ir savanoriškas sutikimas dalyvauti tyrime, anonimiškumo ir gautos informacijos konfidencialumo užtikrinimas bei žalos respondentams vengimas. Tyrimo dalyviai prieš dalyvaudami apklausoje buvo supažindinti su tyrimo tikslu ir anonimiškumo užtikrinimu. Apklausos dalyviams nebuvo daromas spaudimas, jie savanoriškai ir laisvai apsisprendė dalyvauti apklausoje. Užtikrinant anonimiškumą, duomenys buvo pateikiami tik apibendrintai. Iš asmeninių duomenų anketoje buvo prašoma pateikti lytį, amžių, užimamas pareigas (pateikti keli galimi variantai) ir kokio lygio ligoninėje dirba (rajoninėje, regioninėje, respublikinėje). Šie duomenys buvo reikalingi norint pastebėti kaip skiriasi kibernetinio saugumo kultūros suvokimas tarp amžiaus, pareigų ir ligoninių lygmens. Atsakymų rezultatai yra prieinami tik tyrėjui.

Tyrimo klausimų grupės ir tikslai. Anketos užpildymo technikai naudoti uždari klausimai, respondentams pateikti atsakymų variantai, tereikėjo pasirinkti jiems priimtiniausią variantą.

Klausimai buvo sudaryti remiantis autorių Gioulekas, Stamatiadis, Tzikas, Gounaris, Georgiadou, Michalistsi-Psarrou, Doukas, Kontoulis, Nikoloudakis, Marin, Cabecinha ir Ntanos (2022) atliktu kibernetinio saugumo kultūros tyrimu, skirtu ypatingos svarbos sveikatos priežiūros infrastruktūros objektams ir papildyti tyrėją dominančiais klausimais, pritaikytais Lietuvos ligoninėms. Detali klausimyno struktūra ir klausimų grupės tikslai pateikiami 3 lentelėje.

3 lentelė. Anketos struktūra

Grupė	Klausimai	Tikslas
Sociodemografiniai klausimai	1-4 klausimai apie respondentų lytį, amžių, pareigas ir kokio lygmens ligoninėje dirba.	Klausimai padės apibrėžti tyrimo dalyvių kontingentą bei atlikti kryžminę analizę pagal amžiaus ir ligoninių lygmens grupes.
Papildomi klausimai IT darbuotojams	5. Kokius įrankius naudojate nuotoliniam darbui? 6. Ar jūsų organizacijos internetiniam puslapiui naudojami SSL sertifikatai?	Siekiant išsiaiškinti ar organizacijose dirbama nuotoliniu būdu ir kokiais nuotolinio darbo įrankiais naudojamasi. Taip pat ar užtikrinamas bendras saugumas naudojantis ligoninių interneto puslapiais.
Kibernetinio saugumo politikos	7. Ar jūsų organizacijoje egzistuoja kibernetinio saugumo politika? 8. Ar žinote, kam pranešti įvykus kibernetiniam incidentui? 9. Ar Jūsų organizacijoje yra paskirtas asmuo, atsakingas už kibernetinį saugumą? 10. Ar ligoninės vadovybė supranta kibernetinio saugumo svarbą ir ją palaiko?	Norima sužinoti ar organizacijoje yra kibernetinio saugumo politikos ar yra paskirti atsakingi asmenys ar darbuotojai, žino kam pranešti, įvykus kibernetiniam incidentui. Taip pat siekiama išsiaiškinti darbuotojų nuomonę dėl vadovybės įsitraukimo į kibernetinio saugumo kultūros stiprinimą.
Kibernetinio saugumo mokymai	12. Ar pastarųjų dvejų metų laikotarpyje jūsų įstaigoje vyko mokymai kibernetinio saugumo tema? 13. Kaip vyko mokymai? 14. Ar mokymu metu buvo naudojami praktiniai pavyzdžiai?	Norima išsiaiškinti, ar organizacijose vyksta mokymai kibernetinio saugumo klausimais. Ar gilinamos žinios saugumo temomis.

3 lentelės tęsinys kitame puslapyje

3 lentelės tęsinys

Grupė	Klausimai	Tikslas
Kibernetinio saugumo kultūros suvokimas	15. Ar esate susipažinęs su Bendruoju duomenų apsaugos reglamentu (BDAR)? 16. Ar žinote, kas yra socialinės inžinerijos ataka? 17. Ar esate atsargūs, kai atidarote priedą el. paštu? 18. Ar žinote, kas yra sukčiavimas el. paštu ir kaip jį atpažinti? 19. Ar esate atskleidę kolegai ar vadovui savo slaptažodį, prisijungimui prie sistemų, kai jie to prašė?	Siekiama išsiaiškinti, koks procentas darbuotojų yra susipažinęs su BDAR ir kiek iš jų sugebėtų atpažinti socialinės inžinerijos ataką. Sukčiavimas el.paštu yra vienos svarbiausių sveikatos sektoriaus atakų, o dalijimasis asmeniniais slaptažodžiais didina duomenų saugumo rizikas.
Kibernetinio saugumo kultūros svarba	19. Jūsų nuomone, kibernetinis saugumas aktualus sveikatos priežiūros sektoriuje? 20. Kaip manote, ar yra pakankamai kibernetinio saugumo mokymų, skirtų sveikatos specialistams?	Norima sužinoti pačių darbuotojų nuomonę kibernetinio saugumo svarbos klausimais, nes asmeniniai požiūriai daro įtaką kibernetinės saugumo kultūros vystymuisi.

Tyrimo imtis. Remiantis Sveikatos apsaugos ministerijos 2022 metų duomenimis Lietuvoje veikė 65 ligoninės, pavaldžios SAM ir savivaldybėms, kuriose dirba 45 817 darbuotojų. Tai ir gydytojai, slaugytojos, laboratorijų specialistai, administracijos ir IT darbuotojai bei kitas pagalbinis personalas. Paprastai yra naudojamas 95 proc. patikimumo lygmuo kaip kompromisinis pasirinkimas, užtikrinantis toleruotiną patikimumą bei optimalų imties dydį (Gaižauskaitė ir Mikėnė, 2014). Imties tūrio nustatymui pasirinkta V. I. Paniotto formulė:

$$n = 1/ (\Delta^2 + 1/ N)$$

Čia :

Δ = paklaida ($\Delta = 0,05$) – socialiniuose tyrimuose standartine paklaida laikoma 5 %, kurią gauname su 95 proc. tikimybe;

N = tiriamos visumos skaičius (šiuo atveju 45 817 ligoninių darbuotojų);

n = reikiamų apklausti respondentų (darbuotojų) skaičius. Šiuo atveju – 396 respondentai.

Kiekybinio tyrimo eiga. Kadangi respondentai geografiškai yra skirtinguose miestuose, išsisklaidę po visą Lietuvą, nutarta, kad bus atlikta internetinė anketinė apklausa, pasitelkiant „Google Forms“ internetinės apklausos kūrimo priemonę. Prieš pateikiant anketos nuorodą buvo telefonu susisiekiama su ligoninių administracija, kad padidinti atsakymų lygį. Prieš išsiunčiant anketinės apklausos nuorodą, buvo patikrintas anketos informacijos patikimumas: ta pati anketa pateikiama du kartus tiems patiems žmonėms ir palyginami rezultatai. Anketos klausimyno negalima buvo patvirtinti, jei nors vienas klausimas neatsakytas, todėl visos anketos buvo tinkamos analizei. Kiekybinio tyrimo eiga išdėstyta 4 lentelėje.

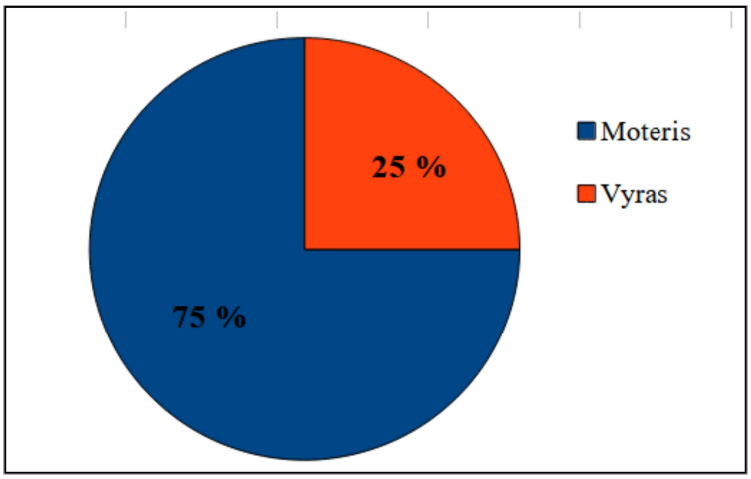
4 lentelė. Kiekybinio tyrimo eiga

Etapas	Etapo veikla	Etapo tikslas
Pasirengimas	Suformuluojamas tyrimo metodas, parengiamas anketinės apklausos klausimynas. Apskaičiuojamas respondentų skaičius. Klausimynas įkeliamas į internetinę platformą ir patikrinamas anketos informacijos patikimumas.	Pasirengti kiekybiniam tyrimui.
Tyrimo vykdymas	Internetinės apklausos nuorodos siuntimas el. paštu ligoninių administracijai. Siekiant padidinti aktyvumą, susisiekiama telefonu su ligoninių administracija ir paskatinama aktyviau dalyvauti.	Surinkti informaciją apie Lietuvos ligoninių darbuotojų suvokimą kibernetinio saugumo kultūros klausimais.
Gautų duomenų analizė	Gautų duomenų sisteminimas. Rezultatų interpretavimas, vertinimas, išvadų pateikimas.	Pateikti tyrimo išvadas.

Duomenų analizės metodai. Anketinės apklausos duomenys buvo apibendrinti statistiniais metodais, taikant *Microsoft Excel* kompiuterinę programą, surinktų duomenų apdorojimui taikyti šie statistinės analizės metodai: aprašomoji statistika, diagramos.

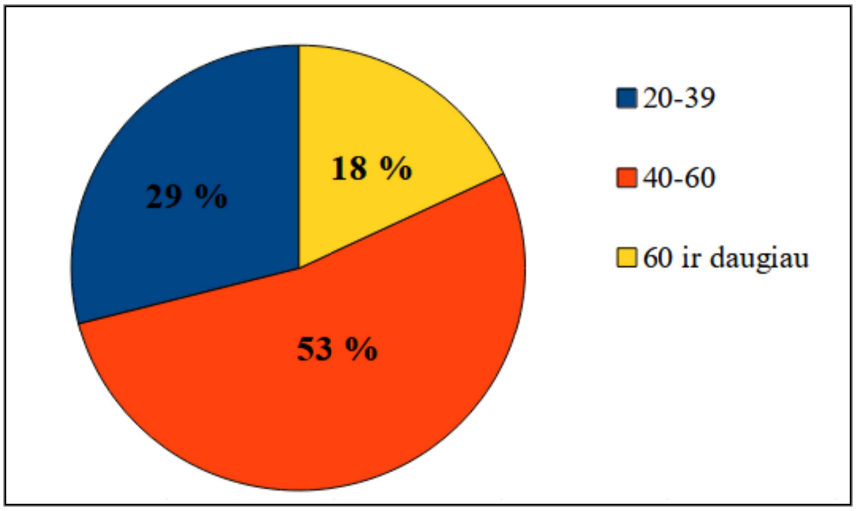
3.3. Kiekybinio tyrimo rezultatai

Kiekybiniame tyrime dalyvavo 398 Lietuvos ligoninių, pavaldžių SAM ir savivaldybėms, darbuotojai. Daugiausia tyrime dalyvavo moterys - 300 (75 %), vyrų buvo 98 (25 %). (9 pav.) Didesnį moterų aktyvumą nulėmė, kad remiantis oficialios statistikos portalo duomenimis, 2021 metais net 83,3% moterų dirba žmonių sveikatos priežiūros ir socialinio darbo srityje. (Oficialus statistikos portalas, 2022)



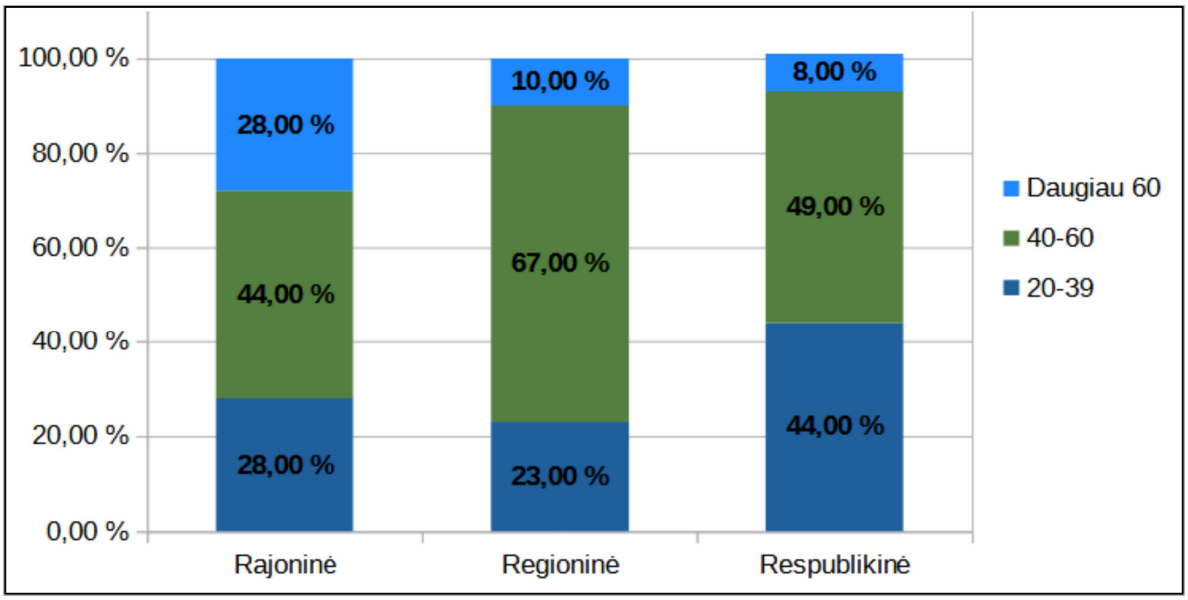
9 pav. Tyrimo dalyvių lytis

Apklausoje buvo pateiktos trys amžiaus grupės, jų pasiskirstymas pateiktas diagramoje. (10 pav.) Daugiausia apklausoje dalyvavo 40-60 metų amžiaus dalyviai – 53 % (211), 20-39 metų – 29 % (115), o 60 metų ir vyresni – 18 % (72) dalyvių.



