MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

RŪTA VALAVIČIŪTĖ

KIBERNETINIO SAUGUMO KULTŪROS VYSTYMAS LIETUVOS BENDROJO UGDYMO MOKYKLOSE

Magistro baigiamasis darbas

Vadovas

doc. dr. M. Laurinaitis

Vilnius, 2021

MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

RŪTA VALAVIČIŪTĖ

KIBERNETINIO SAUGUMO KULTŪROS VYSTYMAS LIETUVOS BENDROJO UGDYMO MOKYKLOSE

Kibernetinio saugumo valdymo magistro baigiamasis darbas

Studijų programa 6211LX066

Vadovas:

doc. dr. M. Laurinaitis

2021 12

Atliko:

KSVvmis19-1 gr. stud.

R. Valavičiūtė

2021 12 12

Vilnius, 2021

TURINYS

LENTELĖS

PAVEIKSLAI

SANTRUMPOS

1. Kibernetinis saugumas – naudojama kaip apibrėžta Lietuvos Respublikos Kibernetinio saugumo įstatyme (2018);
2. Kibernetinė erdvė - naudojama kaip apibrėžta Lietuvos Respublikos Kibernetinio saugumo įstatyme (2018)
3. Skaitmeninė erdvė - tai, kas rodoma skaitmeninio įrenginio ekrane. Visa tai gali turėti daugybę formų: internetiniai puslapiai, aplikacijos arba programos, filmai, nuotraukos ir svetainė užima skaitmeninę erdvę. Visa tai egzistuoja kibernetinėje erdvėje (IGI Global, 2021)

ĮVADAS

Darbo aktualumas. Elektroninė erdvė užima didelę mūsų gyvenimo dalį ir naudojimasis ja yra neatsiejama kiekvienos dienos dalis. Išmanių įrenginių galima rasti beveik kiekvieno, šių dienų, žmogaus namuose, didžioji dauguma net nebeįsivaizduoja kaip reikėtų be to gyventi. Suteikiami technologiniai pranašumai palengvino bendravimą ar buitį. Pasaulis nebeturi sienų, naujienos gali mus pasiekti vos kelių mygtukų paspaudimu. Ypatingai didelė dalis asmenų, įmonių, švietimo sektoriaus organizacijų perkėlė pradėjo intensyviau naudotis ir pritaikė išmaniąsias technologijas prasidėjus COVID-19 pandemijai. Tai padėjo nenutraukti vykdomos veiklos ir nestabdyti tiek darbo, tiek mokymosi procesų. Tačiau informacijos greitis ir patogumas ne visuomet gali būti siejama su saugumu. Vykdydami veiklą kibernetinėje erdvėje, mes norime išsaugoti savo privatumą ir konfidencialumą. Saugumo užtikrinimas svarbus klausimas ne tik viešajame ir privačiajame sektoriuose, bet ir kiekvieno žmogaus asmeniniame gyvenime. Šiuolaikinėje inovatyvioje demokratinėje valstybėje turėtų būti siekiama apsaugoti vartotojus nuo įvairių pavojų, kurie gali nutikti turint per mažai žinių ar išmanymo. Kibernetinis saugumas turėtų būti suprantamas ir įprastas reiškinys kiekvienam piliečiui. Formuojant kibernetinio saugumo kultūrą vienas iš efektyvių metodų tai pasiekti – švietimas. Didelė dalis kibernetinės nusikalstamos veikos šiais laikais yra nukreipta į asmenis, siekiant juos šantažuoti, pateikiant jiems jų asmeninę informaciją ir grasinant ją paviešinti ar sunaikinti, jeigu nebus įvykdytos nurodytos sąlygos. Vienas iš lengviausiai pasiekiamų taikinių yra nepilnamečiai, kuriems tokio tipo šantažas gali turėti ilgalaikių pasekmių, ne tik emocinių, bet ir psichologinių. Kultūros vystymas turėtų būti formuojamas atkreipiant dėmesį į jaunimą ir pradedamas diegti švietimo įstaigose. Lietuvos Respublikos Kibernetinio saugumo strategijos Trečio skirsnio 27 punkte numatoma, jog svarbu vystyti kibernetinio saugumo kultūrą bendrojo ugdymo įstaigose. Švietimo įstaigos yra vienos iš pagrindinių institucijų, kuriose tikslinga medžiaga yra perduodama ugdant jaunuolius (Lietuvos Respublikos Kibernetinio saugumo įstatymas, 2018). Naujausios informacijos suteikimas ir inovatyvus panaudojimas bendrojo ugdymo mokyklose yra svarbi auklėjimo funkcija, kurios dėka yra turėtų būti suteikiamas bazinių žinių bagažas ir taip ugdoma pažangi jaunoji karta.

Mokslinis naujumas ir teorinis reikšmingumas. Kibernetinio saugumo kultūros reikšmingumas ir svarba nagrinėjama jau ne vieną dešimtmetį. 2003 metais Jungtinių Tautų generalinė asamblėja išleido rezoliuciją dėl kibernetinio saugumo globalios kultūros kūrimo. Rezoliucijoje aiškinama svarba švietimo ir asmenų asmeninio indelio, jog elektroninės sistemos būtų apsaugotos (General Assembly, 2003). Ši tema išlieka ypatingai aktuali šiais laikais. Kibernetinis saugumas yra viena labiausiai į priekį žengiančių sričių, tačiau taip pat tobulėja ir elektroninėje erdvėje veika

užsiimantys nusikaltėliai. Kibernetinis saugumas negali būti užtikrinamas tik diegiant apsaugos sistemas ar įdarbinant administratorius, kurie sektų sistemų darbą ir padėtų užkardyti grėsmes, kuomet spragos yra pastebėtos. Žmogaus fizinės saugos reikalingumą kibernetinio saugumo užtikrinimui ir jog tai turi būti pasiekta per švietimą ir kultūros ugdymą (Ani, Hongmei ir Tiwari, 2018). Užsienio mokslininkai atskleidžia jog šių laikų grėsmės yra nutaikytos tiesiai į žmogų, todėl kultūros ugdymas yra vienas svarbiausių veiksnių formuojant tarptautinį supratimą, žmonių sąmoningumą kibernetinio saugumo srityje (Andrii ir Vsevolod, 2019; Paziuk ir Mitsik, 2019). Kibernetinio saugumo švietimą nagrinėjantys mokslininkai atskleidžia jo naudą ir reikalingumą, jog integracija ir kultūros vystymas turėtų prasidėti pradedant mokyklinio amžiaus paaugliais ir nenustojant šviesti ir atnaujinti žinias visiems elektroninės erdvės naudotojams (Tomczy, 2019; Šimandl ir Vaniček, 2017; Dobrinoiu, 2017). Lietuvoje taip pat vyksta mokslinės diskusijos siekiant diegti kibernetinio saugumo kultūros švietimą, tačiau kol kas nepakankamai. Kibernetinio saugumo kultūros vystymas nėra mokyklų prioritetas, o kylančios grėsmės pastebimos gan dažnai, dalis jų yra nutaikytos į jaunus žmones. Galima teigti jog yra didelis poreikis gerinti kibernetinio saugumo kultūrą. Tai leidžia nustatyti darbo problemą, kuri gali būti formuluojama tokiu klausimu:

Darbo problema. Kaip galėtų būti tobulinama Kibernetinio saugumo kultūra bendrojo ugdymo mokyklose?

Šiame darbe bus siekiama nustatyti kas yra kibernetinė saugumo kultūra ir jos svarba ugdant asmenis, kaip atsakingus vartotojus. Darbe bus analizuojami aspektai, kurie svarbūs vystant kibernetinę kultūrą Lietuvos bendrojo ugdymo mokyklose.

Darbo objektas. Kibernetinio saugumo kultūros vystymas Lietuvos bendrojo ugdymo mokyklose.

Darbo tikslas. Teoriškai ir empiriškai ištirti kibernetinio saugumo kultūros vystymą Lietuvos bendrojo ugdymo mokyklose.

Darbo uždaviniai:

1. Išnagrinėti kibernetinio saugumo kultūros sampratą;
2. Pateikti kibernetinio saugumo kultūros teorinį konceptą;
3. Išanalizuoti užsienio šalių patirtį, plėtojant kibernetinio saugumo kultūrą;
4. Atlikti tyrimą siekiant identifikuoti kibernetinio saugumo kultūros tobulinimo galimybes Lietuvoje.

Darbo metodai:

1. Mokslinės literatūros analizė – metodas atliekamas pagal K. Kardelį (2016), kuris teigia, jog tai yra neatsiejama darbo dalis, kuri tęsiasi viso mokslinio tyrimo metu. Kaip pateikia autorius literatūros nagrinėjimas vyko šiais etapais: *1. Perskaitomas pavadinimas, turinys, anotacija įvadas, peržiūrima bibliografija. Tai padeda pasirinkti <...> ar veikalą skaityti išsamiai. <...> 2. Skaitant*

literatūros šaltinį pirmą kartą, būtina visų pirma išsiaiškinti jo turinį, <...> 3. Skaitant veikalą antrą kartą, būtina įvertinti faktinę medžiagą, atrinkti tipingiausius faktus ir palyginti juos su jau žinomais. (K. Kardelis, 2016, p. 112 – 113) Šis darbo metodas buvo naudojamas atliekant literatūros analizę ir siekiant išnagrinėti kibernetinio saugumo kultūros sampratą, bei teorinį konceptą.

2. Lyginamoji literatūros analizė – metodas atliekamas pagal F Cornish, A. Gillespie ir T. Zittoun (2014). Analizuojant ir interpretuojant duomenis buvo atsižvelgiama į skirtingas autorių pateikiamas įžvalgas siekiant atskleisti įvairias perspektyvas.

3. Duomenų vizualizacijos metodas – metodas atliekamas pagal B. Frey (2018). Pasak autoriaus grafinis informacijos vaizdavimas padeda lengviau atskirti svarbius aspektus nuo detalių ir suteikia daugiau aiškumo nagrinėjant problemą bei pateikiant esminę informaciją. Darbe šis metodas naudojamas pateikiant schemas, teiginius, lenteles.