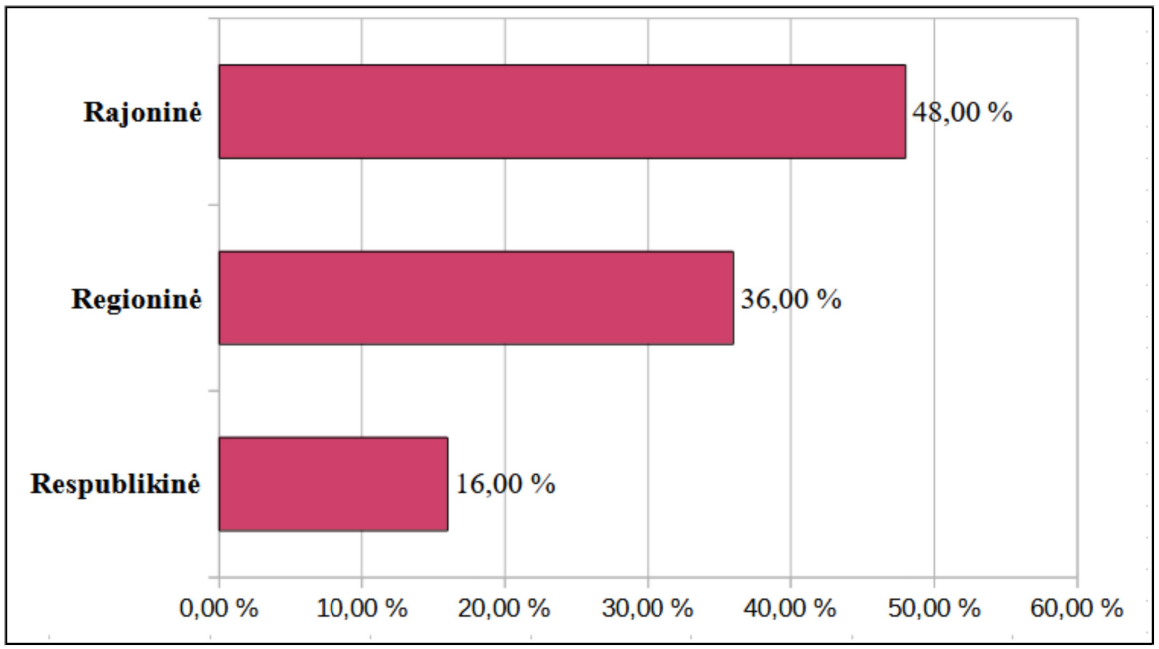
10 pav. Tyrimo dalyvių amžius

Vyresnių nei 60 metų daugiausia dalyvavo rajoninėse ligoninėse, jie sudarė 28% respondentų iš rajoninio lygmens ligoninių, 10 % regioninio ir 8% respublikinio. (11 pav.) Daugiausia 20-39 amžiaus kategorijos dalyvių buvo iš respublikinių ligoninių, tai sudarė 43% visų respublikinio lygmens apklausos dalyvių, rajoninio – 28%, regioninio – 23%.



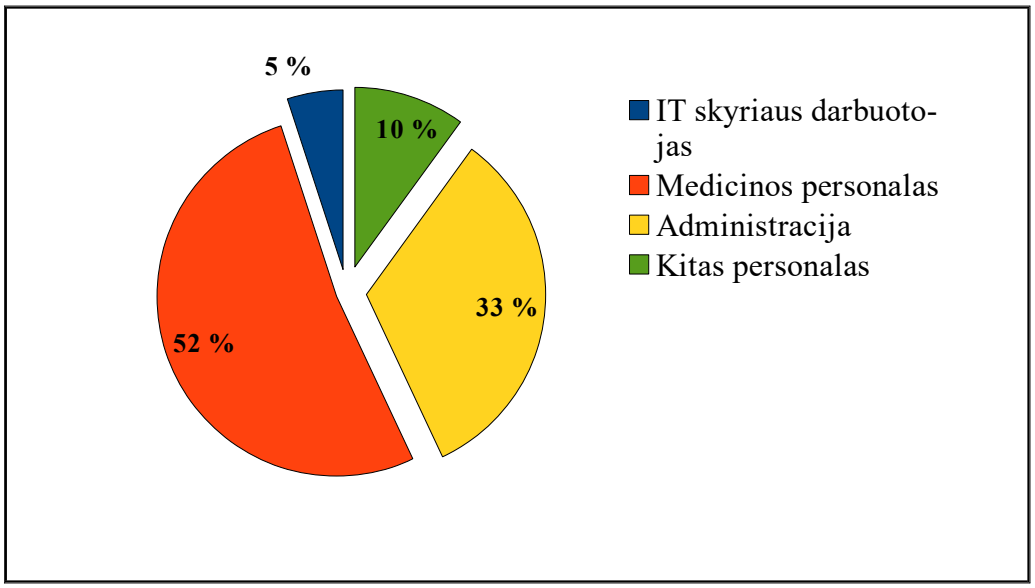
11 pav. Darbuotojų amžiaus pasiskirstymas pagal ligoninių lygmenį

Tyrimo dalyvių buvo prašoma nurodyti ligoninės, kurioje dirba lygmenį, tai 16 % (65) nurodė dirbantis respublikinio lygmens ligoninėje, 36 % (143) regioninio, o 48% (190) dalyvių rajoninio. (12 pav.) Mažą respublikinio lygmens respondentų skaičių nulėmė respublikinių ligoninių atsisakymas dalyvauti apklausoje dėl didelio darbuotojų darbo krūvio.



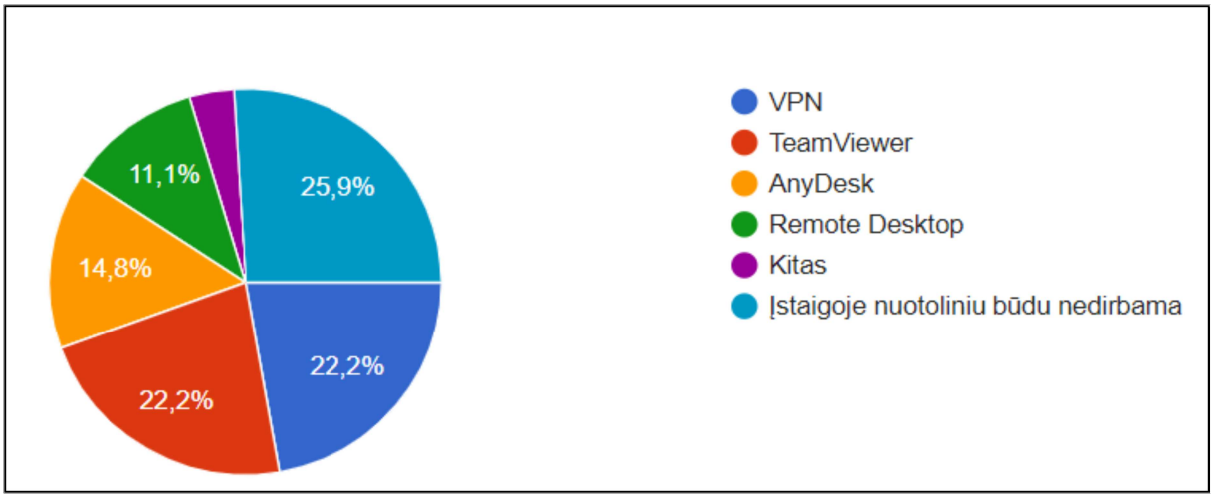
12 pav. Ligoninė, kurioje dirbate, lygmuo

Ketvirtuoju klausimu siekta išsiaiškinti, kokias pareigas užima tyrimo dalyvis. (13 pav.) Buvo išskirtos 4 kategorijos: IT darbuotojai – 19 (5 %), medicinos personalas – 206 (52 %), administracija – 132 (33 %) ir kitas personalas – 41 (10 %). Kaip matoma iš rezultatų daugiausia apklausoje dalyvavo medicinos personalas ir administracijos darbuotojai. IT skyriaus darbuotojų aktyvumas buvo mažas. Daugiausiai IT skyriaus darbuotojų dalyvavo iš rajoninių (N=11) ir regioninių (N=6) ligoninių, respublikinių ligoninių tik 2 respondentai. Mažą IT dalyvių skaičių galėjo nulemti tai, kad IT darbuotojų skaičius įstaigose yra mažas.



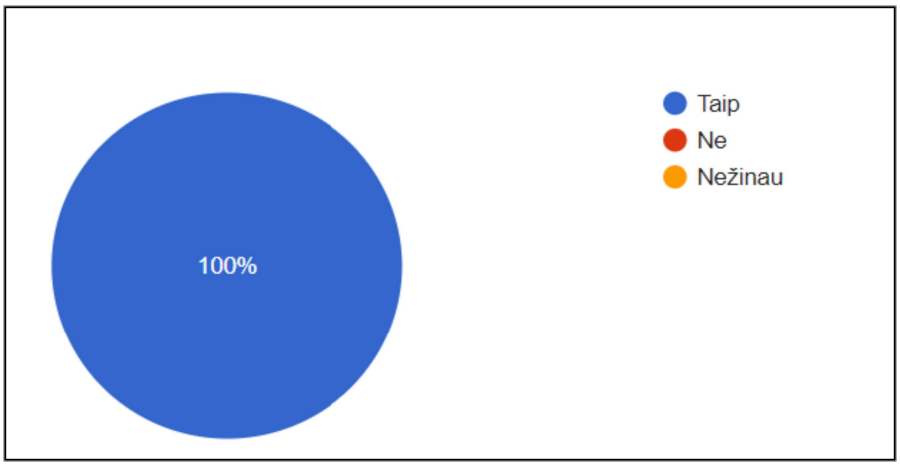
13 pav. Pareigos

Apklausos dalyvis, pasirinkęs IT darbuotojo pareigas, turėjo atsakyti į du papildomus klausimus, kuriuose buvo klausiama, kokius įrankius naudoja nuotoliniam darbui. (14 pav.) Po 22,2 % (po 6) IT darbuotojus nurodė, kad naudoja VPN ir TeamViewer, AnyDesk nurodė 14,8 % (4) ir 11,1 % (3) respondentai pasirinko Remote Desktop. Variantą, kad įstaigoje nuotoliniu būdu nedirbama, pasirinko 25,9 % (7) dalyviai. Galima teigti, kad ligoninėms nuotolinis darbas yra aktualus ir vis dažniau naudojamas, todėl labai svarbu tinkamas įrankių pasirinkimas ir tinkamas saugumo priemonių taikymas, užtikrinant pacientų ir organizacijos duomenų apsaugą.



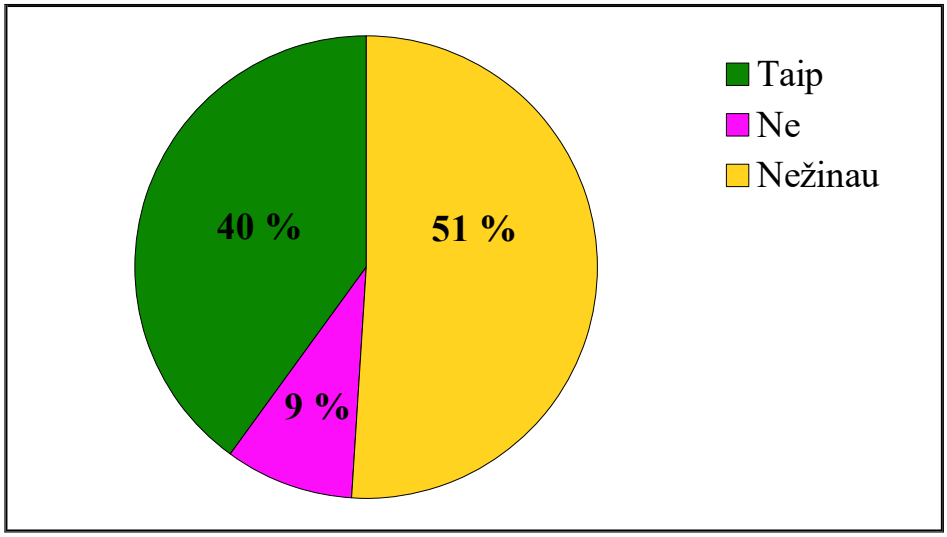
14 pav. Kokius įrankius naudojate nuotoliniam darbui?

Taip pat buvo klausiama, ar ligoninių internetiniam puslapiui naudojami SSL sertifikatai. (15 pav.) 100% nurodė naudojantis SSL sertifikatus, taip užtikrindami interneto svetainės ir pateikiamų duomenų saugumą.



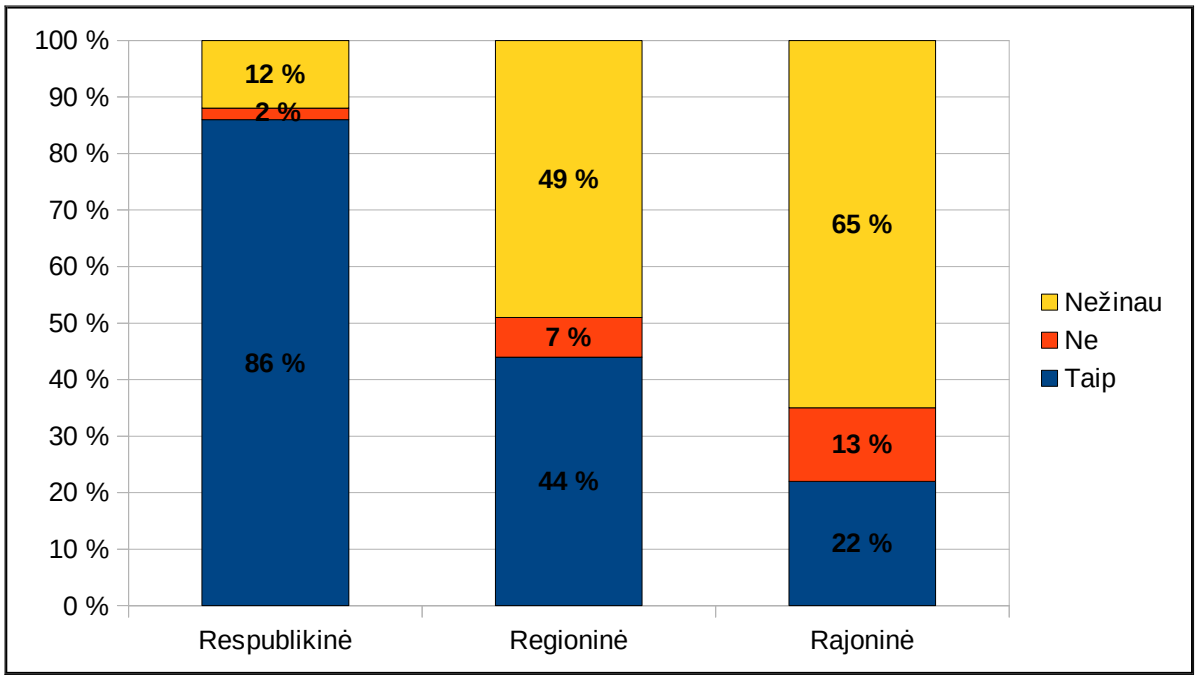
15 pav. Ar jūsų organizacijos internetiniam puslapiui naudojami SSL sertifikatai?

Toliau buvo pateikiami bendri klausimai. Dalyvių buvo klausiama, ar jų organizacijoje egzistuoja kibernetinio saugumo politika. (16 pav.) 40 % (160) dalyvių atsakė taip, 9% (36) teigė, kad jų organizacijose nėra kibernetinio saugumo politikos, o 51 % (202) respondentų nurodė nežinantys, kas leidžia numanyti, kad jei ir egzistuoja kibernetinio saugumo politika, tai tik dokumentuose, kurie nėra įgyvendinami organizacijoje.



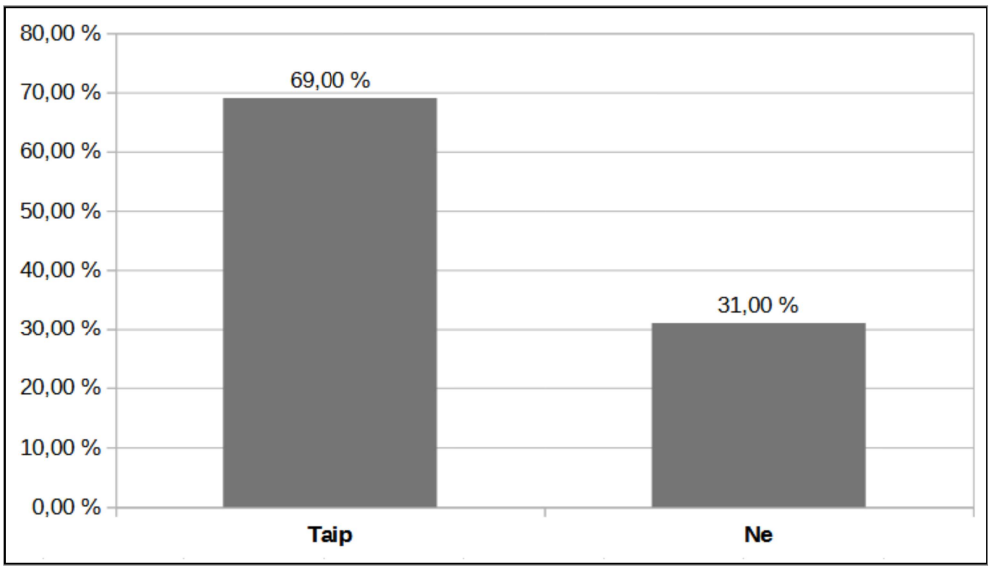
16 pav. Ar jūsų organizacijoje egzistuoja kibernetinio saugumo politika?

Buvo bandoma pastebėti, ar kibernetinio saugumo politikos egzistavimas priklauso nuo ligoninės lygmens. (17 pav.) Akivaizdu, kad respublikinių ligoninių darbuotojai yra informuoti apie kibernetinio saugumo politiką organizacijoje: 86% darbuotojų teigė, kad jų įstaigoje yra kibernetinio saugumo politika; regioninių ligoninių darbuotojų atsakymai pasiskirstė panašiai: 44% - taip, 49 % - nežino. Didesnė dalis rajoninių ligoninių darbuotojų (65%) pažymėjo nežinantys, ar organizacijoje yra kibernetinio saugumo politika, 22% teigė, kad yra, o ne atsakymą pasirinko 13% respondentų. Tai leidžia daryti išvadą, kad respublikinėse ir regioninėse ligoninėse kibernetinio saugumo kultūra yra stipriau įgyvendinama, o rajoninėms ligoninėms trūksta komunikacijos saugumo kultūros įgyvendinimo klausimais, nes jei saugumo politika ir egzistuoja, tai nėra pristatoma visiems darbuotojams.



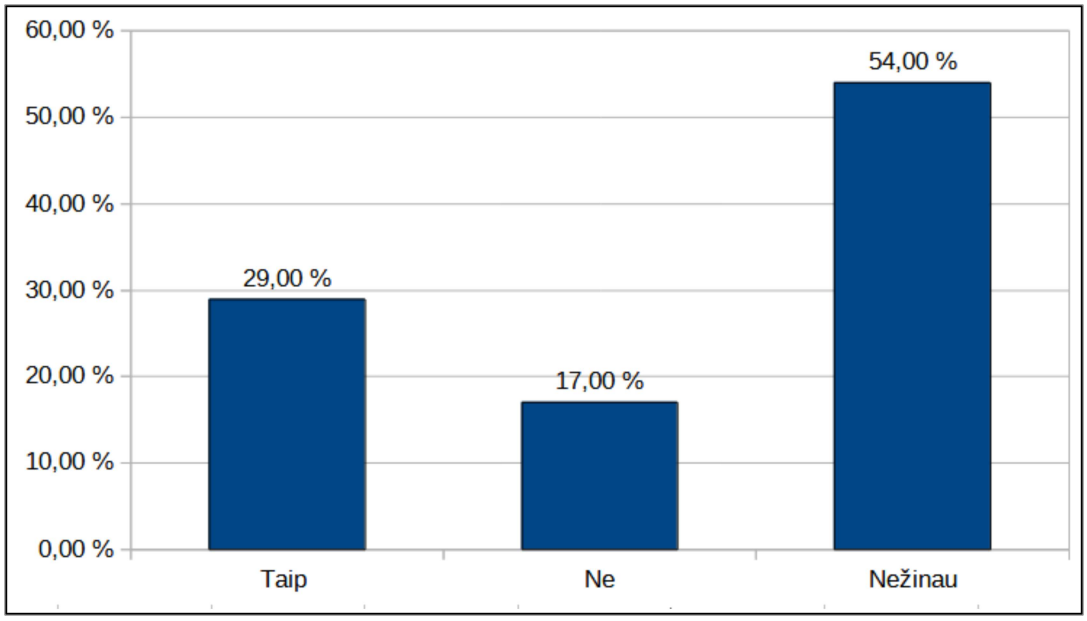
17 pav. Kibernetinio saugumo politikos egzistavimo priklausomybė nuo ligoninės lygmens

Atsakingų už kibernetinį saugumą asmenų žinojimas ir informavimas, padeda greičiau ir efektyviau reaguoti į kibernetinius incidentus, sumažinant kibernetinio incidento poveikį organizacijai. Todėl darbuotojų buvo klausiama, ar žino, kam pranešti įvykus kibernetiniam incidentui, didžioji dalis dalyvių - 273 (69%) teigė žinantys, o 125 (31 %) - nežinantys. (18 pav.) Ne maža dalis darbuotojų dar nežino, kam pranešti apie incidentus, tai kibernetinio incidento atveju prailgintų reagavimo, identifikavimo ir incidento suvaldymo laiką.



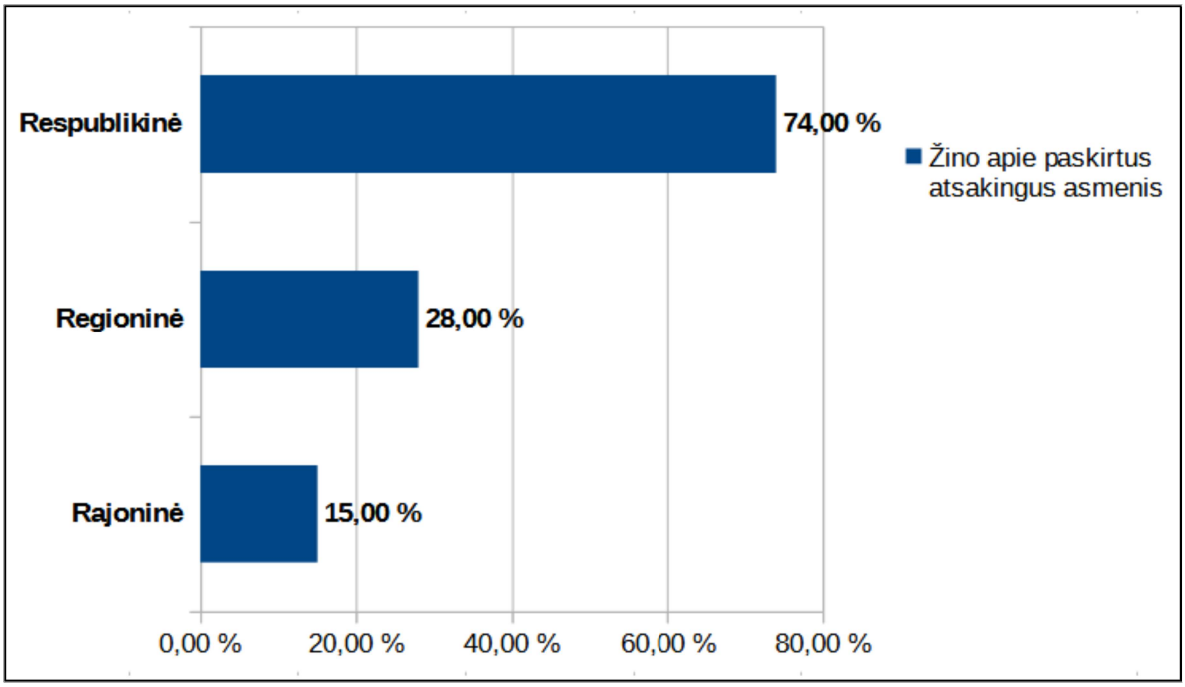
18 pav. Ar žinote, kam pranešti įvykus kibernetiniam incidentui?

Dešimtuoju klausimu, buvo klausiama, ar organizacijoje yra paskirtas asmuo, atsakingas už kibernetinį saugumą, kuris ne tik ruošia saugumo politiką, procedūras, bet dažnai atsakingas ir už mokymų organizavimą. (19 pav.) Teigiamai į šį klausimą atsakė 116 (29 %) dalyvių, ne – 68 (17 %) ir didžiausia dalis 214 (54 %) dalyvių nurodė, kad nežino, ar toks darbuotojas yra, kas leidžia suprasti, kad kibernetinio saugumo kultūros įgyvendinimas nėra efektyvus. Žinios apie atsakingus asmenis, jų vaidmenis ir atsakomybes yra svarbūs veiksniai, įgyvendinantys kibernetinio saugumo kultūrą



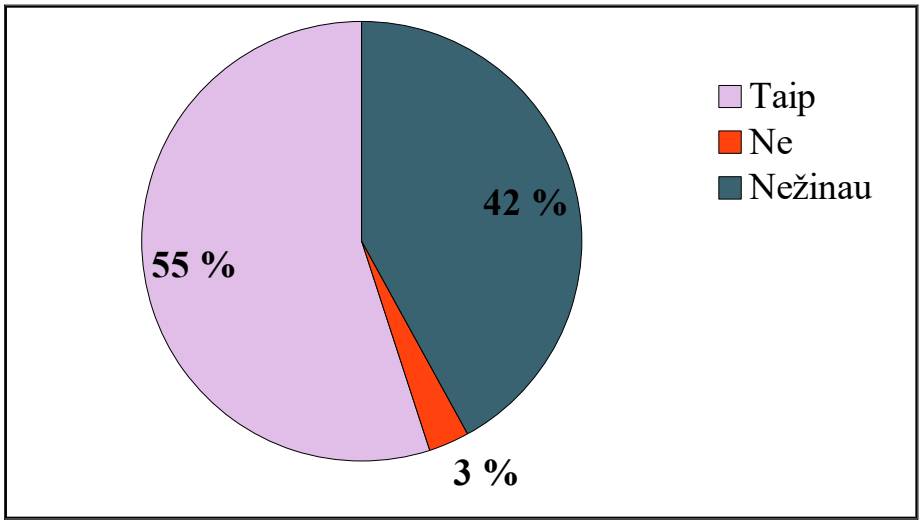
19 pav. Ar Jūsų organizacijoje yra paskirtas asmuo, atsakingas už kibernetinį saugumą?

Panagrinėjus, ar atsakingų asmenų paskyrimą įtakoja ligoninės lygmuo, nustatyta, kad rajoninio lygmens ligoninėse 15% darbuotojų žino apie paskirtus atsakingus asmenis, regioninio lygmens – 28%, respublikinio – 74%, akivaizdu, kad respublikinių ligoninių darbuotojai yra labiau informuoti. (20 pav.)



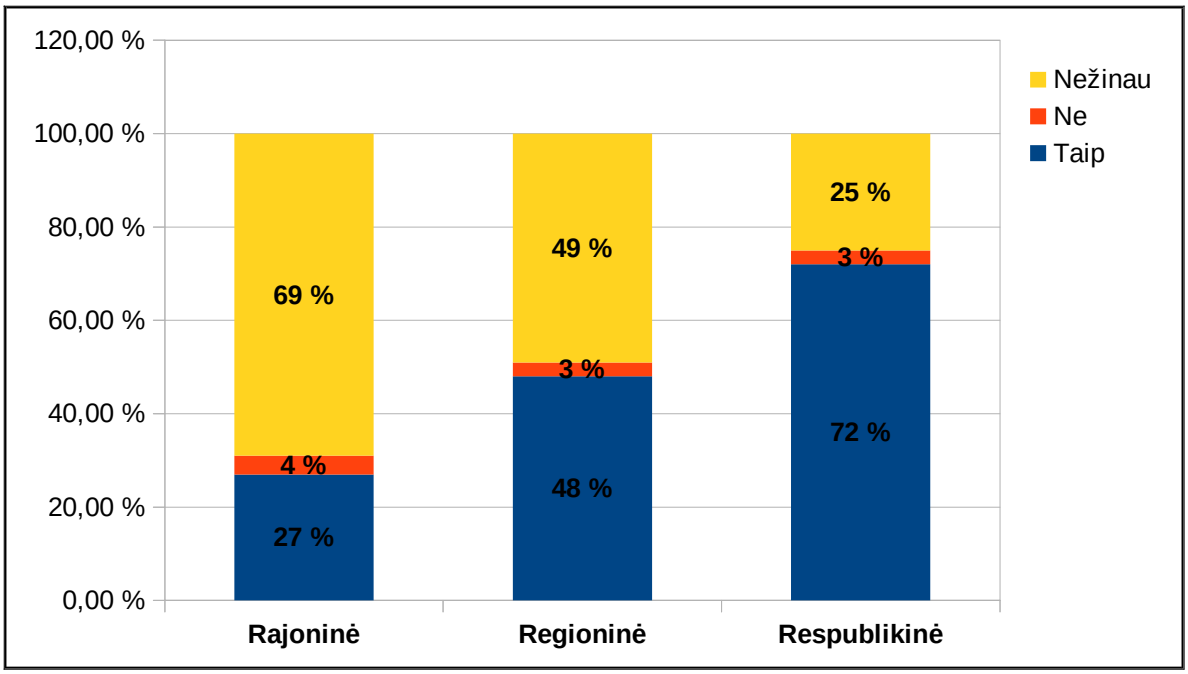
20 pav. Atsakingų asmenų paskyrimas ir ligoninės lygmuo

Kitu klausiamu buvo siekiama išsiaiškinti, ar vadovybė, kaip kertinis kibernetinio saugumo kultūros elementas, rodo pavyzdį darbuotojams, saugumo klausimais, ar jų elgesys ir požiūris leidžia darbuotojams suprasti, kad kibernetinis saugumas yra svarbus jų organizacijoje. (21 pav.) 42% apklausos dalyvių teigė, kad nežino, ar vadovybė supranta kibernetinio saugumo svarbą, atsakymą taip pasirinko 55 % ir ne - 3 % tyrimo dalyvių. Matoma, kad vadovybės palaikymas kibernetinio saugumo klausimais nėra pakankamas.