4. Pusiau struktūrizuotas interviu – (žr. 3.1. poskyrį);

5. Apklausa raštu – (žr. 3.1. poskyrį).

Duomenų analizės metodai:

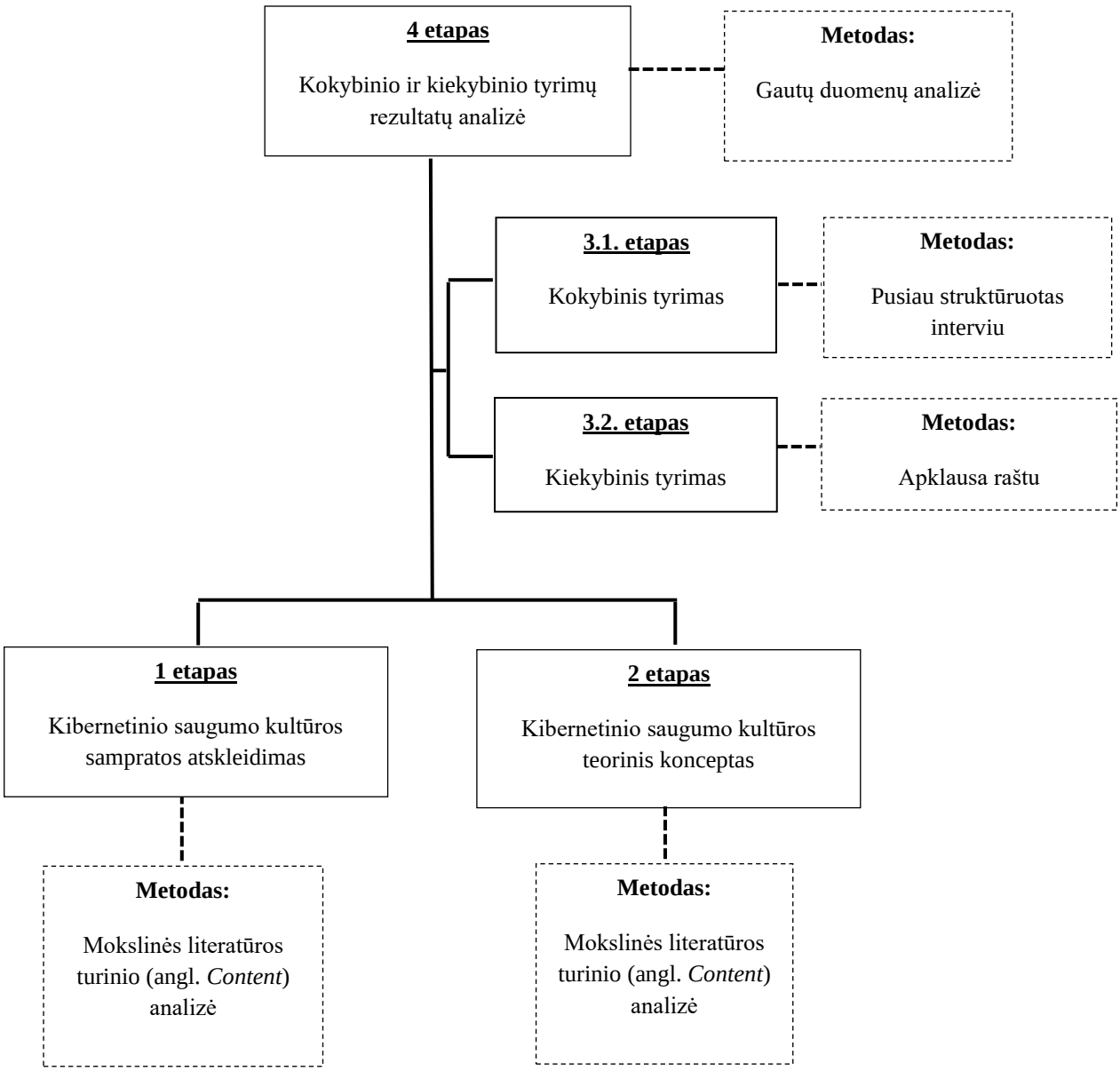
1. Kokybinė turinio analizė – (žr. 3.1. poskyrį);

2. Kiekybinė turinio analizė – (žr. 3.1. poskyrį);

3. Gautų duomenų analizė – (žr. 3.1. poskyrį).

Darbo struktūra. Darbas sudarytas iš 3 dalių. Pirmoje dalyje nagrinėjama kibernetinio saugumo kultūros samprata ir jos reikšmingumas tarptautiniu, nacionaliniu, organizaciniu ir individualiu lygmenimis. Antrojoje dalyje nagrinėjamas kibernetinio saugumo kultūros teorinis konceptas, su kokiomis rizikomis elektroninėje erdvėje yra susiduriama dažniausiai, kokie modeliai ir koks mokytojų bei tėvų vaidmuo turėtų būti taikomas siekiant užtikrinti tinkamą mokinių mokymą. Antrojoje dalyje taip pat apžvelgiama kitų šalių patirtis plėtojant kibernetinio saugumo kultūrą. Trečiojoje dalyje aprašomas kokybinis ir kiekybinis tyrimai. Kokybiniu tyrimu siekiama išsiaiškinti kiek mokyklos įsitraukia į kibernetinio saugumo kultūros tema vykdomą veiklą. Kiekybinio tyrimo tikslas išsiaiškinti kaip Lietuvos mokyklų mokiniai supranta su kibernetiniu saugumu susijusias rizikas ir vertina mokymą teikiamą mokyklose. Darbo struktūros loginė schema pavaizduota 1 paveiksle.

Praktinis taikomumas. Darbo praktinį taikomumą rodo tai, kad išgryninus esamą kibernetinio saugumo kultūros plėtojimo padėtį galima pateikti aktualias išvadas ir suformuoti rekomendacijas švietimo ir sporto ministerijai ir mokyklų direktoriams siekiant tobulinti kibernetinio saugumo kultūrą bendrojo ugdymo mokyklose.



1 pav. Darbo struktūros loginė schema

1. KIBERNETINĖS SAUGUMO KULTŪROS SAMPRATA IR ESMINIAI BRUOŽAI

Technologijos šiais laikais yra tapusios vienu didžiausiu varikliu, varančiu žmoniją į priekį. Kiekvieną dieną žiniasklaidoje galime pamatyti apie tai kaip nauji išradimai stumia mus į priekį vardan patogesnio ir greitesnio rytojaus. Technologijų evoliucija sumažino erdves ir laiką. Dabar daugelį norimų veiksmų galime atlikti ženkliai greičiau. Kibernetinės erdvės atsiradimas sukūrė visiškai naują pasaulį ir dimensiją, kuri yra neatsiejama nuo mūsų kasdieninės veiklos ir jos vartotojų (Tziarras, 2014, p. 320).

Sparčiai tobulėjant technologijoms, buvo pradėtas kreipti didelis dėmesys ne tik į daugelio procesų prastumą, bet ir į saugumą. Ši sąvoka suprantama nuo seniausių laikų, istoriniai pavyzdžiai rodo, kad žmonės siekdami apsaugoti save jungdavosi į sąjungas ir kovodavo prieš bendrą priešą (Tziarras, 2014, p. 321). Kaip ir karyboje, taip ir kibernetiniame saugume yra privaloma apsibrėžti koks yra to tikslas ir kas turėtų būti apsaugota. Lietuvos Respublikos Kibernetinio saugumo įstatyme kibernetinis saugumas apibrėžiamas kaip: *visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą* (Lietuvos Respublikos Kibernetinio saugumo įstatymas, 2018). Panagrinėję šią sąvoką matome jog taikant įvairias saugumo priemones yra siekiama išlaikyti elektroninės informacijos:

1. Prieinamumą – informacija turėtų būti be trukdžių prieinama vartotojui;
2. Vientisumą – užtikrinimas, kad informacija nebuvo pakeista ar kaip kitaip padaryta žala ir ji nesiskiria nuo pirminės sukurtos informacijos. Reikalingas ir autentiškumo nustatymas, jog būtų identifikuotas pirminis informacijos kūrėjas, jog būtų galima identifikuoti ar informacija nebuvo suklastota ar pasisavinta;
3. Konfidencialumą – užtikinimas, jog informaciją gali pasiekti tie asmenys, kuriems ji yra skirta ir nebūtų pasiekiama trečiosioms šalims, jeigu tam nėra būtinybės.

Siekiant užtikrinti kibernetinį saugumą pastebėta, jog vien tik naujų apsaugos sistemų kūrimas ir stiprinimas nėra pagrindinis aspektas. Daugelis tyrimų rodo, jog vis dar pagrindiniu veiksniu, į ką koncentruojasi kibernetiniai nusikaltėliai, yra žmonių padarytos klaidos. Daugelis atakų įvyksta naudojant socialinę inžineriją, kurios tikslas suklaidinti vartotojus, apgauti, jog tam tikri veiksmai būtų

inicijuojami jų pačių. Daugiau nei 90% kibernetinio saugumo problemų kyla dėl žmogiškųjų veiksnių (Aronovich, 2018). Kibernetinių atakų padaroma žala kainuoja labai didelius pinigus siekiant atstatyti sugadintas sistemas, atkurti prarastą informaciją ar atlyginti padarytą žalą. Siekiant kovoti su šiais pavojais, buvo pradėtas skirti didelis dėmesys kibernetinio saugumo kultūrai. Kibernetinio saugumo kultūros vystymas yra didelis žingsnis link saugesnės kibernetinės erdvės (Aiken, 2019, p 20).

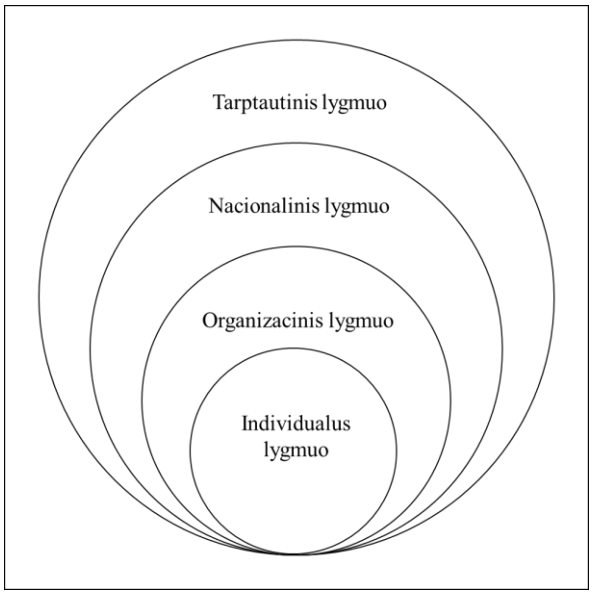
Vartotojų skaitmeninis raštingumas prisideda prie kibernetinė erdvės saugumo. Todėl kultūra turi būti plėtojama, tačiau siekiant suprasti šios plėtros reikšmę yra svarbu panagrinėti ir apibrėžti šią sąvoką.

1.1. Kibernetinio saugumo samprata

Bendrai sąvoka „kultūra“ yra suprantama kaip „visa, kas sukurta žmonių visuomenės fiziniu ir protiniu darbu“ („Kultūra“, 2020). Tai visi procesai, kurie yra sukuri individų ir priimti, kaip naudotini visuotinai, skirti šviesti, nustatyti procesų vienodumą ar gilinti supratimą. Apie siekį kurti kibernetinio saugumo kultūrą globaliu mastu matome ir 2003 metų Jungtinių tautų Generalinės Asamblėjos rezoliucijoje. Rezoliucijoje kibernetinio saugumo kultūros kūrimas apibrėžiamas kaip esamos situacijos įvertinimas, nuolatinis sistemų spragų, organizacijų ir žmonių procesų stebėjimas ir siekis identifikuotas grėsmes pritaikyti mokyme, kad nebūtų kartojamos klaidos (Jungtinių Tautų. Generalinės asamblėjos rezoliucija, 2003)

Tobulėjant technologijoms ir pasauliui sparčiai judant į priekį, kibernetinio saugumo kultūros, supratimas ir taikymas turi būti lankstus ir lengvai pritaikomas aspektas (Pătrașcu, 2019, p 274). Yra labai svarbu, jog būtų dedamas didelis indėlis į supratimo plėtojimą, nes yra nemažai grėsmių, kurių negalima užkardyti techninėmis priemonėmis. Kibernetinio saugumo kultūros supratimas apima ir nagrinėja saugumą ir laisvę kibernetinėje erdvėje, kaip glaudžiai susijusius aspektus (Paziuk ir Mitsik, 2019, p 104). Suderinti šiuos du aspektus yra nemenkas uždavinys. Saugumo ir laisvių užtikrinimas yra susijęs su žmonių teisėmis ir laisvėmis, jog atliekami veiksmai neturėtų daryti įtakos ar kažkokiu būdu varžyti ar pažeisti asmens teisių.