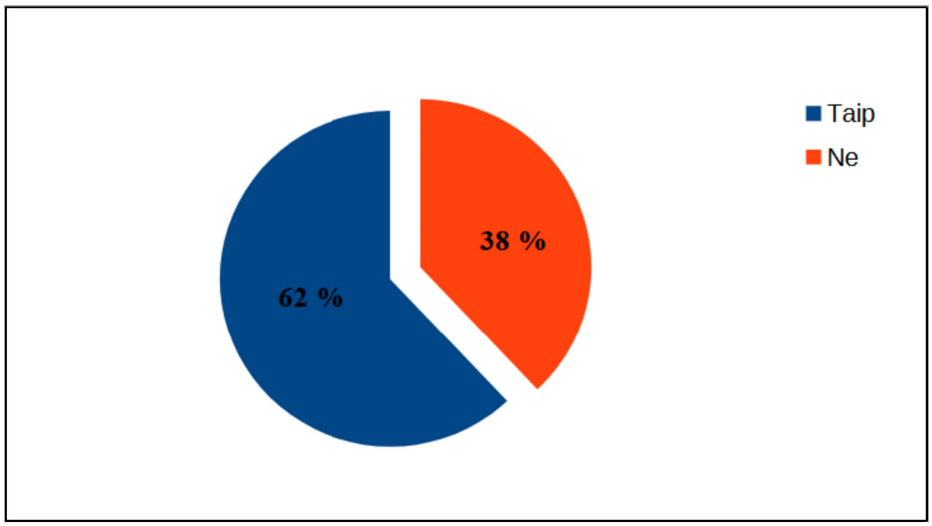
21 pav. Ar ligoninės vadovybė supranta kibernetinio saugumo svarbą ir ją palaiko?

Buvo bandoma pastebėti, ar vadovybės palaikymas kibernetinio saugumo klausimais skiriasi priklausomai nuo ligoninės lygmens.(22 pav.) 72% respublikinių ligoninių darbuotojai žino, kad jų vadovybė suprantą ir palaiko kibernetinio saugumo praktiką, rodo pavyzdį ir darbuotojai neabejoja, kad jų organizacijoje rūpinamasi informacijos saugumu. Regioninų ligoninių – 48%, rajoninių – 27%. Iš rezultatų galima teigti, kad rajoninių ir regioninių ligoninių vadovams reikia aktyviau įsitraukti į kibernetinio saugumo kultūros įgyvendinimą, rodant asmeninį pavyzdį.



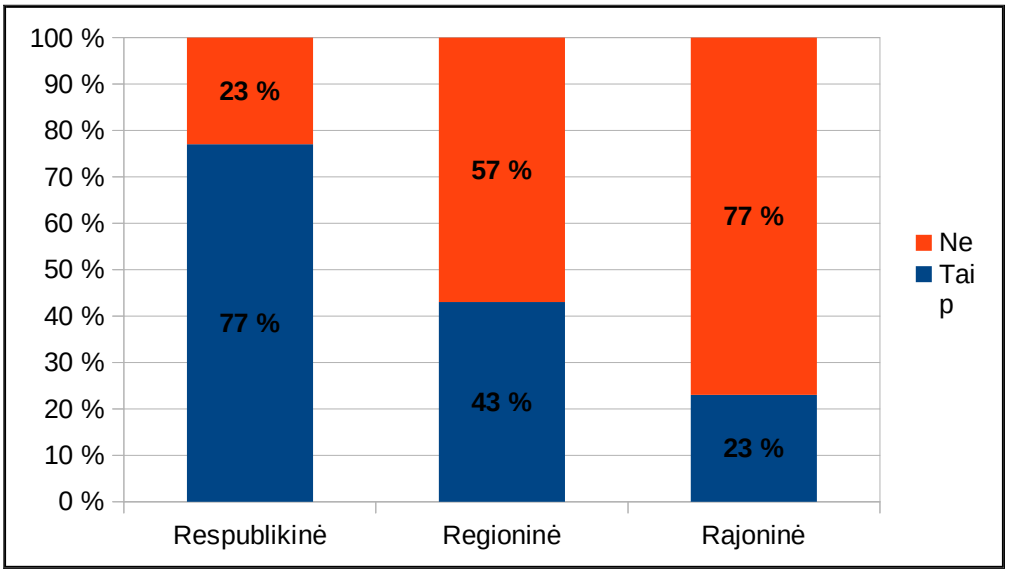
22 pav. Vadovybės palaikymas ir ligoninės lygmuo

Kadangi mokymai kibernetinio saugumo kultūros ekosistemoje yra labai svarbus elementas, skatinantys darbuotojų sąmoningumą, žinių ir įgūdžių stiprinimą, tai apklausos dalyvių buvo klausiama, ar paskutinių dvejų metų laikotarpyje dalyvavo mokymuose, kibernetinio saugumo tema. (23 pav.) Taip atsakė 247 (62%) dalyviai, ne – 151 (38%). Matosi, kad reguliarūs mokymai dar nėra giliai įsišakniję organizacijose arba mokymuose dalyvauja ne visi įstaigos darbuotojai.



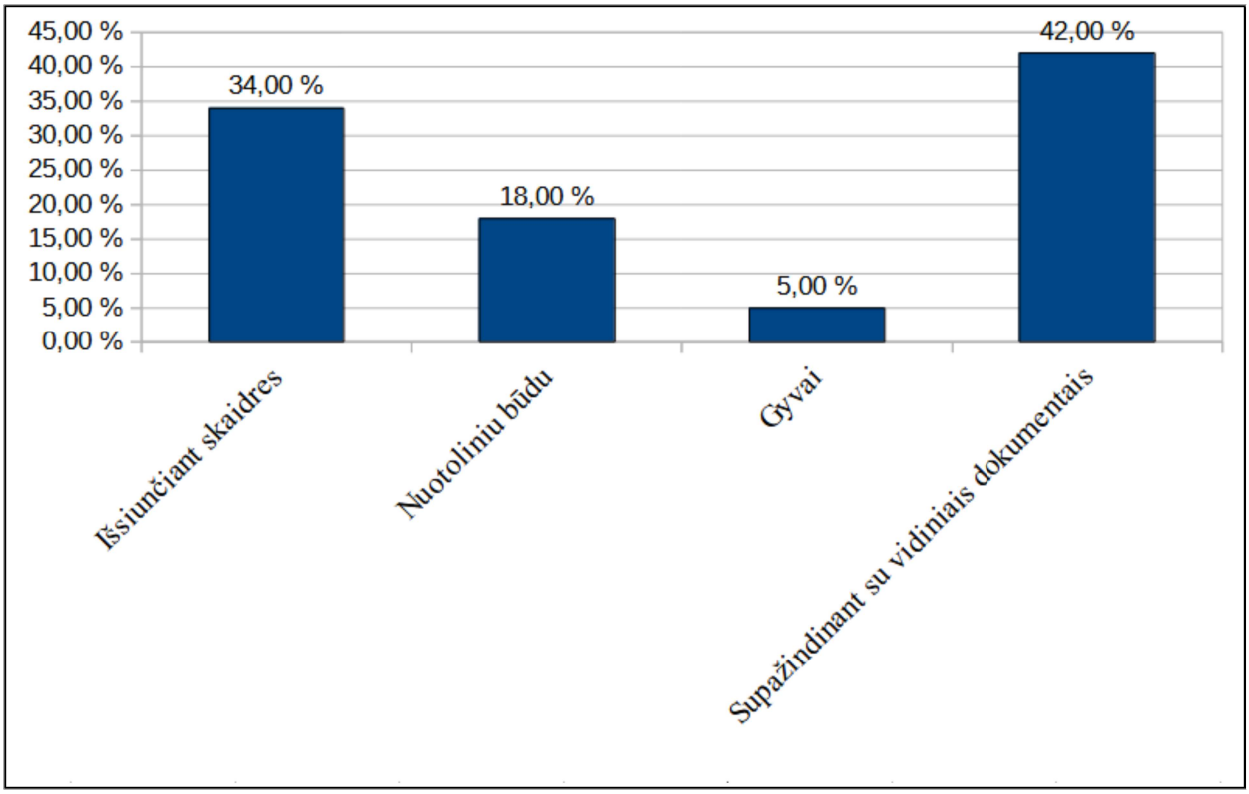
23 pav. Ar pastarųjų dvejų metų laikotarpyje jūsų įstaigoje vyko mokymai kibernetinio saugumo tema?

Buvo bandoma plačiau panagrinėti atsakymus ir pastebėti, kaip skiriasi darbuotojų dalyvavimas mokymuose nuo ligoninių lygmens. (24 pav.) Nustatyta, kad iš respublikinio lygmens ligoninių darbuotojų 77% dalyvių nurodė, kad per paskutinius dvejus metus yra dalyvavę kibernetinio saugumo mokymuose, iš regioninių ligoninių 43% ir rajoninių ligoninių darbuotojų – 23%. Matosi, kad mažiausiai mokymuose yra dalyvavę rajoninio lygmens ligoninių darbuotojai, tai tiesiogiai susiję ir su anksčiau nagrinėtu klausimu, dėl kibernetinio saugumo politikos egzistavimo kur rajoninių ligoninių darbuotojai nežinojo, ar jų organizacijose yra kibernetinio saugumo politikos.



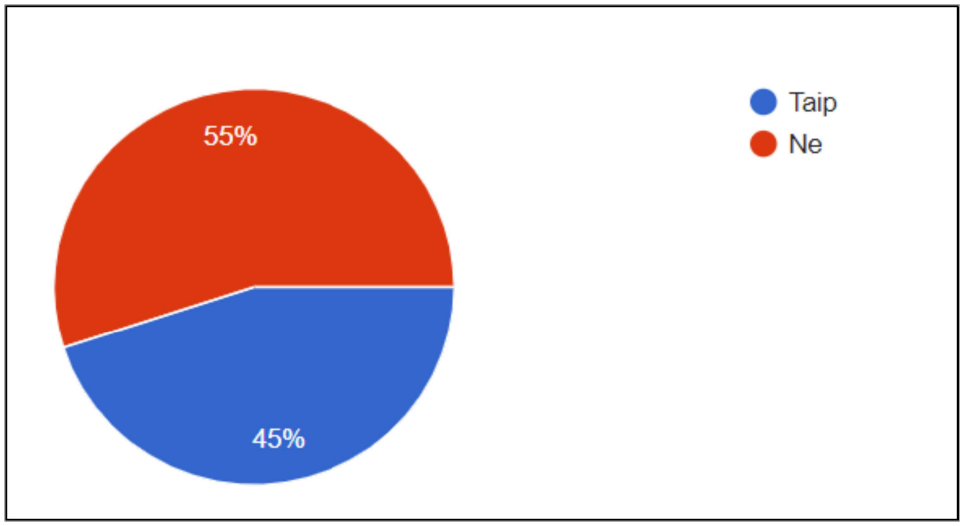
24 pav. Ligoninių lygmuo ir dalyvavimas mokymuose, dvejų metų laikotarpyje

Dalyviams, kurie pastarųjų dvejų metų laikotarpyje dalyvavo kibernetinio saugumo mokymuose, jų buvo 151, prašoma pažymėti, kokia forma vyko mokymai. (25 pav.) 8 (5%) dalyviai teigė, kad mokymuose dalyvavo gyvai, 27 (18%) nuotoliu. Daugiausia dalyvių (42%) pažymėjo, kad jų mokymai apsiribojo tik susipažinimu su vidiniais dokumentais ar tiesiog išsiunčiant skaidres (34%). Supažindinimas su vidiniais dokumentais gali būti nepakankamas būdas kibernetinio saugumo kultūros stiprinimui, turi būti imtasi papildomų veiksmų ir metodų, tokių kaip, kibernetinio saugumo testai ar simuliacijos.



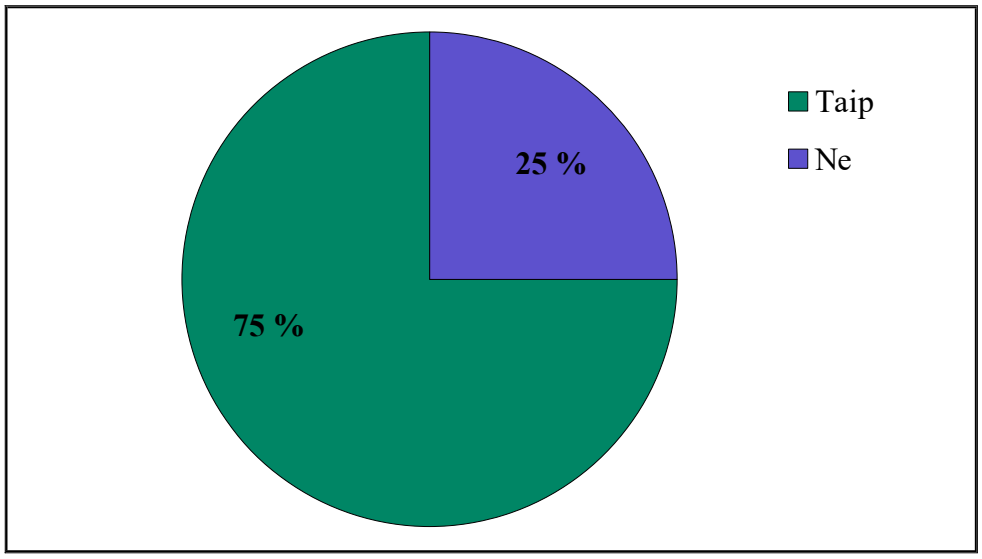
25 pav. Kaip vyko mokymai?

Kibernetinio saugumo mokymai, pasitelkiant praktinius pavyzdžius, yra itin efektyvus būdas didinti darbuotojų žinių lygį ir supratimą apie kibernetines grėsmes, todėl apklausos dalyvių buvo klausiama, ar mokymu metu buvo naudojami praktiniai pavyzdžiai. Atsakymai pasiskirstė panašiai: 68 dalyviai (45%) atsakė taip, o ne atsakė 83 dalyviai (55%). (26 pav.)



26 pav. Ar mokymų metu buvo naudojami praktiniai pavyzdžiai?

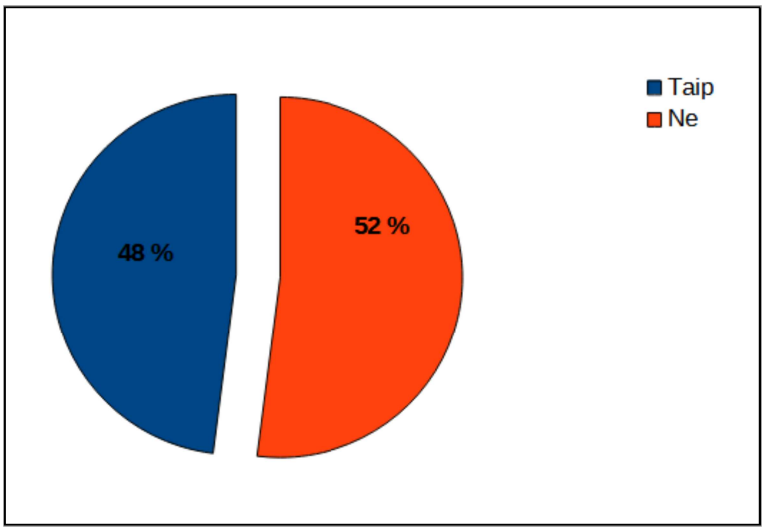
BDAR sveikatos sektoriuje turi labai svarbią reikšmę, užtikrinant duomenų apsaugą, pacientų teises ir skatinant didesnę atsakomybę. Dalyvių buvo klausiama, ar yra susipažinę su BDAR. (27 pav.) 297 dalyvių atsakė taip (75%), ne – 101 (25%). Matoma, kad su BDAR reikalavimais yra susipažinę ligoninių darbuotojai, tikriausiai tam įvykti padėjo duomenų apsaugos darbuotojų paskyrimas ir VDAI aktyvus dalyvavimas, reikalavimų įgyvendinimui.



27 pav. Ar esate susipažinęs su Bendruoju duomenų apsaugos reglamentu (BDAR)?

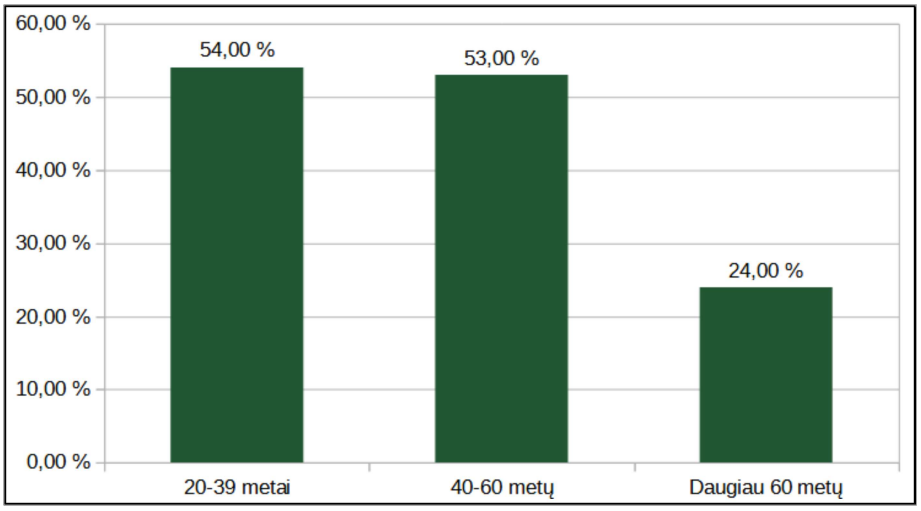
Dėl plataus socialinės inžinerijos metodo naudojimo kibernetiniams nusikaltėliams, dalyvių buvo klausiama, ar žino, kas yra socialinės inžinerijos ataka. (28 pav.) Atsakymai pasiskirstė labai panašiai, nežymiai didesnė dalis respondentų 208 (52%) teigė, kad negalėtų apibūdinti, kas yra

socialinė inžinerija, 190 (48%) dalyviai pažymėjo, kad žino. Labai svarbu, kad darbuotojai turėtų gebėti atpažinti socialinės inžinerijos būdus, taip apsaugodami konfidencialią informaciją ir užtikrindami organizacijos saugumą.



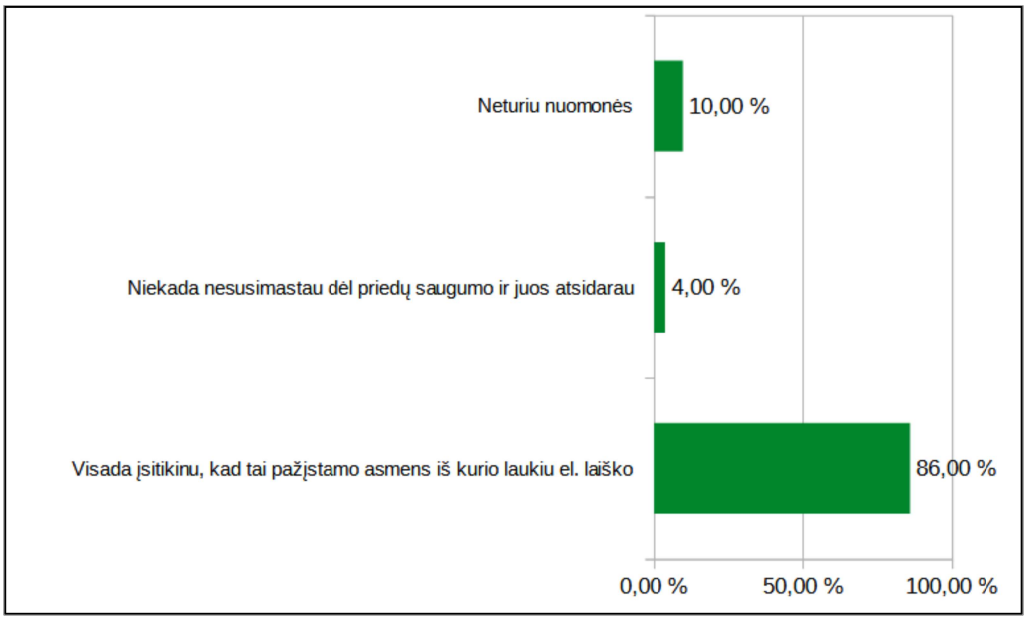
28 pav. Ar žinote, kas yra socialinės inžinerijos ataka?

Buvo bandoma pastebėti, ar yra skirtumas tarp amžiaus kategorijos ir žinių apie socialinės inžinerijos atakas. (29 pav.) 20-39 metų kategorijos darbuotojai 54% žino, kas yra socialinės inžinerijos ataka, 40-60 metų – 53%, 60+ kategorijos – 24%. Taigi vyresni nei 60 metų darbuotojai nežino apie šį atakų metodą ir gali būti jautresni socialinės inžinerijos atakoms dėl mažesnio technologinio išprusimo ir galbūt didesnio pasitikėjimo žmonėmis. Todėl labai svarbu, kad organizacijos padėtų suprasti kibernetinių grėsmių pavojus ir mokytų nuo jų apsisaugoti.



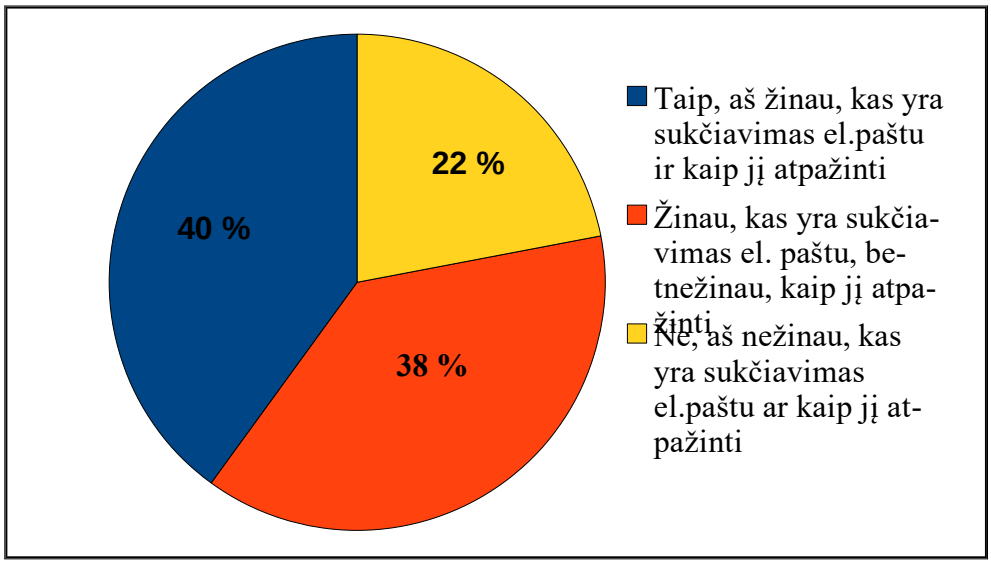
29 pav. Darbuotojų amžius ir žinios apie socialinės inžinerijos atakas

Kadangi el. laiškų priedų saugumas yra svarbus aspektas, užtikrinant duomenų apsaugą. Svarbus darbuotojų sąmoningumas ir žinios, atsidarant el. laiškų priedus, todėl buvo klausiama, ar yra atsargūs, atidarydami priedus el.paštu. (30 pav.) 342 dalyvių (86%) atsakė, kad visada įsitikina, kad tai pažįstamo asmens, iš kurio laukia el. laiško, 15 dalyvių (4 %) niekada nesusimasto dėl priedų saugumo ir juos atsidaro, 41 dalyvis (10%) teigė neturintis nuomonės šiuo klausimu. Darbuotojai šiuo klausimu yra atsargūs ir sąmoningi.



30 pav. Ar esate atsargūs, kai atidarote priedą el. paštu?

Kitu klausimu buvo siekiama sužinoti, ar apklausos dalyviai žino, kas yra sukčiavimas el. paštu ir kaip ji atpažinti. (31 pav.) 159 dalyviai (40%) pažymėjo, kad žino ir gali atpažinti sukčiavimą el. paštu, 151 (38%) - žino, kas tai yra, bet nežino, kaip atpažinti, o 88 respondentai (22%) teigė, kad nežino apie sukčiavimą el. paštu ir negalėtų jo atpažinti. Šis klausimas labai susijęs, su anksčiau nagrinėtų, kur buvo klausiama ar žino, kas yra socialinės inžinerijos ataka, nes vienas iš socialinės inžinerijos metodų yra „phishing“- sukčiavimas el. laiškais. Todėl žinios apie socialinės inžinerijos atakas ir jos metodus, leistų pažinti ir sukčiavimą el. paštu bei išlikti budriems. Mokymai vienas iš būdų, didinti darbuotojų žinias ir gebėjimą atpažinti sukčiavimą el. paštu.



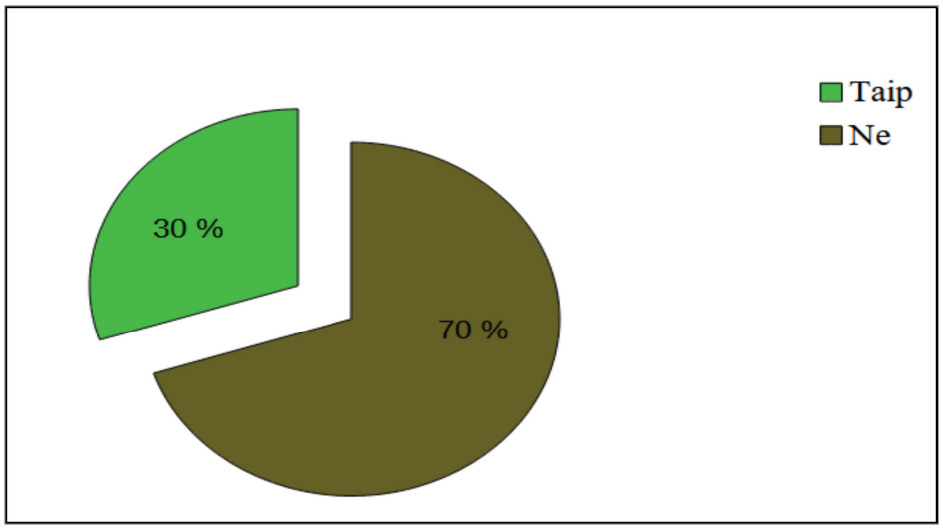
31 pav. Ar žinote, kas yra sukčiavimas el. paštu ir kaip jį atpažinti?

Atsakymą „Taip, aš žinau, kas yra sukčiavimas el.paštu ir kaip jį atpažinti“ buvo bandoma panagrinėti plačiau ir pažiūrėti, ar šiam atsakymui įtakos gali turėti amžius ir ligoninės lygmuo (5 lentelė). Atsižvelgiant į amžiaus kategoriją, tai daugiausia 40-60 metų darbuotojai 57% žino, kas yra sukčiavimas el.paštu ir kaip jį atpažinti, 20-39 metų – 34%, mažiausiai: virš 60 metų darbuotojai – 9%. Pagal ligoninės lygmenį, tai respublikinio lygmens ligoninių darbuotojai (71%) žino ir gebėtų atpažinti sukčiavimą el. paštu, 38% regioninių ir nežymiai mažiau – 31% rajoninių ligoninių darbuotojai. Šiam klausimui įtakos galėjo turėti tai, kad daugiausia vyresnių nei 60 metų dalyvių buvo iš rajoninio lygmens ligoninių.

5 lentelė. Žino, kas yra sukčiavimas el. paštu ir kaip jį atpažinti pasiskirstymas pagal kategorijas

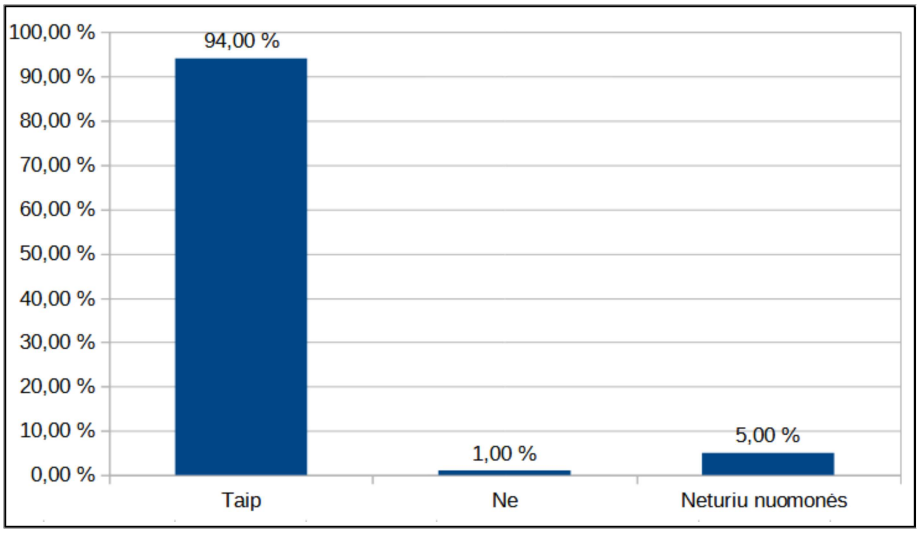
Kategorija		**Žino, kas yra sukčiavimas el. paštu ir kaip jį atpažinti (%)**
Amžius	20-39 metų	34
	40-60 metų	57
	60+ metų	9
Ligoninės lygmuo	Respublikinė	71
	Regioninė	38
	Rajoninė	31

Kadangi dalijimasis slaptažodžiais didina saugumo rizikas, dalyvių buvo klausiama, ar yra atskleidę savo slaptažodį, prisijungimams prie sistemų, kolegai ar vadovui. (32 pav.) Didžioji dalis 279 dalyviai (70%) pažymėjo atsakymą ne, 119 dalyvių (30%) - taip, kas kelia didelę riziką duomenų saugumui. Mokymai vienas iš būdų informuoti darbuotojus apie rizikas, dalijantis slaptažodžiais.