Kibernetinio saugumo kultūros bendrosios gairės turėtų būti plėtojamos globaliu mastu, nes nebelikus sienų, tai tampa ne tik bendra, nacionalinė ar organizacinė, atsakomybė (Paziuk ir Mitsik, 2019, p 104). Kibernetinis saugumo kultūra įvairių autorių darbuose yra pateikiama per keturias dimensijas: tarptautinę, nacionalinę, organizacinę ir individualią. Šie kibernetinio saugumo kultūros lygiai yra skirstomi nuo apimančių viską globaliai (tarptautinis) iki asmeninių gebėjimų (individualus) ir yra vienas nuo kito priklausomi (1 pav.).



Šaltinis: adaptuota pagal Da Veiga, 2016, p. 1008

2 pav. Kibernetinio saugumo kultūros lygmenys

Kalbėdamas apie kibernetinio saugumo kultūros kūrimo svarbą, Paziuk ir Mitsik (2019) pateikia svarbiausius elementus, kurie turėtų būti pagrindas, tai: sąmoningumas, atsakomybė, reagavimas, etika, demokratija, rizikos vertinimas, saugumo kūrimas ir įgyvendinimas, saugumo valdymas ir pakartotinis vertinimas (p. 104).

George M. Aiken (2019) nagrinėdamas kibernetinio saugumo kultūros ištakas pateikia, jog pagrindiniai elementai sudarantys kibernetinio saugumo kultūrą turėtų būti: įrenginių fizinis saugumas; nuolatinis mokymas apie galimas grėsmes, veiklos proceso sukūrimas, numatymas veiksmų planų, rizikos vertinimas, priėjimo kontrolės diegimas, audito ir atskaitomybės sistemų diegimas (p. 18–19).

Kibernetinio saugumo kultūros sąvokos apibrėžiamos įvairiapusiškai, vieni mokslininkai daugiau tai mato kaip organizacijos vidaus procesinius aspektus, kiti kaip visuotinai kintantį reiškinį. 1 lentelėje nagrinėjamos autorių pateikiamų sąvokų variacijos.

1 lentelė. Kibernetinio saugumo kultūros sąvokų apibrėžimai

Eil. Nr.	**Autorius**	**Sąvoka**
1.	Frenken, 2020	Saugumo kultūra yra daugiau nei tik kibernetinio saugumo suvokimas. Tai reikalauja, kad darbo jėga žinotų saugumo riziką ir procesą, kad būtų išvengta šios rizikos. Tai užduočių vykdymo proceso kūrimas ir vykdymas, užtikrinantis įmonės saugumą.

1 lentelės tęsinys kitame puslapyje

1 lentelės tęsinys

2.	Da Veiga, Astakhova, Botha ir Herselman, 2020, p. 2 .	Kibernetinio saugumo kultūra yra susijusi su tuo, kaip žmonės suvokia kibernetinį saugumą ir iš jo kylantis elgesys elektroninėje erdvėje, darantis įtaką skaitmeninės informacijos, sistemų ir žmonių apsaugai.
3.	Pătrașcu, 2019, p. 274	Kibernetinio saugumo kultūra nukreipta į evoliuciją ir plėtrą, prisitaikant prie naujų informacinių technologijų ir naujausių skatinimo būdų. Kibernetinio saugumo kultūrai būdingas lankstumas ir pritaikomumas, kintantis kartu su visuomenės, ypač skaitmeninės visuomenės, raida.
4.	European Union Agency for Network and Information Security, 2017, p. 7	Organizacijų kibernetinio saugumo kultūra reiškia žmonių žinias, įsitikinimus, suvokimą, požiūrį, prielaidas, normas ir vertybes apie kibernetinį saugumą ir tai, kaip jie pasireiškia žmonių elgesiu su informacinėmis technologijomis. Kibernetinio saugumo kultūra siekia, kad informacijos saugumo sumetimai būtų neatsiejama darbuotojo darbo, įpročių ir elgesio dalis, įtraukiant juos į kasdienius veiksmus.
5.	Da Veiga, 2016, p. 1008	Kibernetinio saugumo kultūra, tai tyčinis ir netyčinis kibernetinės erdvės panaudojimas iš tarptautinės, nacionalinės, organizacinės ar individualios perspektyvos aspektą kibernetinio vartotojo požiūrio, prielaidų, įsitikinimų, vertybių ir žinių kontekste. Atsirandanti kibernetinio saugumo kultūra tampa tuo, kaip viskas daroma sąveikaujant elektroninėje erdvėje, ir ji gali skatinti arba slopinti įvairių subjektų saugumą, saugumą, privatumą ir pilietines laisves.
6.	Paul ir Porche, 2012, p. 71	Bendrų pagrindinių prielaidų modelis, palaikantis informacijos saugumą, tampa natūraliu visos armijos personalo, veikiančio virtualioje erdvėje, kasdieninės veiklos aspektu.

Išanalizavus pateiktus apibrėžimus, pastebima, kad dalis mokslininkų ar kitų tyrėjų koncentruojasi daugiau į organizacinio lygmens kibernetinio saugumo kultūrą ir apibrėžia ne tokiu globaliu mastu. Tačiau galima įžvelgti šiuos pagrindinius punktus, kurie apibrėžia šią sąvoką: lankstumas, pritaikomumas, žinios, požiūris, suvokimas, įpročiai, kaita.

Kibernetinio saugumo kultūra, tai lanksti, greitai kintanti ir prisitaikanti prie pasaulio tendencijų procesų visuma, kuria siekiama didinti žinias ir žmonių požiūrį, suvokimą, įpročius naudojantis kibernetine erdve siekiant stiprinti technologinius įgūdžius ir skaitmeninį raštingumą. Norint geriau

įsigilinti į šios kultūros plėtojama verta panagrinėti skirtingus lygmenis, kuriuos išskiria tyrėjai, norėdami pateikti kokios atsakomybės tenka plėtojant tarptautinį, nacionalinį, organizacinį ir individualų lygmenis.

1.2. Tarptautinė kibernetinio saugumo kultūra

Ribų nebuvimas elektroninėje erdvėje kaip niekad sujungė pasaulio valstybes, vardan vieno tikslo – siekio, kad kibernetinė erdvė būtų apsaugota. Apsaugota turi būti tarptautinė kritinė infrastruktūra. Europos Sąjunga yra aktyvi žaidėja skatinant bendrą kibernetinio saugumo kultūrą, nes yra platinamas požiūris, jog supratimas turi būti ugdomas per formalųjį švietimą įtraukiant ne tik mokinius, bet ir mokytojus ar jų tėvus. Tačiau tarptautiniu lygmeniu yra sunku pasiekti sutarimą, dėl skirtingų šalių esamo technologijų pažangumo, žmonių suvokimo lygio ar valdžios palaikymo (Paziuk ir Mitsik, 2019, p. 104). Nepaisant to, kad skirtingi šalių supratimo lygmenys sudaro nelengvas sąlygas sprendimams priimti, jog konsensusas būtų pasiektas, tarptautiniu mastu kuriama kultūra turėtų turėti pamatines vertybes, kuriomis būtų siekiama etikos principų laikymosi, saugumo elektroninėje erdvėje. Nereikėtų pamiršti ir svarbiausio aspekto, tai – žmogaus teisių apsauga.

Kibernetinėje erdvėje žmonės yra įgalinti veikti savarankiškai. Kiekvienas yra atsakingas už atliekamus veiksmus, todėl reikia laikytis bendrųjų sutarimų ir suprasti, kokie veiksmai yra galimi, o kokie yra pažeidžiantys tam tikras numatytas normas arba darantys neigiamą poveikį kritinei infrastruktūrai.

Tarptautinės kibernetinio saugumo kultūros plėtra turėtų rūpintis sąjungos, aljansai kurie apima didelę dalį šalių arba būti kuriami tarptautiniai susitarimai, kurie numatytų gaires šalims, kaip rekomenduojama kurti procesus nacionaliniu lygmeniu.

Išnagrinėjus tarptautinės kibernetinio saugumo kultūros kūrimo aspektus galima įžvelgti šiuos privalumus:

1. Dėmesys skiriamas vertybėms, kurios formuoja kibernetinio saugumo kultūros pamatą;
2. Kuriama bendra kritinės infrastruktūros apsauga;
3. Duodamos bendros gairės, jog nacionalinė kibernetinė saugumo kultūra atitiktų bendras pasaulines tendencijas.

Atsižvelgiant į tai, kad užtikrinti tarptautinio lygmens reguliavimą vis dar kyla problemų, galima išskirti šiuos trūkumus, su kuriais susiduriama kuriant bendrą supratimą:

1. Yra sunku apibrėžti bendras gaires, kurios tiktų ir būtų pritaikomos visoms valstybėms, dėl skirtingų šalių vidinės politikos ir valdymo tvarkos;
2. Sunku pasiekti bendrą valstybių konsensusą siekiant įgyvendinti bendrą tvarką.

1.3. Nacionalinė kibernetinio saugumo kultūra

Pasaulyje sudaryta nemažai sąjungų ar galioja bendrų sutarimų, kuriais šalys įsipareigoja vardan bendrų tikslų, kurių yra siekiama. Nepaisant to, kiekviena valstybė turi skirtingą tvarką, politinį režimą, ekonominį lygį, kurie daro didelę įtaką priimamiems sprendimams. Šalims siekiant kuo kokybiškiau apsaugoti vidinę kritinę infrastruktūrą yra atkreipiamas vis didesnis dėmesys į kibernetinio saugumo didinimą ir kultūros vystymą.

Nacionalinis kibernetinio saugumo poreikis, tai siekis išlaikyti kritinę aplinką, skatinančią efektyvumą, inovacijas ir ekonominę gerovę, tuo pačiu skatinanti saugumą, verslo konfidencialumą, privatumą ir piliečių teises (National Institute of Standards and Technology, 2018, p 1–2). Susipažinus su pateiktu apibrėžimu, galima teigti, jog siekiant, kad kuriama kultūra būtų teigiamai priimama ir adaptuotųsi, yra reikalinga, jog būtų matoma nauda. Nacionaliniu lygmeniu privaloma sukurti ne tik normas, bet ir įdiegti metodus, kaip tai galima būtų pasiekti kokybiškiau. Siekiant efektyvumo pirmiausiai reikėtų išsikelti tikslus ir įvertinus esamą situaciją numatyti į ką ji turėtų pasikeisti. Pirmiausia kibernetinio saugumo kultūros dėmesys turėtų būti atkreipiamas ir stiprinamas šiose srityse:

1. Programų kūrimas siekiant plėtoti supratimą. Programos turėtų būti skirtos tiek viešajam, tiek privačiajam sektoriams, visuomenei;
2. Saugaus interneto ir kompiuterių naudojimo švietimo programos švietimo srityje;
3. Užtikrinamas profesinis mokymas su kibernetinio saugumo sritimi dirbantiems asmenims, išduodamų pažymėjimų populiarinimas;
4. Kibernetinio saugumo temų įtraukimas į viešojo ir privataus sektorių vadovų mokymo programas. (Pătrașcu, 2019, p 276–278)

Kibernetinės grėsmės yra nuolatos besikeičiančios ir tobulėjančios, todėl tik reguliavimas nacionaliniu lygmeniu gali užtikrinti bendrus saugumo standartus. Negali būti pamirštamas ir didelio indėlio įdėjimas į asmenų mokymą, kas padėtų išvengtų daugelio problemų, kurių negalima pašalinti techninėmis priemonėmis. Nacionaliniu lygmeniu į mokymą turėtų plačiai būti įtraukiami mokiniai ir mokytojai, jog žinios būtų perduodamos ir formuojamos nuo ankstyvo amžiaus. Edukaciją taip pat galima užtikrinti per formalųjį ir neformalųjį švietimą (įvairūs popamokiniai užsiėmimai, specialios mokyklos, kuriose būtų mokoma su kibernetinio saugumu susijusių temų) ir žinoma per asmeninį individualų švietimą. Reikėtų nepamiršti ir kuriamos kultūros populiarinimo. Siekiant šviesti kuo didesnį šalies gyventojų kiekį, informaciją reikėtų skleisti pasitelkus įvairius komunikacijos kanalus, tokius kaip tradicinė ir skaitmeninė žiniasklaida, socialiniai tinklai, viešosios iniciatyvos (Paziuk ir Mitsik, 2019, p. 277).

Apibendrinus, galima teigti, jog kibernetinė saugumo kultūra kiekvienoje šalyje gali skirtis ir

priklausyti nuo šalies politinio režimo, galiojančios tvarkos, papročių ar ekonominės padėties. Plėtojant ir tobulinant nacionalinę kibernetinę saugumo kultūrą pirmiausiai turėtų būti įvertinta esama padėtis šalyje, išsikeliami tikslai, įvertinamos rizikos ir biudžetas, bei apsibrėžiamos priemonės ir laikotarpiai, siekiant efektyvaus įgyvendinimo.

1.4. Organizacijų vidinė kibernetinio saugumo kultūra

Organizacinė kibernetinė saugumo kultūra yra bene labiausiai nagrinėjama mokslininkų tema. Verslo ir vyriausybinių institucijų atstovai rodo norą ir susirūpinimą, dėl savo sistemų ir duomenų apsaugojimo. Kibernetinių grėsmių augimas daro didelę įtaką investicijoms į siekį apsaugoti sitemas ir informaciją (Loishyn ir kt., 2021, p. 1448). Prasidėjus pasaulinei COVID-19 epidemijai, kas lėmė daugumos darbuotojų ir moksleivių persikėlimą dirbti ir mokytis nuotoliniu būdu. Praleidžiamas prie elektroninės erdvės ilgesnis laiko tarpas negu įprastai lėmė, šiuo laikotarpiu, elektroninių nusikaltimų išaugimą šešis kartus (Loishyn ir kt., 2021, p. 1450). Organizacinės kibernetinės saugumo kultūros tinkamas veikimas gali padėti užtikrinti saugumą, siekiant patirti kuo mažiau išorinių nuostolių ar kaip išvengti pakenkimo sistemoms ir duomenims.

Kuriant bendrą organizacinę kibernetinio saugumo koncepciją turėtų būti numatyta saugumo teisinė bazė, taip pat kokie yra koncepcijos pasiekimai ir galutinis tikslas, dalyviai ir jų įgaliojimai. Tai pradėti reikėtų apsibrėžiant skirtingų pareigybių priėjimą prie informacijos ir jos valdymą, išteklių ir rangovų numatymą, instrukcijų parengimą darbuotojas (Loishyn ir kt., 2021, p. 1451). Būtent darbuotojai yra apibrėžiami kaip silpniausia saugumo grandis, todėl kultūros skatinamas ir vienodas supratimas gali sumažinti riziką ir galimus su tuo susijusius nuostolius. Naudos galima pasiekti pritaikant metodus ir ugdant suvokimą apie skirtingas situacijas, taip organizacijų darbuotojai turėtų daugiau šansų žinoti kaip elgtis ir kokių veiksmų imtis vienoje ar kitoje situacijose (Leading Minds of Governance, 2019, p. 49).

Vystant kibernetinio saugumo kultūrą verslo sektoriuje ir pradedant kurti sistemą organizacijoje būtina taip pat atsižvelgti į:

1. Organizacijos vertybes;
2. Prielaidas, kas yra priimtina ir kas nepriimtina užtikrinant informacijos saugumą;
3. Koks žmonių elgesys ir veiksmai yra priimtini;
4. Koks yra žmonių supratimas saugumo srityje (Alnatheer, 2014, p 104).

Kuriama kibernetinio saugumo kultūra turi būti tinkama organizacijai, kuriai siekiama ją pritaikyti. Priešingu atveju sukurti procesai neduos norimų rezultatų. Įvertinus organizacinę ir darbuotojų aplinką galima priimti sprendimus, kurie būtų efektyvūs ir lengvai pritaikomi. Norimų tikslų pasiekti galima per mokymą, skirtingo lygio darbuotojams gali būti sudaryti skirtingo lygmens

kursai, jog žinios būtų suvienodintos. Šioje vietoje yra labai svarbus ir organizacijos vadovų palaikymas ir noras investuoti į kibernetinio saugumo kultūros plėtojimą. Darbuotojų kompetencijų tobulinimas organizuojant įvairius kursus, seminarus, skaitmeninio raštingumo mokymus gali tapti raktu į sėkmę kovojant su kibernetinėje erdvėje iškylančiomis grėsmėmis. Organizacinės kibernetinės saugumo kultūros lygis yra neatsiejamas nuo kiekvieno individualaus supratimo.

1.5. Individuali kibernetinio saugumo kultūra

Individuali kibernetinio saugumo kultūra apima žmonių asmeninius sugebėjimus operuoti skaitmeninėje erdvėje ir suprasti kaip reikia elgtis, bei valdyti įvairias iškylančias situacijas. Šiais laikais sunku surasti asmenį kuris vienokiu ar kitokiu būdu nebūtų susijęs su kibernetine erdve. Žmonės visa tai naudoja stengdamiesi pagerinti savo buitį. Kiekvienas joje nori jaustis laisvas, galėti reikšti savo nuomonę ir turinį rinktis pagal savo poreikius, tačiau svarbu nepamiršti jog prie teisių ir laisvių, turi būti pareiga ir supratimas kokių bendrų taisyklių reikėtų laikytis.

Šiais laikais vaikai išmanias technologijas pradeda naudoti būdami dar visai mažo amžiaus, todėl ne tik suaugę asmenys turėtų galvoti apie saugumo problemas, bet ir kaip tėvai turėtų apsaugoti savo vaikus (Pătrașcu, 2019, p 278). Neribota prieiga prie elektroninės erdvės sukelia daug iššūkių, tiek kibernetinių, tiek socialinių. Socialiniai iššūkiai apima tas sritis, kurios teigia, jog elektroninės erdvės netinkamas ir neatsakingas naudojimas gali daryti didelę neigiamą įtaką vartotojo psichologinei būsenai. Todėl vartotojas turi suprasti kaip apsaugoti save ir savo aplinkos asmenis.

Vartotojai sąveikaudami su elektronine erdve turi prisidėti prie pagrindinių kibernetinio saugumo pagrindinių principų išlaikymo. Nors dauguma žmonių kritiškai nevertina savo veiksmų, tačiau norint sustiprinti saugumą, tai privaloma daryti visapusiškai, kad įvyktų kuo mažiau žmogiškojo faktoriaus klaidų.

Šiais laikais jautri tema yra žmogaus asmeninės informacijos sauga. Yra pastebima daug atvejų kuomet asmenų duomenys yra renkami, tačiau netinkamai tvarkomi, todėl kyla įvairių nesusipratimų kuomet informacija yra atskleidžiama, ištrinama ar kitaip pakeičiama. Naudodamiesi išmaniosiomis technologijomis vartotojai net ir siekdami apsaugoti savo asmeninius duomenis susiduria su jų paviešinimo atvejais (Da Veiga, 2016, p. 1007). Iškyla paradoksas, jog vartotojai reiškia didelį susirūpinimą kaip bus tvarkomasi su jo pateiktais duomenimis, kai to reikalaujama pavyzdžiui, užsakant tam tikras paslaugas, bet patys individai labai daug informacijos atiduoda į viešą erdvę patys. Todėl matoma, jog vis dar trūksta kritinio mąstymo, kur ir kokius duomenis pateikti yra reikalinga, o kokių ne.

Individualus lygmuo yra pats žemiausias, tačiau pamatinis, kuris daro didelę įtaką aukštesniems kibernetinio saugumo kultūros lygmenims. Stiprinant individualius įgūdžius yra ugdomas kritinis

mąstymas ir gebėjimai tinkamai reaguoti į įvairias iškylančias situacijas. Kuomet vartotojas yra raštingas kibernetinėje saugumo srityje ir turi supratimą jo gebėjimai gali užkirsti kelią grėsmėms iškylančioms tiek organizaciniame, tiek nacionaliniame lygmenyje. Kibernetinio saugumo kultūrą palaikantys, stiprinantys ir kūrimą užtikrinantys aspektai yra: vartotojų požiūris, įsitikinimai, vertybės, žinios ir žinojimas, kas padeda skatinti naujoves, tačiau taip pat išlaikyti konfidencialumą, privatumą ir ginti piliečių teises (Da Veiga, 2016, p. 1008). Įgyvendinant kultūrą numatant šias gaires, bei pritaikant tinkamą edukavimą būtų pasiekiamas daug didesnis saugumo lygmuo visuose kibernetinio saugumo kultūros lygmenyse.

2. KIBERNETINIO SAUGUMO KULTŪROS TEORINIS KONCEPTAS

Kibernetinio saugumo kultūra yra labai svarbus aspektas šių dienų gyvenime, todėl norit išlaikyti save kuo labiau nepažeidžiamais elektroninėje erdvėje šiuos įpročius privaloma ugdyti nuo pat vaikystės. Kibernetinė sveikata, kaip asmeninė higiena, kurios laikytis privaloma kiekvieną kartą prisijungus prie elektroninės erdvės. Skaitmeninis raštingumas, turi padėti supažindinti ir įgalinti tinkamą vartotojo elgesį elektroninėje erdvėje. Jaunimą į skaitmeninio pažinimo pasaulį turi vesti tėvai, mokytojai ir kiti subjektai gebantys padėti suprasti ir susipažinti su jame esančiomis galimybėmis, procesais, bei slypinčiomis grėsmėmis.

Kibernetinę kultūrą sudaro žmogiškieji faktoriai, vartotojo žinios ir žinojimas, bei elgesys (Gcaza ir von Solms, 2017, p. 98). Galima teigti, kad du pagrindiniai aspektai palaikantys kibernetinio saugumo kultūrą yra suvokimas ir mokymas, turint šių faktorių stiprų pamatą žmogiškųjų klaidų rizika tampa vis kokybiškiau suvaldoma. Išugdyti įpročiai jauname amžiuje tampa rutina kasdienoje ir besikeičiant tendencijomis yra lengviau prie jų prisitaikyti.