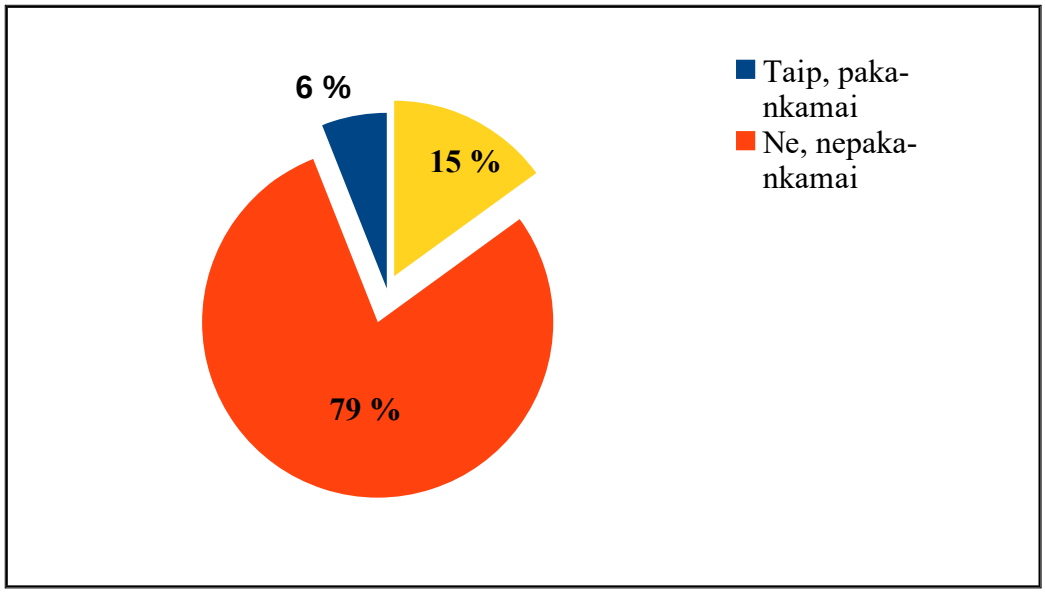
32 pav. Ar esate atskleidę kolegai ar vadovui savo slaptažodį, prisijungimams prie sistemų, kai jie to prašė?

Kitu klausimu buvo siekiama sužinoti dalyvių nuomonę, dėl kibernetinio saugumo svarbos, sveikatos priežiūros sektoriuje. (33 pav.) Net 94% (373) dalyvių atsakė, kad kibernetinis saugumas yra aktualus sveikatos sektoriuje, ne - 1% (6) respondentų, o neturi nuomonės 5% (19) dalyvių. Ligoninių darbuotojai supranta, kad kibernetinis saugumas yra labai aktualus sveikatos sektoriuje, dėl šio sektoriaus tvarkomų duomenų jautrumo.



33 pav. Jūsų nuomone, kibernetinis saugumas aktualus sveikatos priežiūros sektoriuje?

Paskutiniu klausimu buvo siekiama sužinoti apklausos dalyvių nuomonę, ar yra pakankamai kibernetinio saugumo mokymų, skirtų sveikatos specialistams. (34 pav.) Tik 26 dalyviai (6 %) teigė, kad mokymų yra pakankamai, daugiausia dalyvių - 314 (79%) pažymėjo, kad mokymų nėra pakankamai, o nuomonės šiuo klausimu neturėjo 58 respondentai (15%). Dalyvių nuomone, mokymų trūksta, todėl kursų ir mokymų rengėjai, galėtų atsižvelgti ir pasiūlyti mokymus, pritaikytus sveikatos sektoriaus darbuotojams. Apžvelgus mokymo platformas, skirtas sveikatos specialistams, pasigendama temų susijusių su kibernetiniu saugumu.



34 pav. Kaip manote, ar yra pakankamai kibernetinio saugumo mokymų, skirtų sveikatos specialistams?

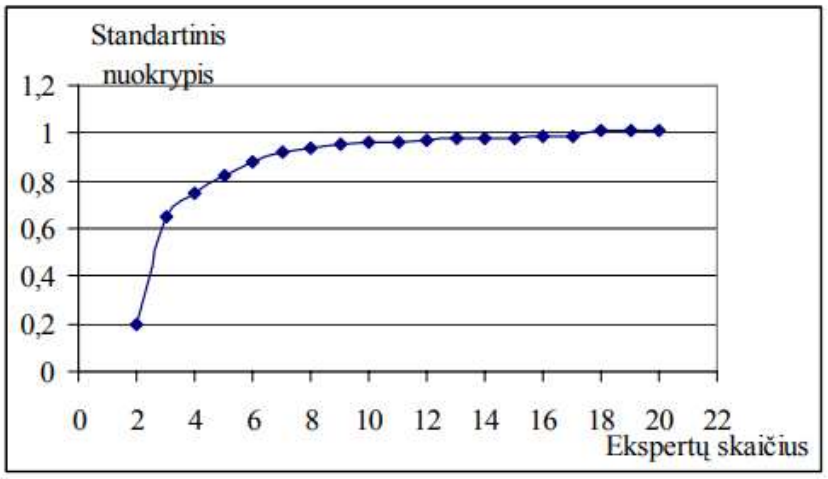
Atlikus kiekybinę apklausą internetu nustatyta, kad didesnė dalis ligoninių darbuotojų nežino, ar jų organizacijoje yra kibernetinio saugumo politika, ar yra paskirti atsakingi asmenys, nežino vadovybės požiūrio kibernetinio saugumo klausimais, kas leidžia suprasti, kad yra nepakankamas vadovų dėmesys kibernetinio saugumo kultūrai. Ne visose įstaigose vykdomi reguliarūs mokymai arba ne visi darbuotojai juose dayvauja, todėl nemaža dalis darbuotojų nežino apie socialinę inžineriją ar kaip atpažinti sukčiavimą el.paštu. Teorinėje dalyje buvo pristatyta, kad būtent kibernetinio saugumo politikos, vadovybės rodomas pavyzdys, reguliarūs mokymai yra pagrindiniai elementai, leidžiantys įgyvendinti kibernetinio saugumo kultūrą organizacijose. Su BDAR nuostatomis ir reikalavimais yra susipažinusi didžioji dalis darbuotojų, tai užtikrina, kad jautrūs pacientų duomenys tvarkomi laikantys reikalavimų. Dauguma apklausos dalyvių supranta, kad kibernetinio saugumo kultūra svarbi sveikatos sektoriuje, bet pripažįsta, kad mokymų skirtų sveikatos specialistams yra nepakankamai. Pastebėtas skirtumas tarp ligoninių lygmens:

respublikinių ligoninių darbuotojai geriau informuoti apie kibernetinio saugumo politikas, daugiau žino apie socialinę inžineriją ir geriau gebą atpažinti sukčiavimą el. paštu.

3.4. Kokybinio tyrimo organizavimas.

Kokybinio tyrimo organizavimas. Tyrimui pasirinktas ekspertinis interviu el.paštu. Interviu el. paštu pasirinktas ne tik dėl kiekvienai šaliai asmeniškai patogaus laiko, bet ir dėl geografiškai nutolusių dalyvių ir tyrimo dalyvių užimtumo. (Gaižauskaite ir Valavičiene, 2016)

Tyrimo imtis parengta vadovaujantis metodologinėmis prielaidomis, suformuluotomis klasikinėje testų teorijoje, kurioje teigiama, jog agreguotų sprendimų patikimumą ir priimančių sprendimą (šiuo atveju ekspertų) skaičių sieja greitai gęstantis netiesinis ryšys. Libby ir Blashfield (1978) įrodė, jog agreguotų ekspertinių vertinimų moduliuose su vienodais svoriais nedidelės ekspertų grupės sprendimų ir vertinimų tikslumas nenusileidžia didelės ekspertų grupės sprendimų ir vertinimų tikslumui. (35 pav.)



Šaltinis: Libby ir Blashfield, 1978

35 pav. Ekspertų vertinimų standartinio nuokrypio priklausomybė nuo ekspertų skaičiaus

Tai reiškia, kad kai ekspertų skaičius didesnis nei 9, vertinimo tikslumas daugiau nei 90%, o toliau didėjant ekspertų skaičiui, tikslumas didėja nežymiai. Tyrimui buvo pasirinkti 9 ekspertai iš skirtingo lygmens ligoninių.

Imties sudarymui pasirinkta kriterinė atranka, kai pats tyrėjas nusprendžia, kokiais kriterijais vadovautis, atrenkant respondentus. Interviu dalyviai buvo atrinkti pagal ligoninių lygmenį: respublikinis, regioninis, rajoninis. Siekiant apimti didesnę Lietuvos teritoriją ir gauti tikslius duomenis, buvo pasirinktos ligoninės iš skirtingų apskričių. Buvo atsižvelgta į ekspertų patirtį, kad

vadovaujamo darbo patirtis ne mažiau penki metai, o šiuo metu vadovauja įstaigai ne mažiau kaip dveji metai. Dvejų metų vadovavimo patirtis dabartinėje gydymo įstaigoje pasirinkta dėl to, kad per šį laikotarpį jau realu įgyvendinti kibernetinio saugumo kultūros plėtrą, vadovaujamoje organizacijoje.

Tyrimo etika. Interviu buvo laikomasi Gaižauskaitės ir Valavičienės (2016) aprašytų svarbiausių interviu tyrimo etikos principų, kai tyrimo dalyviai turi galimybę pasirinkti dalyvauti ar atsisakyti dalyvauti tyrime, suteikti tyrimo dalyviui informacijos apie vykdomą tyrimą, rūpintis tyrimo dalyvių saugumu bei užtikrinti tyrimo dalyvio anonimiškumą, konfidencialumą ir privatumą. Tyrimo dalyviai dalyvavo savo valia ir savanoriškai. Tyrime nėra atskleidžiami tyrimo dalyvių vardai ir pavardės, tik apskritis, ligoninės lygmuo ir interviu dalyvio vadovaujamo darbo patirtis, todėl tyrimo dalyviams buvo priskirti kodai. (žr. 6 lent.)

6 lentelė. Kokybinio tyrimo dalyvių grupė

Kodas	Apskritis	Ligoninės lygis	Vadovaujamo darbo patirtis	Vadovauja įstaigai
L01	Alytaus	Respublikinė	39 metai	21 metus
L02	Šiaulių	Respublikinė	8 metai	2 metai
L03	Vilniaus	Respublikinė	26 metai	5 metai
L04	Vilniaus	Regioninė	11 metų	11 metų
L05	Telšių	Regioninė	22 metai	6 metus
L06	Tauragės	Rajoninė	14 metų	6 metus
L07	Šiaulių	Rajoninė	19 metų	3 metus
L08	Utenos	Rajoninė	9 metai	9 metai
L09	Kauno	Rajoninė	10 metų	10 metų

Kokybinio tyrimo eiga. Pagal išsikeltus kriterijus buvo atrinkti tyrimo dalyviai. El. paštu buvo siunčiami laiškai su prisistatymu, tyrimo tikslais ir prašoma atsakyti į pateiktus klausimus. Dalyviui atsisakius dalyvauti tyrime, pasirenkamas kitas, atsižvelgiant į iškeltus kriterijus. Kokybinio tyrimo eiga pateikta 7 lentelėje.

7 lentelė. Kokybinio tyrimo eiga

Etapas	Etapo veikla	Etapo tikslas
Pasirengimas	Suformuluojamas tyrimo metodas, atliekama dalyvių atranka, pagal nustatytus kriterijus	Pasirengti kokybiniam tyrimui.
Tyrimo vykdymas	El. paštu susisiekiama su tyrimo dalyviais, supažindinama su tyrimo tikslais, atliekamas interviu el. paštu.	Išsiaiškinti kaip ligoninių vadovai supranta kibernetinio saugumą kultūrą ir kaip skatina jos stiprinimą ir plėtrą.
Gautų duomenų analizė	Gauta informacija yra analizuojama ir apibendrinama.	Pateikti tyrimo išvadas.

Tyrimo dalyvių apklausos analizė. Kokybiniam interviu buvo sudaryti 9 klausimai.

1. Jūsų nuomone, kas yra kibernetinio saugumo kultūra?
2. Jūsų nuomone, kokią naudą teikia kibernetinio saugumo kultūra organizacijai?
3. Ar įstaigoje investuojate į kibernetinį saugumą? Esate nusimatę papildomas išlaidas kibernetinio saugumo stiprinimui?
4. Ar jūsų įstaigoje vyksta mokymai susiję su asmens duomenų apsauga ar kibernetinio saugumo tema? Jei taip, tai kokia forma?
5. Ar Jūsų įstaigoje yra kibernetinio saugumo politika?
6. Ar Jūsų įstaigoje yra atsakingas asmuo už kibernetinį saugumą?
7. Kaip skatinate kibernetinio saugumo kultūrą?
8. Kaip manote, ar kibernetinio saugumo kultūra yra svarbi sveikatos sektoriui?
9. Kaip manote, ar reikėtų kibernetinio saugumo mokymus įtraukti į privalomus sveikatos specialistų mokymus?

Duomenų analizės metodai. Kokybinio tyrimo duomenys analizuoti pasitelkiant turinio (angl. *content*) analizės metodą.

3.5. Kokybinio tyrimo rezultatai

Atlikus kokybinį tyrimą, nagrinėjami respondentų atsakymai į klausimus.

1. Jūsų nuomone, kas yra kibernetinio saugumo kultūra?

Respondentai L02 ir L07 teigė, kad kibernetinio saugumo kultūra yra organizacijos kolektyvinis požiūris į kibernetinį saugumą. L03 kibernetinio saugumo kultūrą apibūdino, kaip visų organizacijos narių samoningumą, atsakomybę ir įsipareigojimą laikytis saugumo praktikų ir principų. L04 nuomone, kibernetinio saugumo kultūros sąvoka ”apima žinių, įgūdžių ir elgesio modelių formavimą įstaigoje.” Ir išskyrė svarbius aspektus: darbuotojų informavimas apie grėsmes ir galėjimas jiems prisidėti prie bendro įstaigos saugumo užtikrinimo. Du dalyviai nurodė, kad kibernetinio saugumo kultūra, tai darbuotojų elgesys skaitmeninėje erdvėje, L09 – “tai kompleksas priemonių, kurių turi imtis vadovas, kad įstaiga jaustųsi saugiau skaitmeninėje erdvėje.” Tai vienintelis dalyvis, kuris išskyrė vadovybės svarbą kibernetinio saugumo kultūroje.