2021 metų sausio mėnesio duomenimis pasaulyje yra 4,66 milijardai aktyvių interneto vartotojų iš jų 4,2 milijardai yra aktyvūs socialinės erdvės naudotojai (Johnson, 2021). Pasaulinis interneto vartotojų procentas yra 59,5 (Johnson, 2021). Pateiktoje statistikoje Europa pirmauja turėdama daugiau nei 95% interneto vartotojų (Johnson, 2021). Aukštas socialinės erdvės naudotojų skaičius rodo kaip pasikeitė šiandieninės tendencijos ir popierinius laikraščius pakeitus elektroninės erdvės priemonėmis, visa žiniasklaida ir informavimo įrankiai buvo perkelti į kitą lygmenį. Žymiai laisvesnis ir greitesnis dalinimasis informacija atveria naujų galimybių žmonėms kurti ir skleisti savo mintis vis didesnei auditorijai. 2019 metais prasidėjus COVID-19 epidemijai, pasauliui užsidarius, vartotojai buvo ir yra priversti leisti žymiai daugiau laiko internetinėje erdvėje. Karantino laikotarpis visiems tapo iššūkiu, kuomet formalųjį kontaktinį mokymą turėjo pakeisti nuotolinis, pritaikant elektronines platformas ir keičiant mokymosi formatą (Mishra, Gupta ir Sheree, 2020, p. 2). Esama situacija privertė jaunimą sumažinti kontaktinį bendravimą ir dar aktyviau persikelti į elektroninę erdvę.

Šiame skyriuje siekiant atskleisti kibernetinio saugumo koncepciją bus apžvelgiama kokios grėsmės slypi skaitmeninėje erdvėje, kokios priemonės gali sumažinti susidūrimą su rizikomis, kaip turėtų veikti mechanizmas siekiant apsaugoti vartotojus. Taip pat bus apžvelgiamos JAV, bei Baltijos šalių situacija kibernetinio saugumo kultūros plėtojime ir mokyme.

2.1. Socialinė medija ir naudojimo rizikos

Internetinė socialinė erdvė, kaip įrankis teikia daug teigiamų galimybių supaprastinančių veiklą:

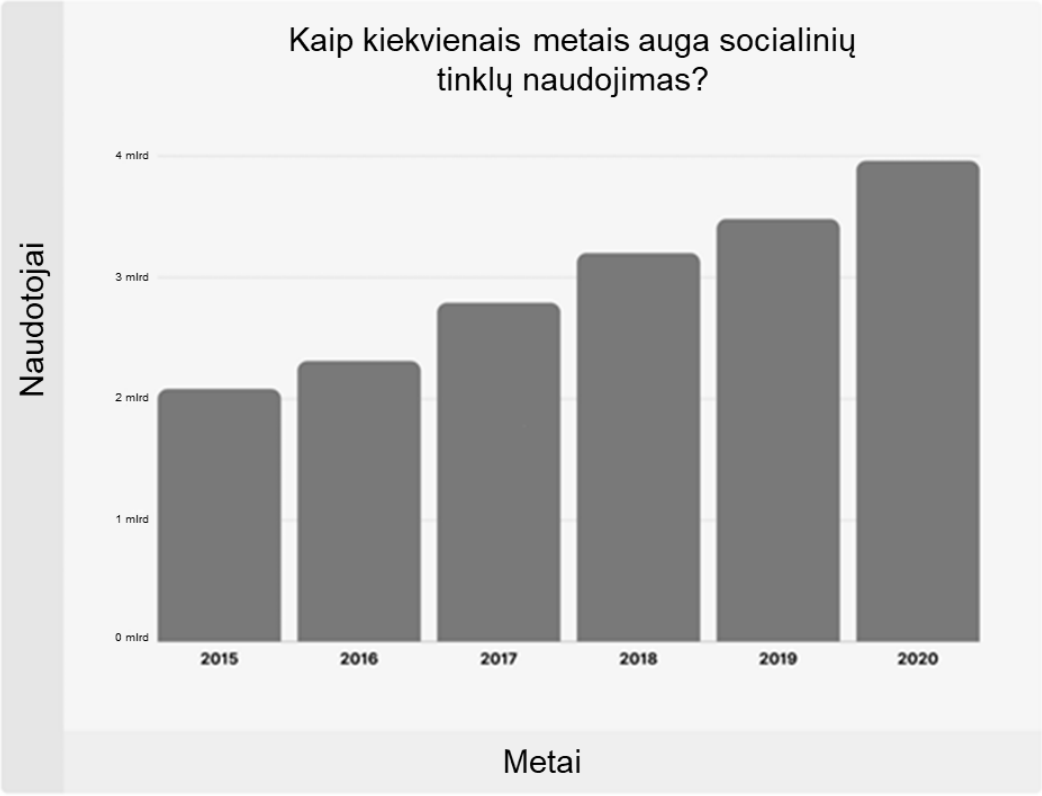
padeda patogiai susijungti žmonių grupėms, greitai dalintis informacija, kurti savo individualų turinį, kuris būtų pasiekiamas didelei auditorijai. Priklausomai nuo poreikių naudojantis suteikiamomis galimybėmis individai turi galimybę pasiekti tikslų, pavyzdžiui rasti reikalingą informaciją, mokytis, bendrauti ir bendradarbiauti, vystyti prekybą, kurti internetinį turinį, be didelių techninių išteklių. Pagrindinės išskiriamos socialinės medijos kategorijos yra šios (Cross, 2014, p. 3-15):

1. Bendradarbiavimo projektai (angl. *collaborative projects*) – puslapiai, prie kurie vartotojams leidžia prisidėti prie turinio kūrimo ir papildyti esamą turinį naujais faktais. Vienas iš plačiai žinomų tokio tipo projektų yra *Wikipedia*;
2. Blogai – platformos, kur asmenys gali pateikti savo mintis ir išsakyti nuomonę, požiūrį iš savo perspektyvos. Paskelbti įrašai dažniausiai turi laiko ir datos žymas, kiti vartotojai turi galimybę reaguoti į paskelbus įrašus komentuodami ar dalindamiesi informacija;
3. Bendro turinio bendruomenės (angl. *content communities*) – tai yra svetainės, kuriose yra dalinamasi daugialypės terpės (angl. *multimedia*) turiniu. Tokį turinį sudaro kelių komunikacijos tipų (teksto, vaizdo, garso failų, animacijos) kombinacija (Sarokin, 2021). Vartotojai kelia savo turinį: vaizdo įrašus, paveiksliukus ar kitą turinį pateikdami jo aprašymą, jog kiti vartotojai galėtų lengviau surasti ir peržiūrėti. Taip kuriamos bendruomenės, kurie peržiūrėdami turinį įsitraukia į diskusijas komentarų skiltyje. Vienas iš plačiai žinoma tokio turinio bendruomenių platforma yra *YouTube*.
4. Socialiniai tinklai – platforma, kurioje vartotojai prisijungdami prie tinklo naudoja savo asmeninius profilius. Platformoje leidžiama pateikti informaciją apie save, dominančius dalykus, kas padeda vartotojams susiburti į grupes, kur jie galėtų bendrauti ir dalintis informacija;
5. Virtualūs žaidimai (angl. *virtual game world*), virtualūs socialiniai pasauliai (angl. *virtual social worlds*) – simuliuojama erdvė, kuri sujungia didelę dalį vartotojų, kurie save pristato pasirinkdami ikoną ir slapyvardį. Virtualių žaidimų erdvėje tik yra nagrinėjamas simuliuojamas pasaulis, bet dalyvaujama įvairiose veiklose, žaidžiama, bet ir suteikiama galimybė komunikuoti su kitais vartotojais.

Neribotos galimybės palengvina kasdieninę veiklą, tačiau visa tai slepia ir dideles rizikas. Pateikta informacija gali būti neteisingai suprasta, pavogta, būti panaudota prieš kūrėją. Verta paminėti jog labai dažnai apie kibernetinį saugumą yra kalbama kaip apie suvokimą kaip reikia apsaugoti informaciją, tačiau šios nėra tapačios. Kibernetinis saugumas ir informacijos saugumas, tai įrankių visuma, siekiant apsaugoti informaciją nuo įvairių grėsmių ir pažeidžiamumo, o kibernetinis saugumas yra nebūtinai tik pačios skaitmeninės erdvės apsauga ar tų, kurie veikia joje, bet ir bet kokio turto, kurį galima pasiekti naudojantis virtualia aplinka (von Solms ir van Niekrek, 2013, p. 101). Kibernetiniai nusikaltėliai išnaudodami kompiuterines technologijas siekia daryti tiesioginę įtaką vartotojui naudojant internetą, elektroninį paštą, pokalbių svetaines, siekiant įvairių veikų kaip asmens tapatybės vagystės ar šantažavimas ir nusikaltimai prieš žmogaus privatų gyvenimą.

Socialinės medijos pagrindinis tikslas informuoti visuomenę ir siųsti tam tikras žinutes, tačiau iš to iškyla grėsmė, jog esant dideliam informacijos srautui yra ypatingai paprasta sklisti ir apgaulingai ar melagingai informacijai. Didelis dėmesys yra atkreipiamas būtent į socialinius tinklus, kurių naudojimas auga kiekvienais metais (2 pav.). Socialiniais tinklais naudojasi 50,64% žmonių pasaulyje ir iš jų vyresnių nei 13 metų auditorijoje 63% yra aktyvūs vartotojai ir šis skaičius auga kiekvienais metais (Dean, 2021). Kuo daugiau vartotojų jungiasi, tuo sudaromos paprastesnės sąlygos pasiekti asmenis kaip tikslinius ar netikslinius taikinius.

Būtent socialiniai tinklai yra išskiriami, kaip turintys didelę kibernetinių rizikų grėsmę. Kibernetiniai nusikaltėliai rado potencialą socialiniuose tinkluose ne tik siekiant paleisti kenkėjiškas programas kaip reklamines programas sistemoje, esant tokiam dideliam kiekiui duomenų socialinių tinklų vartotojų paskirose ir įrašuose, jiems tai tapo konkurencinga rinka siekiant stebėti paskyrų pažeidimus ir inicijuoti tapatybės vagystes (Enescu, 2019, p. 183).



Šaltinis: išversta pagal Dean, 2021.

3 pav. Socialinių tinklų vartotojų augimas (2015 – 2020 m.)

Socialiniai tinklai suteikia daug laisvių realizuoti save, turėti ryšį su draugų ratu ar jį išplėsti, būti bendraminčių grupėse, užmegzti kontaktus kitais asmenimis (Miguel, Morales, Ynalye, 2020, p. 124). Toks laisvas informacijos pasiekimas atveria naujus kelius nedraugiškai nusiteikusiems individams ar kibernetiniams nusikaltėliams vykdyti įvairių formų nusikaltimus kaip: patyčios elektroninėje erdvėje,

kibernetinis apsimetinėjimas, tapatybės vagystės ir pan. Kalbant apie socialinių tinklų grėsmes, galima pastebėti jog socialiniai tinklai dirbtinai kuria neigiamą spaudimą jaunų žmonių tarpe, norint būti aktyviems ir atrodyti populiariems visą laiką (Ofcom, 2021, p. 8). Tai tik parodo, kodėl yra svarbus kritinio mąstymo ir supratimo ugdymas siekiant formuoti gebėjimus atsirinkti informaciją, kuri yra pateikiama gražesniu formatu, tačiau ne visuomet atspindi tikrąją realybę.