2. Jūsų nuomone, kokią naudą teikia kibernetinio saugumo kultūra organizacijai?

Keturi respondentai nurodė reputacinę naudą organizacijai, vienas iš jų (L04) dar išskyrė šias pagrindines naudas: didinamas saugumas, sumažinamas rizikos veiksnys, efektyvesnis incidentų valdymas ir įstaigos veiklos užtikrinimas. L05 teigė, kad kibernetinio saugumo kultūra apsunkina sąlygas kibernetiniams nusikaltėliams pakenkti jų įstaigai. L09 nurodė, kad kibernetinio incidento padariniai gali būti itin skaudūs ir rašė, kad kibernetinio saugumo kultūros nauda yra „*...efektyviai ir laiku identifikuojant kibernetinius incidentus, užkertant kelią jų atsiradimui ir plitimui, valdant kibernetinių incidentų sukeltas pasekmes, užtikrinti galimybę ligoninės personalui saugiai naudotis informacinių ir ryšių technologijų teikiamomis galimybėmis*.“

3. Ar įstaigoje investuojate į kibernetinį saugumą? Esate nusimatę papildomas išlaidas kibernetinio saugumo stiprinimui?

Šeši iš devynių interviu dalyvių teigė investuojantis į kibernetinio saugumo stiprinimą. L05 rašė, kad ruošiasi TIS2 direktyvos įgyvendinimui. Trys respondentai teigė neturintys tam papildomų lėšų. L03 teigė, kad yra įsipareigoję rasti pusiausvyrą tarp būtinų saugumo priemonių įgyvendinimo ir esamų biudžeto apribojimų, nes supranta, kad kibernetinis saugumas gyvybiškai svarbus jų organizacijai

4. Ar jūsų įstaigoje vyksta mokymai susiję su asmens duomenų apsauga ar kibernetinio saugumo tema? Jei taip, tai kokia forma?

Septyni dalyviai nurodė, kad mokymai, susiję su asmens duomenų apsauga ar kibernetinio saugumo tema, vyksta. L03 vykdo reguliarius mokymus, kurie vyksta gyvai ir nuotoliu. L05 ir L09 dalyvauja NKSC vykdomose mokymuose ir pratybose, L01 nurodė, kad mokymai vyksta su KVTC.

Vienas dalyvis teigė, kad mokymai nevyksta, o dar vienas – kad labai retai. L02 ir L04 teigė vykdantys simuliacinius testavimus.

5. Kaip skatinate kibernetinio saugumo kultūrą?

Du dalyviai teigė neskatinantys kibernetinio saugumo kultūros. L02 dalyvis rašė, kad kibernetinio saugumo kultūrą skatina dviem lygmenimis: IT skyriaus ir visos organizacijos lygmeniu. L03 „...įgyvendina saugumo ambasadorių programą, kurioje saugumo lyderiai padeda skleisti žinią apie svarbius saugumo klausimus.“ Darbuotojų nuolatinį žinių atnaujinimą, kaip kibernetinio saugumo kultūros skatinimą, nurodė penki dalyviai. L04 dalyvis išvardino šešis būdus, kaip skatina saugumo kultūrą: *1. Reguliarūs mokymai ir testavimai; 2. Simuliacijos; 3. Priminimų ir informacinių pranešimų siuntimai; 4. Saugumo komiteto/tarybos sudarymas, dokumentų reguliarios peržiūros ir atnaujinimai, saugumo dokumentų patikrinimai ir kitų numatytų metodų taikymai; 5. Kibernetinių atakų vykdymai; 6. Darbuotojų įsipareigojimai pagal priskirtus prioritetus ir atsakomybes.*

6. Ar Jūsų įstaigoje yra kibernetinio saugumo politika?

Šeši respondentai teigė turintys kibernetinio saugumo politikas, du – ne, o vienas dalyvis pabrėžė, kad kibernetinio saugumo politikos neturi, bet turi apsirašę asmens duomenų tvarkymo taisykles. L03 detalizavo, kad jų kibernetinio saugumo politikoje yra apibrėžti saugumo tikslai, procedūros, atsakomybės ir elgesio standartai, nustatyti būdai, kaip valdyti ir reaguoti į kibernetinius incidentus.

7. Ar Jūsų įstaigoje yra atsakingas asmuo už kibernetinį saugumą?

Aštuoni dalyviai nurodė turintys asmenis, atsakingus už kibernetinį saugumą, vienas dalyvis – ne. L03 teigė, kad toks asmuo jų organizacijoje yra atsakingas už saugumo politikos įgyvendinimą, saugumo rizikų ir incidentų valdymą, mokymų koordinavimą.

8. Kaip manote, ar kibernetinio saugumo kultūra yra svarbi sveikatos sektoriui?

Visi interviu dalyviai teigė, kad kibernetinio saugumo kultūra yra svarbi sveikatos sektoriui. L04 pabrėžė, kad ne tik svarbi, bet ir privaloma. L05 teigė, kad tai svarbu visiems sektoriams, ne tik sveikatos. L03 plačiau išreiškė savo nuomonę: *„Kibernetinio saugumo kultūra yra nepaprastai svarbi sveikatos sektoriui, nes šis sektorius tvarko itin jautrius ir gyvybiškai svarbius duomenis. Sveikatos priežiūros įstaigos kasdien rūpinasi pacientų sveikatos informacija, įskaitant asmens tapatybę, medicinos istoriją ir kitus duomenis, kurie, patekę į netinkamas rankas, gali sukelti didžiulę žalą paciento privatumui ir netgi gyvybei. Be to, sveikatos sektoriuje vykdomos operacijos ir teikiamos paslaugos dažnai yra gyvybiškai svarbios, todėl bet koks sutrikimas, sukeltas kibernetinės atakos, gali turėti tiesioginį poveikį pacientų sveikatai ir saugumui. Tai reiškia, kad kibernetinis saugumas čia yra ne tik technologinis ar informacinis klausimas, bet ir esminis*

pacientų priežiūros aspektas.“ Respondentas L06 rašė, kad svarbi, bet jie neturintys papildomų lėšų ir žmogiškųjų išteklių jos skatinimui ir įgyvendinimui.

9. Kaip manote, ar reikėtų kibernetinio saugumo mokymus įtraukti į privalomus sveikatos specialistų mokymus?

Septyni dalyviai mano, kad reikėtų kibernetinio saugumo mokymus įtraukti į privalomus sveikatos specialistų mokymus, du – ne ir plačiau nepakomentavo. L04 dar papildė, kad „...tokio pobūdžio mokymai skatintų saugumo kultūros kūrimą įstaigose ir kolektyvuose.“ L03 teigė: „įtraukiant kibernetinio saugumo mokymus į privalomą sveikatos specialistų mokymų programą, galima užtikrinti aukštesnį duomenų saugumo lygį ir stiprinti visuotinį pasitikėjimą sveikatos priežiūros sistema.“

Apibendrinant kokybinio tyrimo rezultatus, galima teigti, kad ligoninių vadovai supranta kibernetinio saugumo kultūrą kaip svarbią ir būtiną organizacijai, bet per mažai atsakomybės prisiima patys, daugiau tikisi iš darbuotojų, pamiršdami, kad vadovai yra vienas iš esminių kibernetinio saugumo kultūros elementų ir jų įsitraukimas į kultūros stiprinimą, jų rodomas pavyzdys saugumo klausimais yra svarbūs stiprinant ir plėtojant kibernetinio saugumo kultūrą organizacijoje. Dauguma organizacijų turi kibernetinio saugumo politikas, atsakingus asmenis, vykdo mokymus. Vadovu nuomone, kibernetinis saugumas turi ne tik finansinę ir reputacinę naudą, bet ir padeda užtikrinti duomenų saugumą ir veiklos tęstinumą ir stengiasi investuoti į kibernetinio saugumo užtikrinimą. Didžioji dalis vadovų pritartų, kibernetinio saugumo mokymus įtraukti į sveikatos priežiūros specialistų profesinės kvalifikacijos privalomojo tobulinimo tikslinių programų sąrašą.

IŠVADOS IR REKOMENDACIJOS

1. Atlikus mokslinės literatūros analizę, pristatyti pagrindiniai kibernetinio saugumo kultūros elementai: reguliarūs mokymai, aiškios politikos, vadovybės įsitraukimas ir palaikymas, nuolatinė kibernetinio saugumo kultūros analizė. Identifikavus šiuos elementus ir jų pagrindu kuriant kibernetinio saugumo kultūrą organizacijoje, galima vystyti stiprią saugumo kultūrą, kur darbuotojai yra sąmoningi kibernetinio saugumo klausimais, turi žinių ir įgūdžių kibernetinių grėsmių identifikavimui. Kibernetinio saugumo klausimai tampa nuolatine įmonės veikla ir visa organizacija yra įsitraukusi į kibernetinio saugumo kultūros plėtrą, suvokia, kad organizacijos duomenis, jos veiklos tęstinumą užtikrina ne tik informacinės technologijos, bet ir jos darbuotojai. Organizacijos įgyvendindamos kibernetinio saugumo kultūrą apsisaugo ne tik nuo finansinės, bet ir reputacinės žalos.

2. Remiantis atlikta literatūros analize galima daryti išvadą, kad kibernetinio saugumo kultūra yra neatsiejama ir priklausoma nuo keturių lygmenų: tarptautinio, nacionalinio, organizacinio ir individualaus. Sveikatos sektorius ne išimtis, čia pagrindiniai tarptautiniai reglamentai BDAR ir TIS2 darbo tiesioginę įtaką nacionaliniams teisės aktams, kuriuos turi įgyvendinti organizacijos, keisdamos savo vidaus tvarką ir darbuotojų požiūrį ir elgesį saugumo klausimais.

3. Išanalizavus literatūroje kibernetinės grėsmės sąvoką ir esminius bruožus galima teigti, kad tai neigiamas įvykis, turintis neigiamą poveikį informacinėms sistemoms, tinklams ir jų naudotojams. Suvokimas apie galimas kibernetines grėsmes ir žinojimas, joms būdingų bruožų, padėtų kurti tvirtas kibernetinio saugumo politikas. Pasigendama vieningos kibernetinių grėsmių klasifikavimo sistemos.

4. Išpirkos reikalaujančios programos, sukčiavimas el.paštu, Ddos atakos buvo vienos dažniausių kibernetinių atakų, minimų mokslinės literatūros šaltiniuose ir ataskaitose, būdingų sveikatos sektoriui. Medicininis daiktų internetas, implantuojami ir nešiojami medicinos prietaisai kelia didelę kibernetinio saugumo riziką visai sveikatos priežiūros sistemai ir šių technologijų naudojimas auga greičiau nei galimybė užtikrinti saugumą.

5. Sveikatos sektoriuje dažniausi minimi kibernetinių atakų veikėjai: kibernetiniai nusikaltėliai, įsilaužėliai, haktyvistai, valstybių remiami veikėjai ir vidinės grėsmės. Kibernetiniai veikėjai vykdydami nusikaltimus siekia net tik finansinės, bet ir asmeninės ar politinės naudos.

Žinojimas, kokie gali būti veikėjai ir jų motyvai, yra dar vienas svarbus stiprios kibernetinio saugumo politikos kūrimo elementas.

6. Atlikus kiekybinį tyrimą, kuriame dalyvavo Lietuvos ligoninių darbuotojai ir kokybinį tyrimą, kuriame dalyvavo atrinkti iš skirtingo lygmens ir apskrities ligoninių vadovai, galima daryti išvadą, kad dauguma organizacijų yra kibernetinio saugumo politika, bet ne visi darbuotojai yra susipažinę. Dar daug darbuotojų nežino, kam pranešti įvykus kibernetiniam incidentui ir nežino, ar yra paskirtas atsakingas asmuo kibernetinio saugumo klausimais, kas leidžia teigti, kad nėra pakankamai komunikuojama organizacijose tarp skyrių ir darbuotojų ir remiasi į tai, kad nėra tinkamai supažindinti su kibernetinio saugumo politika ir atsakingais asmenimis. Vadovybė per mažai įsitraukia į kibernetinio saugumo kultūros plėtrą, rodydami nepakankamą pavyzdį savo organizacijos darbuotojams. Mokymai nors ir vyksta, bet nėra pakankamai efektyvūs arba juose dalyvauja ne visi darbuotojai. Pastebėta, kad respublikinio ir regioninio lygmens ligoninės daugiau dėmesio skiria kibernetinio saugumo kultūros stiprinimui, aktyviau ir dažniau rengia mokymus ir kuria saugumo politikas, nei rajoninės ligoninės.

Rekomendacijos:

1. LR Sveikatos apsaugos ministerijai rekomenduojama papildyti sveikatos priežiūros specialistų profesinės kvalifikacijos privalomojo tobulinimo tikslinių programų sąrašą, įtraukiant kibernetinio saugumo mokymus. Patys darbuotojai būtų suinteresuoti mokytis, norėdami įgyti ar prasitęsti sveikatos priežiūros specialisto licenciją.

2. Sveikatos priežiūros specialistų švietimo teikėjams siūloma plėsti kvalifikacijos tobulinimo programas, įtraukiant kibernetinio saugumo temas, kad sveikatos priežiūros specialistai turėtų galimybę pasirinkti mokymus, leidžiančius pagilinti ar atnaujinti žinias, gebėjimus ar praktinius įgūdžius kibernetinio saugumo klausimais.

3. Sveikatos priežiūros įstaigų vadovams rekomenduojama aktyviau dalyvauti organizacijos kibernetinio saugumo kultūros formavime. Paskirti asmenys, atsakingus už kibernetinio saugumo kultūros įgyvendinimą, o juos paskyrus, pranešti darbuotojams. Peržiūrėti esamas finansines galimybes ir paskirti kasmetines išlaidas kibernetinio saugumo užtikrinimui. Nepamiršti, kad kibernetinio saugumo kultūra yra nuolat kintantis procesas, reikalaujantis nuolatinio dėmesio ir reguliariai vykdyti kibernetinio saugumo kultūros analizę, taip prisitaikant prie nuolat kintančio grėsmių kraštovaizdžio.

LITERATŪROS SĄRAŠAS

1. Adegoke, A., Navya, A., Jordan, F., Jenifer, N., Begley, R.D. (2022). *Cyber Security as a Threat to Health Care.* Prieiga internete: https://www.researchgate.net/publication/366267376_Cyber_Security_as_a_Threat_to_Health_Care
2. Ahmed, M. M., Maglaras, L., Ferrag, M. A. (2020). *Cyber Threats in Healthcare sector and countermeasures.* Prieiga internete: https://www.researchgate.net/publication/340448389_Cyber_Threats_in_Healthcare_sector_and_countermeasures
3. Ahmed, A., Sindi, F. H., Nour, M. (2022). *Cybersecurity in Hospitals: An Evaluation Model.* Prieiga internete: https://www.mdpi.com/2624-800X/2/4/43
4. Alder, S. (2024). *At Least 141 Were Hospitals Directly Affected by Ransomware Attacks in 2023.* Prieiga internete: https://www.hipaajournal.com/2023-healthcare-ransomware-attacks/
5. Alder, S. (2023). *July 2023 Healtcare Data Breach Report.* Prieiga internete: https://www.hipaajournal.com/july-2023-healthcare-data-breach-report/
6. Ashik, M. (2023). *Building an Effective Cybersecurity Culture Program.* Prieiga internete: https://secureread ing.com/building-an-effective-cybersecurity-culture-program/
7. Canadion Centre For Cyber Security (2022). *An Introduction to the Cyber Threat Environment.*
8. Cassetto, O. (2023). *Cybersecurity Threats: Everything you Need to Know.* Prieiga internete: https://www.exabeam.com/information-security/cyber-security-threat/
9. Cynerio ataskaita (2022). *The State of Healtcare IoT Device Security 2022.*
10. Coventry L. & Branley A. (2018). *Cybersecurity in healthcare: A narrative review of trends, threats and ways forward.* Prieiga internete: https://doi.org/10.1016/j.maturitas.2018.04.008
11. Corradini I. (2020). *Building a Cybersecurity Culture. 63–86 p.*
12. Da Veiga, A. (2016). *A Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument.* Prieiga internete: https://www.researchgate.net/publication/306407687_A_Cybersecurity_Culture_Research_Philosophy_and_Approach_to_Develop_a_Valid_and_Reliable_Measuring_Instrument
13. ENISA ataskaita (2016).

14. ENISA ataskaita (2022). *ENISA Threat landscape 2022. 64-110.*
15. ENISA ataskaita (2023). *ENISA Threat landscape: Health sector 2023.*
16. Europos parlamento ir tarybos reglamentas *(ES) 2016/679* (2016)
17. Europos parlamento ir tarybos reglamentas *(ES) 2019/881* (2019) *p. 19*
18. Europos parlamento ir tarybos reglamentas *(ES) 2022/2555* (2022)
19. Everard, T., (2023). *What is Cyber Security Culture and why does it matter for your organisation?* Prieiga internete: https://www.paconsulting.com/insights/what-is-cyber-security-culture-and-why-does-it-matter-for-your-organisation
20. Frenken, P. (2020). *Building a Culture of Security.* Prieiga internete: *https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/building-a-culture-of-security*
21. Gaižauskaitė I. ir Mikėnė S. (2014). *Socialinių tyrimų metodai: apklausa., 45-46 p.*
22. Gaižauskaitė I. ir Valavičienė N. (2016). *Socialinių tyrimai metodai: kokybinis interviu.* Prieiga internete: *https://cris.mruni.eu/server/api/core/bitstreams/6bc9b0c7-425b-4420-a2cd-e6ec2d12736a/content*
23. Giansanti D. (2021). *Cybersecurity and the Digital-Health: The Challenge of This Millennium.* Prieiga internete: https://doi.org/10.3390/healthcare9010062
24. Gioulekas, Stamatiadis, Tzikas, Gounaris, Georgiadou, Michalistsi-Psarrou, Doukas, Kontoulis, Nikoloudakis, Marin, Cabecinha & Ntanos (2022). *A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures.* Prieiga internete: *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8871847/*
25. Higienos instituto duomenys (2018-2021). Prieiga internete: https://hi.lt/php/spr1.php?dat_file=spr1.txt
26. HIMSS (2022). *2022 HIMSS Healtcare Cybersecurity Survey.*
27. Kost, E. (2023). *Biggest Cyber Threats in Healthcare.* Prieiga internete: https://www.upguard.com/blog/biggest-cyber-threats-in-healthcare
28. Kovacs, A. M., Besenyo, J. (2023). *Healthcare Cybersecurity Threat Context and Mitigation Opportunities.* Prieiga internete: https://www.researchgate.net/publication/370060798_Healthcare_Cybersecurity_Threat_Context_and_Mitigation_Opportunities
29. Libby, R. ir Blashfield, R. (1978). *Performance of a composite as a function of the number of judges. Organizational Behavior and Human Performance.* Prieiga internete: https://www.sciencedirect.com/science/article/abs/pii/0030507378900442?via%3Dihub

30. Lietuvos Respublikos Valstybės saugumo departamento (2021). *Grėsmių nacionaliniam saugumui vertinimas.,* p. 50 Prieiga internete: https://www.vsd.lt/wp-content/uploads/2021/03/2021-LT-el_.pdf
31. LR sveikatos apsaugos ministerijos internetinis puslapis. Prieiga internete: https://sam.lrv.lt/lt/naujienos/pratybose-cyber-europe-lietuvos-sveikatos-prieziuros-istaigos-stiprino-savo-gebejimus-valdyti-kibernetinius-incidentus
32. Luis Emilio Alvarez-Dionisi, Ph.D. & Nelly Urrego-Baquero (2019). *Implementing a Cybersecurity Culture.* Prieiga internete: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/implementing-a-cybersecurity-culture#1
33. Malik, A., Abid, A., Farooq, S., Abid, I., Navaz, N. A. & Ishaq, K. (2022).*Cyber threats: taxonomy, impact, policies, and way forward.* Prieiga internete: *https://www.researchgate.net/publication/362386737_Cyber_threats_taxonomy_impact_policies_and_way_forward*
34. Mason Hayes & Curran (2023). *Digital Health Annual Review 2022.* Prieiga internete: https://www.mhc.ie/uploads/documents/MHC-Digital-Health-Annual-Review-2022.pdf
35. Mazzardo, G., Jurcut, A. D., (2019). *Insider Threats in Cybersecurity: The Enemy within the Gates.* Prieiga internete: https://www.researchgate.net/publication/337438838_Insider_threats_in_Cyber_Security_The_enemy_within_the_gates
36. Mckeon, J. (2023). *Lehigh Valley Health Network Hit By BlackCat Ransomware Attack.* Prieiga internete: https://healthitsecurity.com/news/lehigh-valley-health-network-hit-by-blackcat-ransomware-attack
37. Nacionalinis kibernetinio saugumo centras (2020). *Kibernetinis saugumas ir verslas.* Prieiga internete: https://www.nksc.lt/doc/Kibernetinio_saugumo_vadovas_verslui_2020.pdf
38. Nas, A. (2023) *What are the benefits of an effective security culture?* Prieiga internete: https://thesecuritycompany.com/the-insider/what-are-the-benefits-of-an-effective-security-culture/
39. NIST Computer security resource center glossary. Prieiga internete: https://csrc.nist.gov/glossary/term/Cyber_Threat#:~:text=Any%20circumstance%20or%20event%20with%20the,from%20human%20actions%20and%20natural%20events.&text=Any%20circumstance%20or%20event,actions%20and%20natural%20events.&text=or%20event%20with%20the,from%20human%20actions%20and

40. Nurse, J. (2023). *5 big factors in a strong cybersecurity culture.* Prieiga internete: https://www.cybsafe.com/blog/5-factors-strong-cybersecurity-culture/
41. Oficialios statistikos portalas (2022). Prieiga internete: https://osp.stat.gov.lt/darbo-rinka-lietuvoje-2021/darbo-uzmokestis-darbo-sanaudos-ir-streikai/darbuotoju-skaicius
42. Parks, M. (2021). *The 7 Elements of an Organization's Cybersecurity Culture.* Prieiga internete: https://csgtechnologies.net/2021/05/the-7-elements-of-an-organizations-cybersecurity-culture/
43. Roy, R. (2021). *What Is a Cyber Threat? Definition, Types, Hunting, Best Practices, and Examples.* Prieiga internete: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-cyber-threat/#_001
44. Rupšienė L. (2007). *Kokybinio tyrimo duomenų rinkimo metodologija.,* 34-37 p.
45. Silomon J. (2020). *Der Hackerangriff auf die Düsseldorfer Uniklinik und was daraus folgen sollte.* Prieiga internete: https://ifsh.de/en
46. Ting D., (2022). *Healthcare and Cybersecurity: 35 Key Statistics and Facts You Should Know.* Prieiga internete: *https://www.tausight.com/healthcare-and-cybersecurity-key-statistics/*
47. Uchendu, B., Nurse, J. R. C., Bada, M., Furnell, S. *Developing a cyber security culture: Current practices and future needs.* Prieiga internete: *https://www.sciencedirect.com/science/article/abs/pii/S016740482100211X*
48. Willie, M. M., (2023). *The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture.* Prieiga internete: https://www.researchgate.net/publication/371399113_The_Role_of_Organizational_Culture_in_Cybersecurity_Building_a_Security-First_Culture

Šimonienė I. (2024). *Kibernetinio saugumo kultūros vertinimas Lietuvos ligoninėse* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

ANOTACIJA

Magistro baigiamajame darbe atliktas kibernetinio saugumo kultūros vertinimas Lietuvos ligoninėse. Pirmajame skyriuje nagrinėjami kibernetinio saugumo kultūros teoriniai aspektai, pristatant kibernetinio saugumo kultūros elementus, jos naudą organizacijoms, aprašomi kibernetinio saugumo kultūros lygmenys ir jų įtaka, kultūros vystymuisi. Antrojoje dalyje pateikiama kibernetinių grėsmių samprata ir esminiai bruožai, pristatomos pagrindinės kibernetinės grėsmės sveikatos sektoriuje, analizuojama jų statistika taip pat šiame skyriuje aprašomi kibernetinių grėsmių veikėjai ir jų motyvai. Trečiajame skyriuje pateikiami kiekybinis ir kokybinis tyrimai. Kiekybiniu tyrimu siekiama išsiaiškinti Lietuvos ligoninių darbuotojų supratimą, nuomonę ir požiūrį kibernetinio saugumo klausimais, o kokybinio tyrimo metu siekiama įvertinti, kaip ligoninių vadovai vertina ir kaip skatina kibernetinio saugumo kultūrą vadovaujamose ligoninėse. Paskutiniame skyriuje, susisteminus gautus rezultatus, pateikiamos tyrimų išvados ir rekomendacijos, kibernetinio saugumo kultūros plėtrai Lietuvos ligoninėse.

Pagrindiniai žodžiai: kibernetinio saugumo kultūra, kibernetinės grėsmės, sveikatos sektorius.

Šimonienė I. (2024). Assessment of cyber security culture in Lithuanian hospitals (master's thesis). Vilnius: Mykolas Romeris University

ANNOTATION

Assessment of cyber security culture in Lithuanian hospitals was carried out in the master's thesis. The first chapter examines the theoretical aspects of cyber security culture, presenting the elements of cyber security culture, its benefits for organizations, describing the levels of cyber security culture and their influence on the development of culture. The second part presents the concept and essential features of cyber threats, presents the main cyber threats in the health sector, analyzes their statistics, and also describes the actors of cyber threats and their motives in this chapter. The third chapter presents quantitative and qualitative research. The quantitative study aims to find out the understanding, opinion and attitude of Lithuanian hospital employees on cyber security issues, while the qualitative study aims to assess how hospital managers evaluate and promote the culture of cyber security in the hospitals they manage. In the last chapter, after systematizing the obtained results, research conclusions and recommendations for the development of cyber security culture in Lithuanian hospitals are presented.

Key words: cyber security culture, cyber threats, health sector.

Šimonienė I. (2024). *Kibernetinio saugumo kultūros vertinimas Lietuvos ligoninėse* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas.

SANTRAUKA

Kibernetinio saugumo kultūra sveikatos sektoriuje turėtų būti vienas iš esminių elementų, užtikrinančių, kad labai jautri ir asmeninė pacientų informacija būtų apsaugota nuo kibernetinių grėsmių, o organizacijos užtikrintų paslaugų ir veiklos tęstinumą. Buvo iškelta darbo problema, kuri gali būti formuojama tokiu klausimu: Kaip stiprinti kibernetinio saugumo kultūrą Lietuvos ligoninėse? Darbo objektas - kibernetinio saugumo kultūra sveikatos sektoriuje. Tyrimo tikslas – įvertinti kibernetinio saugumo kultūrą Lietuvos ligoninėse. Tikslui pasiekti išsikelti šie uždaviniai: išnagrinėti kibernetinio saugumo kultūros teorinius aspektus, apžvelgti pagrindines kibernetines grėsmes sveikatos sektoriuje ir atlikti mišrų tyrimą siekiant įvertinti Lietuvos ligoninių darbuotojų žinias ir jų vadovų supratimą apie kibernetinio saugumo kultūrą. Darbe taikomi metodai: mokslinės literatūros ir antrinių statistinių duomenų analizės, duomenų vizualizacija, kokybinio ir kiekybinio tyrimų turinio analizės.

Atlikus empirinį tyrimą, buvo nustatyta, kad ligoninių darbuotojai ir vadovai supranta kibernetinio saugumo kultūros svarbą, tačiau per mažai dėmesio ir iniciatyvos šiuo klausimu rodo patys vadovai. Kibernetinio saugumo kultūros stirpinimui Lietuvos ligoninėse trūksta reguliarių mokymų, bendradarbiavimo ir komunikacijos tarp skyrių ir pačių darbuotojų.

Magistro baigiamojo darbo pabaigoje pateikiamos išvados ir rekomendacijos, kibernetinio saugumo kultūros stiprinimui sveikatos sektoriuje.

Šimonienė I. (2024). Assessment of cyber security culture in Lithuanian hospitals (master's thesis). Vilnius: Mykolas Romeris University.

SUMMARY

A cybersecurity culture in the health sector should be one of the essential elements in ensuring that highly sensitive and personal patient information is protected from cyber threats and that organizations ensure continuity of services and operations. A work problem was raised, which can be shaped by the following question: How to strengthen the culture of cyber security in Lithuanian hospitals? The object of the work is the cyber security culture in the health sector. The purpose of the study is to assess the cyber security culture in Lithuanian hospitals. In order to achieve the goal, the following tasks were set: to examine the theoretical aspects of cyber security culture, to review the main cyber threats in the health sector and to conduct a mixed research in order to assess the knowledge of Lithuanian hospital employees and their managers' understanding of cyber security culture. Methods used in the work: analysis of scientific literature and secondary statistical data, data visualization, qualitative and quantitative analyzes of research content.

Empirical research has shown that hospital employees and managers understand the importance of cyber security culture, but managers themselves show too little attention and initiative in this regard. In order to strengthen the culture of cyber security in Lithuanian hospitals, there is a lack of regular training, cooperation and communication between departments and the employees themselves.

At the end of the master's thesis, conclusions and recommendations are presented for strengthening the cyber security culture in the health sector.