Broadband komisija (2019), kurios tikslas yra naudojant skaitmeninio bendradarbiavimo galimybes kurti saugius ir tvarius elektroninio bendradarbiavimo paslaugas, nagrinėdama vaikų saugumą internete išskiria šias pagrindines rizikas su kuriomis dažniausiai yra susiduriama socialiniuose tinkluose ir internete bendrai (4 pav.) (Gegenheimer ir kt., p. 31–34):

1. Kontaktinės rizikos: viliojimas, kibernetinės patyčios, persekiojimas ir priekabiavimas;

Kibernetinės patyčios yra viena vaikų teisių pažeidimo formų elektroninėje erdvėje. UNICEF kibernetines patyčias apibrėžia kaip elektroninių žinučių panaudojimą siekiant grasinti, bauginti ar kitaip atakuoti kitą asmenį (Gegenheimer ir kt., 2019, p. 31). 2015 m atliktame tyrime JAV, kur buvo tiriami 457 mokyklinio amžiaus vaikai nuo 11 iki 15 metų pateikia, jog 34,4% yra identifikuojami kibernetinių patyčių aukos arba jas patyrę individai, o 14,6% yra patys tyčiojęsi kibernetinėje erdvėje. Australijoje apie 11% jaunuolių nuo 10 iki 17 metų amžiaus yra patyrę patyčias. Europos sąjungoje 12% vaikų identifikuojami kaip patyrę patyčias. Didžiausia rizika iškyla tuomet kai šis reiškinys tampa vaiko paslaptimi, tai yra sunku pastebėti ir padėti aukai (Gimenez, Luengo, Bartrina, 2017, p 536).

Kitas kibernetinių patyčių aspektas yra virtualus seksualinis priekabiavimas. 2017 metais atliktame tyrime Danijoje, Vengrijoje ir Didžiojoje Britanijoje duomenys atskleidė jog 6% iš tirtųjų vaikų nuotraukos buvo pasidalintos be jų leidimo, 25% buvo skleidžiami gandai apie jų seksualinį gyvenimą ir 31% yra matę, kaip jų amžiaus paaugliai susikuria netikrus socialinius profilius, jog pasidalintų savo seksualinio pobūdžio nuotraukomis su trečiosiomis šalimis (Gegenheimer ir kt., 2019, p. 46).

Viliojimas internetinėje erdvėje yra apibrėžiamas kaip procesas, kurio metu suaugęs žmogus užmezga santykius su vaiku, siekdamas palengvinti internetinį ar neinternetinį seksualinį kontaktą (Gegenheimer ir kt., 2019, p. 46). Tokio pobūdžio rizika yra ypatingai pavojinga ir tai gali būti pirmtakas nusikalstamai veikai, kuomet jaunam žmogui gali kilti tiek psichologinių tiek gyvybiškai svarbių pasekmių.

2. Turinio rizikos: pornografija, vaikų seksualinės prievartos medžiaga, žiaurumai, žaidimai ir azartiniai lošimai;

Internete turinys turi būti filtruojamas, jog netinkamas, žeidžiantis ar nusikalstamos veikos pobūdžio informacija nepasiektų vartotojų, o ypatingai vaikų. Kai kuris turinys internete yra leidžiamas, bet nepritaikytas jaunajai auditorijai, kas galėtų daryti žalą psichologinei sveikatai ir

sukelti emocinius sutrikimus. Tokio pobūdžio turinį vis labiau prieinamu padarė socialiniai tinklai ir nuotraukų dalinimosi programos (Martellozzo, Monaghan, Davidson, Adler, 2020, p 1).

Viena populiariausių vaizdo įrašu platformų *YouTube* naudodami asmenys iki pilnametystės, turėtų pasiekti „gerą“ turinį: skirtą mokymuisi, tobulėjimui, sveikatos klausimams, tvarkymuisi su nerimo klausimais, saugios seksualinės sveikatos praktikavimą, informacijai apie medicinines rekomendacijas gauti. Tačiau kai kurie tyrimai pranešė, apie platformos naudojimą ir turiniui įvadintam kaip „blogas“ peržiūrėjimą (Hattingh, 2021, p. 2). Platformoje galima rasti visiems prieinamų vaizdo įrašų, kuriuose yra propaguojamas rūkymas, alkoholio vartojimas, kūno apnuoginimas, patyčios, savęs skriaudimas ar nusižudymas, narkotikai ir kitos grėsmės. Tėvai ar globėjai turėtų susirūpinti dėl turinio, kurį peržiūri jų vaikai. Kai kuriuose vaizdo įrašuose taip pat yra skelbiami pranešimai tėvams, jog jie turi užtikrinti, kad jų vaikai netaptų apatiški dėl per didelio panašaus turinio žiūrėjimo, nes dažnai jaunimas nesuvokia galimų pasekmių ir netinkami vaizdo įrašai jiems atrodo kaip linksmas dalykas (Hattingh, 2021, p. 8).

Nors daugelis reguliavimo aspektų priklauso pačioms tinklų platformoms, tačiau didelė dalis turinio gali nebūti įvertinta kaip kelianti riziką, todėl tėvai ar globėjai turi būti patys filtruoti, koks turinys yra peržiūrimas ir stengtis apsaugoti savo vaikus, nuo galimo žalos.

Didžiojoje daugumoje pasaulio šalių nepilnamečiams asmenims azartiniai lošimai yra uždrausti ir jie įleidžiami į lošimų namus. Tačiau plėsdami rinkas verslininkai perkėlė azartinius žaidimus į internetines platformas. Nors dauguma Rizika iškyla ten, jog net internetinis puslapis turėtų amžiaus apribojimus, jungiantis internetu savo amžių yra sufalsifikuoti lengviau, negu tai būtų bandoma padaryti realiai.

3. Elgesio rizikos: piktnaudžiavimas duomenimis, finansinis piktnaudžiavimas ir netinkamas elgesys;

Kai kurie puslapiai ar socialiniai tinklai turi amžiaus limitus, prie kurių vaikai negali prisijungti arba tam reikalingas globėjo sutikimas, jog įpareigojimai būtų ribojami pagal amžių. Pavyzdžiui *YouTube* apriboja turinį, kuris nebūtinai yra žeidžiantis, bet netinkamas žiūrovams iki 18 metų, paprašydami prisijungti prie savo *Google* paskyros, jog amžius būtų patvirtinamas ir esant jaunesnio amžiaus asmeniui arba neprisijungus prie paskyros vaizdo įrašo nebus leista peržiūrėti („Age-restricted content“, 2021). Nors sistemos yra sukurtos, jog turinys būtų filtruojamas ir neperžiūrimas tam tikroms grupėms, realybė yra kiek kitokia, nes dalis jaunų asmenų norėdami patenkinti savo smalsumą susikuria anketas patvirtinimui su netikru amžiumi. Šiuo atveju tėvai turėtų taip pat rodyti atsakomybę ir paaiškinti kodėl yra reikalingi amžiaus apribojimai, bei dalyvauti su vaiku jo paskyros anketos kūrime, jog kuo labiau padėtume jaunimui saugiai jaustis internete.

Mokslininkai aiškinasi kaip socialinių tinklų vartotojai suvokia informacijos privatumą prieš naudą būti socialinio tinklo nariu. Buvo atliktas tyrimas, kuris parodė, jog apklausus vartotojus jiems

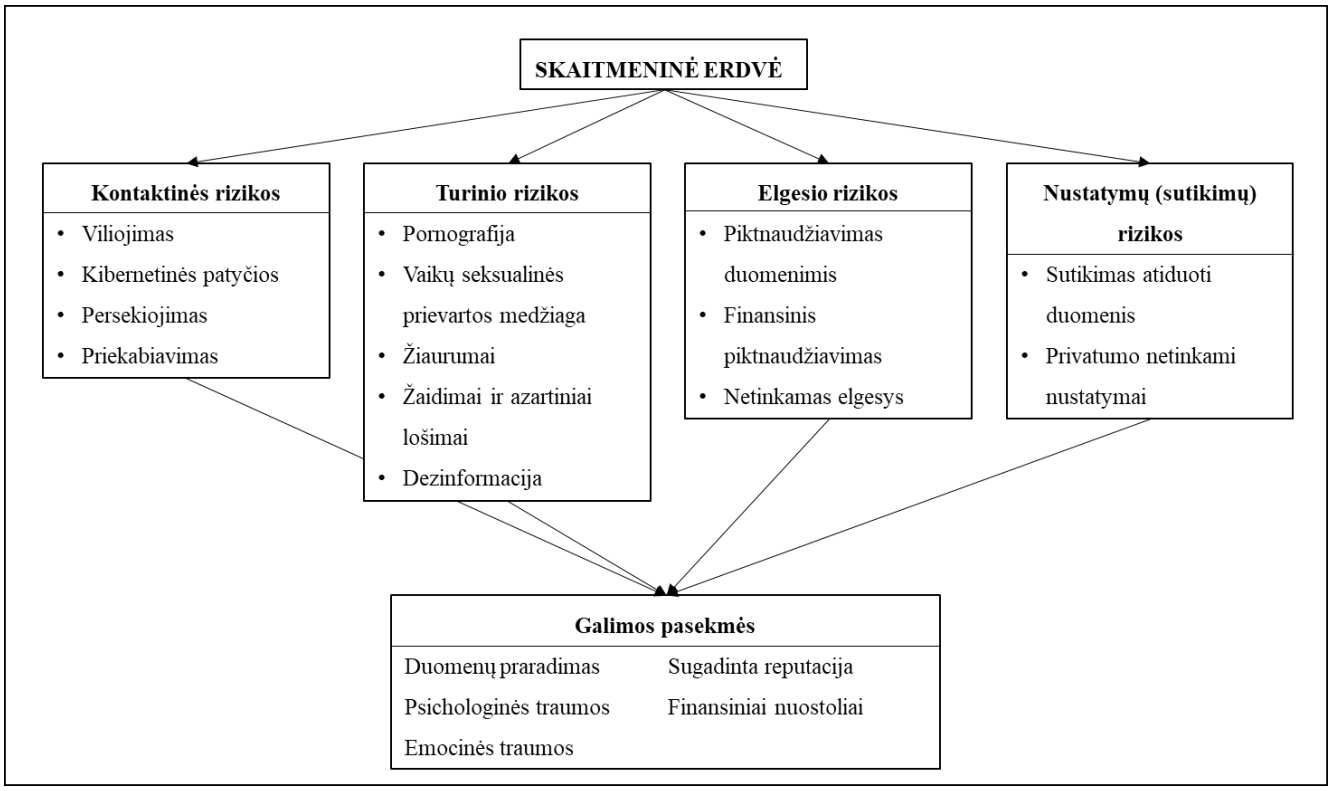
rūpi būti atsakingiems už tai kokia informacija dalinasi ir savęs atskleidimas yra privatumo kompromisas pagrįstas sąmoningumu, tačiau didžiausią nerimą kelia tai, jog jų tapatybe gali piktnaudžiauti trečiosios šalys (Presthus ir Vatne, 2019, p. 46). Facebook platformoje yra susiduriama su privatumo paradoksu, dalis naudotojų supranta apie galimą žalą atskleidžiant savo duomenis, bet gaunama nauda yra didesnė, todėl dažnu atveju rizikuoja savo privatumu (Presthus ir Vatne, 2019, p. 41). Vienas didžiausių duomenų nutekėjimo skandalų atskleistas 2018 metais, kuomet duomenų analizės bendrovė „Cambridge Analytica“ kompanija be aiškaus sutikima galėjo pasiekti apie 87 milijonus *Facebook* vartotojų asmeninių duomenų be vartotojų sutikimo ir sukūrė psichografiškai pritaikytus skelbimus, kuriais tariamai buvo siekiama paveikti žmonių balsavimo pasirinkimus 2016 m. JAV prezidento rinkimuose (Hindsa, Williamsb ir Joinson, 2020, p. 1). Tyrimas, kaip vertinamas toks duomenų nutekėjimas, atskleidė, jog kaip pažeidimą vartotojai laiko tai kas labiau apčiuopiama, nematoma realybė tiek nerimo nekelia, kuri gali būti dar labiau pažeidžiama (Hindsa, Williamsb ir Joinson, 2020, p. 10).

Didžiausias iššūkis yra paaiškinti mokiniams koks yra svarbus tinkamas elgesys skaitmeninėje erdvėje. Dažnai jaunuoliai turi būti įtikinti jog jų požiūris į privatumą riboja jų galimybes apsaugoti savo duomenis nuo išnaudojimo ir jog jie turi tiksliai įvertinti riziką, kurią jie prisiima aukodami privatumą internetinėje erdvėje (Reilly, 2021, p 3).

4. Sutarties, sutikimų su nuostatomis rizikos.

Grėsmė, kuri iškyla daugumai vartotojų, tai parsisiunčiamos aplikacijos ar prisijungimas, prie tinklapių, kuriuose reikalinga registracija – duomenų atidavimas trečiosioms šalims. Nors Europos Sąjungoje galioja Europos Sąjungos Bendrasis duomenų apsaugos reglamentas, kuris siekia apriboti trečiųjų šalių veiklą, tačiau yra išlygos kuomet informaciją leidžiama rinkti (Binns, 2018, p. 2). Todėl priklausomai nuo programėlės patikimumo, ne visuomet yra žinoma kur nukeliauja duomenys asmens teikiami duomenys. Mobilieji įrenginiai ar kompiuteriai neatsižvelgiant į jų prekės ženklą ar įdiegtą operacinę sistemą naršant internete nėra saugūs. Išmaniuosiuose įrenginiuose daugumoje aplikacijų, net ir iš anksto įdiegtų, gali slypėti kibernetinės grėsmės pavojus (Enescu, 2019, p. 183).

Didelė dalis vaikų, taip pat ir suaugusiųjų, dažnu atveju neturi supratimo kur jie registruojasi, kuomet atsisiunčia aplikacijas neįvertinę jų reitingo arba neįvertinę rizikos, kad jos gali būti ne visiškai patinimo arba jungiasi prie abejotinos reputacijos paskyrų. Didžioji dalis privatumo politikų ar kitų sąlygų yra parašytos teisine, sunkiai suprantama kalba, todėl ne tik jaunimui, bet ir suaugusiems kartais yra sunku suprasti su kuo jie sutinka registruodami savo paskyrą (Gegenheimer ir kt., 2019, p. 34). Vartotojai turėtų kritiškai įvertinti ar verta ir kokius asmens duomenis pateikti registruojantis ar kuriant savo asmenines paskyras įvairiose programėlėse ir interneto svetainėse.



Šaltinis: adaptuota pagal Gegenheimer ir kt., 2019, p. 31–34

4 pav. Skaitmeninės erdvės rizikos ir galimos pasekmės

Susidūrus su rizikomis skaitmeninėje erdvėje ir tinkamai negebant į jas reaguoti vartotojai gali neišvengti ir pasekmių, kurios palies juos asmeniškai. Neatsargiai elgiantis su sistemomis gali būti prarasti ar sugadinti duomenys. Atskleidus tam tikrus asmeninius duomenis, tai gali pakenkti asmens reputacijai nepriklausomai nuo jo statuso visuomenėje, tai ypatingai pavojinga vaikams, nes jie lengvai gali tapti patyčių objektu kas gali sukelti emocines ar psichologines problemas. Vartotojai neatsargiai vertinant informaciją gali lengvai pakliūti į sukčių pinklias ir patirti finansinių nuostolių.

Nepaisant visų galimų rizikų naudojimosi skaitmenine procentas išlieka aukštas ir jis vis didės, todėl visiško saugumo užtikrinti vartotojui yra tiesiog neįmanoma, nes galime susidurti tiek su matomomis, tiek su nematomomis grėsmėmis. Kiekvienas turi kritiškai atsirinkti turinį kurį pasiekia ir kuriuo naudojasi. Siekiant didinti saugumą vartotojams apie tai reikia kalbėti ir dalintis aktualia informacija, o taip pat prie to veiksmingai gali prisidėti kibernetinė higiena.

2.2. Kibernetinė higiena

Siekiant sumažinti nesaugaus skaitmeninio pasaulio rizikas, individai turėtų pradėti nuo savęs ir savo įpročių formavimo, todėl elektroninės erdvės saugumas yra pradėtas lyginti su mūsų kasdiene sveikata. Kibernetinę higieną sudaro nustatymas ir išlaikymas svarbių kibernetinės sveikatos įpročių.

Kibernetinę sveikatą sudaro daugelis elementų pavyzdžiui kaip: nuolatinis grėsmių ar bandymų įsilaužti stebėjimas, slaptažodžių keitimas ir vienodų slaptažodžių vengimas, antivirusinės programos atnaujinimas, saugus internetinės informacijos rinkimas/ naršymas, tinkamų saugumo programų veikimas saugumą (Neigel, Claypoole, Waldfogle, Acharya, Hancock, 2020, p. 1). Kibernetinė higiena yra svarbi norint išlaikyti kibernetinį saugumą, bet šios dvi sąvokos neturėtų būti laikomos kaip sinonimai. Kibernetinis saugumas yra tam tikri veiksmai, kurių imamasi siekiant išlaikyti saugumą ir išlaikyti atsparumą prieš kibernetines atakas, o kibernetinė higiena daugiau yra susijusi su žinojimu apie skaitmeninį saugumą ir praktika susijusia su siekiu didinti kibernetinį saugumą (Neigel ir kt., 2020, p. 1).

Daugelis ekspertų teigia, jog yra kibernetinės higienos trūkumas vartotojų tarpe, tačiau tai yra ganėtinai nauja tyrimų sritis, todėl nėra visiškai aišku kas kibernetinė higiena yra iš tikrųjų (Vishwanath ir kt., 2020, p. 1). Kibernetinė higiena labiausiai siejasi su naudotojais, kurie, turėdami menkus skaitmeninės erdvės naudojimosi įgūdžius ir nesilaikydami pagrindinių taisyklių, tampa pagrindiniu nusikaltėlių taikiniu norint įgyvendinti kenkėjiškus tikslus. Yra du pagrindiniai tyrimų keliai siekiant plėtoti kibernetinę higieną, tai: supratimas unikalių žmogaus faktorių, kas didintų kibernetinę higieną ir panaudojimas šių išvadų diskusijai individualius kibernetinės higienos skirtumus šiuolaikinėje kompiuterių ir informacinių sistemų mokslų programose (Neigel ir kt., 2020, p. 2).

Visuomenės sveikatos literatūroje higiena aiškinama kaip daugialypė sąvoka reguliuojanti įvairius elementus, kurie bendrai: apima asmens higieną, pateikiami gairių pavidalu tam, jog dėmesys būtų skiriamas tam, kad kiti žinotų kaip turi elgtis, apibrėžimai yra pateikiami plačiai ir apimantys kultūrinę tikrovę (Neigel ir kt., 2020, p. 2).

Pateiktus aiškinimus galima empiriškai pritaikyti ir kibernetinės higienos plėtojime jog kibernetinio saugumo higienos turėtų laikytis visi vartotojai siekiant išlaikyti informacijos saugumą ir vientisumą įrenginiuose, kuriuose veikia internetas nuo kibernetinių atakų pavojaus.

Mokslininkai nagrinėdami ir kibernetinės higienos galimas atšakas, suskirstė į penkis svarbiausius pogrupius, kur turėtų būti laikomasi rutininių taisyklių siekiant saugiai naudotis skaitmenine erdve: saugyklų ir įrenginių higiena, perdavimo higiena, socialinių tinklų higiena, autentifikavimo ir įgaliojimų higiena, elektroninio pašto higiena (Vishwanath ir kt., 2020, p. 9). Šios pateiktos kryptis galėtų būti pirminio mokymo gairės, kurios sukurtų sveiko dalyvavimo internetinėje erdvėje elgseną. Reikėtų nepamiršti diegiant kibernetinę saugumo kultūrą ir skatinant skaitmeninę higiena ją reikia pritaikyti esamų poreikių, todėl, kad kaip ir asmeninės higienos įpročiai gali skirtis esant: asmeniniams įsitikinimams apie technologijų naudojimą, skirtingam suvokimo lygmeniui apie kibernetinę saugumo kultūrą, esant skirtingiems skaitmeninio raštingumo sugebėjimams, todėl siekiant veiksmingų rezultatų individų kibernetinio lygio supratimas turėtų būti įvertintas ir periodiškai matuojamas norit suprasti ar yra taikomos tikslingos priemonės (Vishwanath ir kt., 2020, p. 9).

Su jaunimu apie kibernetinę higieną ir kibernetinio saugumo kultūros ugdymą reikia nuo pirmųjų dienų, kuomet jie pradeda naudotis skaitmenine erdve. Jauniesiems išmaniųjų technologijų naudotojams reikia aiškinti koks yra tikslas turėti saugius slaptažodžius, kodėl reikia saugiai elgtis internete, kaip veikia elektroninė erdvė. Su vyresniais mokiniais galima nagrinėti temas apie dabartinę situaciją, esamas kibernetines atakas, įvairius sukčiavimo būdus, kurie gali juos paveikti asmeniškai, pateikti praktinius pavyzdžius kas nutinka palikus savo paskyras prijungtas viešuosiuose kompiuteriuose ir kitus dažnai nutinkančius dalykus (Schwartz, 2018, p. 5).

Kaip ir asmeninė higiena, kurios laikytis vaikai turi būti skatinami nuo jauno amžiaus, tai ilgainiui tampa rutininiu įpročiu, taip pat ir kibernetinės higienos laikytis turi būti skatinama tik pradėjus naudotis skaitmeninėmis technologijomis, jog ilgainiui atliekami veiksmai elektroninėje erdvėje taptų įprasti ir būtų sumažinama galima rizika. Tačiau taisyklių laikymasis yra maža dalis visos sistemos, kuri veikdama užtikrintų saugų naudojimąsi skaitmenine erdve. Svarbus aspektas šalies mastu yra tinkamai veikianti kibernetinio saugumo ekosistema.

2.3. Kibernetinio saugumo kultūros diegimo ekosistema

Skaitmeninių technologijų vartotojai turi suprasti apie galimas grėsmes ir kaip į jas reaguoti, tačiau to nepakanka, valstybės mastu turėtų būti veikiantis modelis, kuris leistų užkardyti kylančioms grėsmėms arba jau atsiradusioms veikoms internetinėje erdvėje. *Broadband* (2019) komisija savo leidinyje apie vaikų saugumą internete pateikia saugaus interneto ekosistemos modelį (5 pav.), kurį šalys turėtų taikyti norint apsaugoti jaunimą nuo elektroninėje erdvėje slypinčių kibernetinių grėsmių.

Modelis apžvelgia reikalavimus pagrindinėms sritims norint sukurti saugią aplinką jauniems žmonėms. Patarimai apima šias pagrindinius dalyvius: valdžios, teisėkūros, ryšio tinklų reguliavimą užtikrinančias institucijas, kompanijas užtikrinančias elektronines paslaugas, bei mokymo organizacijas, kurios turėtų įsitraukti į veiksmų kūrimą ir sprendimų priėmimą siekiant užtikrinti tinkamą elektroninės erdvės reguliavimą (Gegenheimer ir kt., 2019, p. 56):

1. Valdžios organai turi priimti įsipareigojimus dirbti su trečiųjų šalių organizacijomis. Organizacijos dirbančios tarptautiniu mastu siekia padėti šalims diegti, bei sumažinti galimas rizikas. Bendradarbiavimas su tarptautinėmis organizacijomis reikalingas siekiant sužinoti naujausias iniciatyvas, technologijas skirtas kovai su patyčiomis elektroninėje erdvėje. Kitas svarbus aspektas nacionalinių iniciatyvų skatinimas. Nacionaliniuose kibernetinio saugumo planuose turi būti numatytos nuostatos, susijusios su vaikų apsaugos internete iniciatyvas, grindžiamos konkrečiais tikslais. Tai sudaro tiek iniciatyvas, kurių turėtų būti imtasi norint plėtoti saugumą, tiek iniciatyvos, kurios užkardytų kelią galimiems nusikaltimams;

2. Teisėkūros institucijos. Priėmimas tarptautinių konvencijų ir protokolų. Tai rodo šalies susirūpinimą esamomis problemomis ir įsipareigojimą priimti geriausią praktiką, įrankius, nuostatas, standartus, dalintis informacija, bei bendradarbiauti šiais klausimais su kitomis šalimis priėmusiomis įsipareigojimus. Pagrindiniai išskiriami tarptautiniai dokumentai apibrėžiantys vaikų saugumą internete yra šie: Jungtinių tautų vaiko teisių konvencija – įtvirtina įvairias vaikų teises, įskaitant pilietines, kultūrines, ekonomine, politines ir socialines teises; Jungtinių tautų vaikų teisių konvencijos dėl vaikų pardavimo, vaikų prostitucijos ir vaikų pornografijos protokolas – sistema skirta analizuoti požiūrį į vaikų seksualinės prievartos nusikaltimus; Budapešto konvencija dėl elektroninių nusikaltimų – pirmoji privaloma tarpvyriausybinė priemonė, skirta kovai su kompiuteriniais vaikų pornografijos nusikaltimais; Europos Tarybos konvencija dėl vaikų apsaugos nuo seksualinio išnaudojimo ir seksualinės prievartos – sprendžia vaikų seksualinės prievartos nusikaltimus ir internetinio viliojimo nusikaltimus.

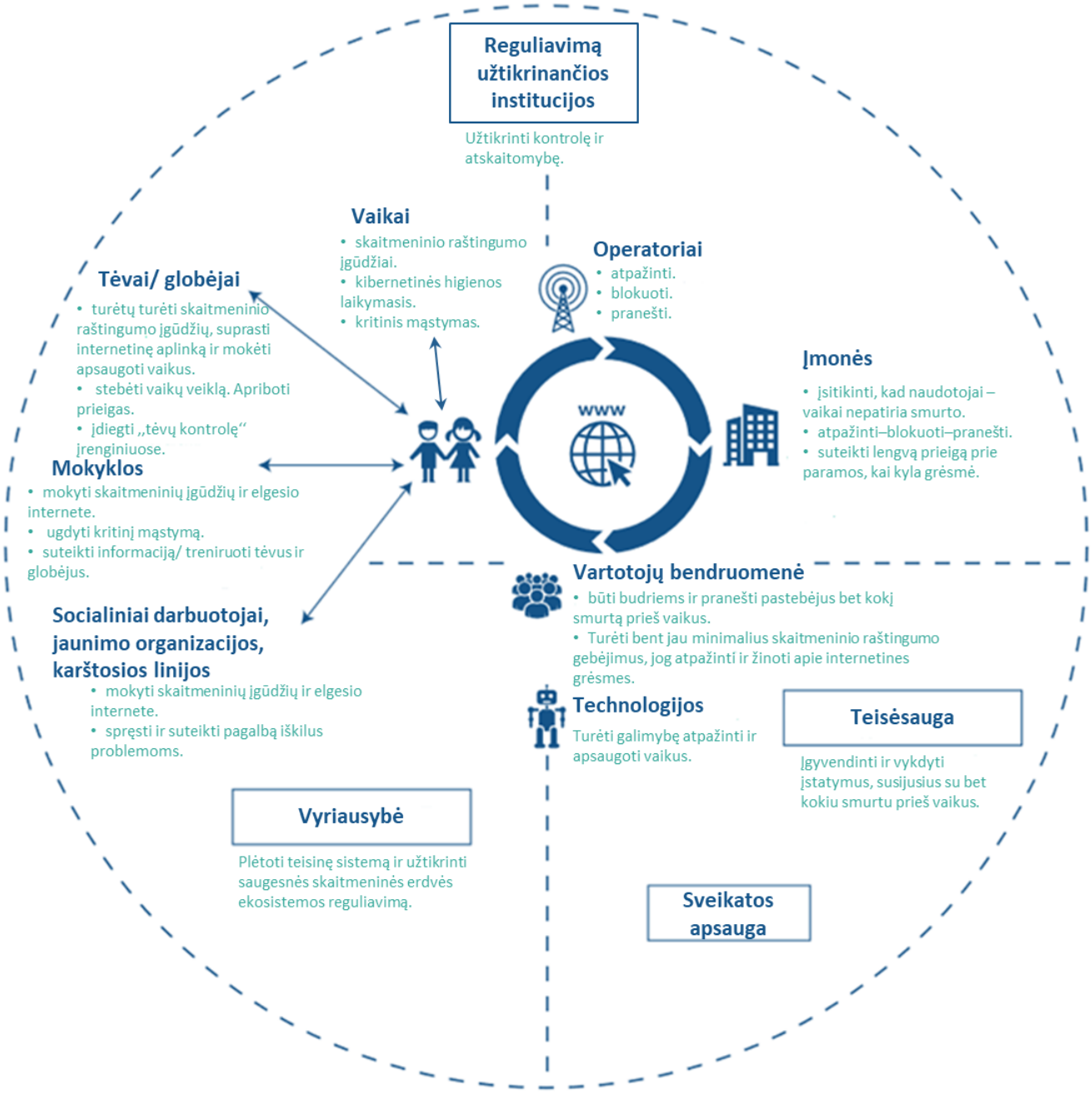
Tiek tarptautiniu, tiek nacionaliniu mastu svarbus yra apibrėžimų nustatymas kaip kiekviena sąvoka yra traktuojama, jog nebūtų interpretacijos, kaip suprantami kibernetiniai nusikaltimai ir kokios sudedamosios dalys į juos įeina. Taip pat šalys turi nusimatyti tinkamus standartus susijusius su duomenų apsauga, ypatingai kai tai liečia vaikų duomenis. Apibrėžimai ir taikymo sritys turėtų būti numatytos šalies įgyvendinančios Bendrąjį duomenų apsaugos reglamentą ir kitus nacionalinius teisės aktus.

3. Reguliavimą užtikrinančios institucijos turi būti atsakingos ir įsitraukti į skaitmeninio gerbūvio kūrimą vartotojams. Valdžia turi numatyti nacionalines pareigas, kurios būtų skirtos įvairiems su kibernetine erdve susijusių paslaugas teikiančių šalių atstovams, pavyzdžiui elektroninių ryšių tinklų tiekėjai ir pan. Paslaugas teikiančios įmonės šalyje turi priimti įsipareigojimus, jog vaizdo įrašai ar kita informacija susijusi su vaikų prievarta nebūtų rodomi įmonių valdomuose portaluose. Įmonės turėtų įsipareigoti jog įvykus tokiam aktui būtų galima gauti informaciją apie pažeidėją. Pastebėjus pažeidimus įmonės turėtų pranešti apie įtariamą pažeidėją, pačios pateikti informaciją, ištrinti esančią medžiagą iš interneto. Žaidimų kūrėjai turėtų įsipareigoti į savo kurią produktą įtraukti tėvų kontrolės nuostatas, suteikti informaciją apie amžiaus ribojimus naudotis produktu. Siekiant išvengti patyčių ir persekiojimo žaidimų platformų administratoriai turėtų sekti susirašinėjimų kambarius ir blokuoti vartotojus, kurie įtariami darantys pažeidimus.

4. Kompanijos, kurios teikia elektronines paslaugas turėtų individualiai užtikrinti vaikų apsaugą. Tai turėtų padaryti integruodamos į kompanijos politiką ir procesus vaikų teises, gaminamo produkto turinys turi būti tinkamas numatytam amžiui arba paskelbiami amžiaus apribojimai, įmonės turi mokyti vaikus kaip produktu naudotis atsakingai ir pateikti atitinkamas rekomendacijas.

5. Mokymo institucijos privalo prisitaikyti prie esamų skaitmeninio pasaulio pokyčių ir tinkamai teikti informaciją jaunimui kaip reikėtų elgtis internetinėje erdvėje. Kibernetinio saugumo

mokymas yra vienas pagrindinių ir svarbiausių šaltinių siekiant apsaugoti vaikus nuo galimų pavojų ir siekiant supažindinti su teikiamomis elektroninės erdvės galimybėmis.



Šaltinis: adaptuota pagal Gegenheimer ir kt., 2019, p. 56

5 pav. Saugaus interneto ekosistema

Valstybės tinkamas reguliavimas ir teisėkūros sukurti instrumentai gali padėti užkardyti galimas kibernetines grėsmes jog jaunimas nepatirtų galimos žalos. Tačiau vien reguliavimas negali apsaugoti, jei vartotojas nesupras galimų grėsmių. Europos Komisijos 2021–2027 m. skaitmeninio švietimo veiksmų plane „Švietimo ir mokymo pritaikymas prie skaitmeninio amžiaus“ pabrėžiama švietimo ir

mokymo svarba diegiant skaitmenines technologijas ir siekiant mažinti skaitmeninės atskirties rizikas (Europos komisijos komunikatas Europos Parlamentui, Tarybai, Europos Ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui, 2020). Todėl galima pridėti jog pats vartotojas turintis skaitmeninio raštingumo tinkamus įgūdžius, laikydamasis kibernetinės higienos ir kritiškai vertindamas pateiktą ar gaunamą informaciją gali išlikti saugus, todėl mokymas išlieka vienas svarbiausių aspektų norint suteikti tinkamas žinias. Viena svarbiausių rolių – tinkama edukacija, tenka mokytojams ir tėvams.

2.3.1. Mokytojo vaidmuo vystant kibernetinę saugumo kultūrą

Skaitmeninis raštingumas šiais laikais tapo toks pats svarbus kaip ir visi kiti dalykai mokomi mokykloje. Skaitmeninis gyvenimas yra dabartis ir norint paremti jaunimą reikia daugiau žinių nei paprastos rekomendacijos kiek laiko praleisti kibernetinėje erdvėje ar kaip susikurti patikimą slaptažodį. Tėvai ne visuomet turi supratimą apie kibernetinį saugumą ir įpročius elektroninėje erdvėje, todėl mokytojai yra vienas iš svarbiausių autoritetų, ruošiant jaunus žmones išnaudoti teigiamą potencialą ir įvertinti iškilusius iššūkius. Informacinių technologijų mokytojai yra įvardinami kaip vieni iš svarbiausių formuojant vaikų požiūrį ir elgseną naudojantis kompiuterinėmis technologijomis (Šimandl ir Vaniček, 2017, p. 1489). Šios specialybės pedagogai turi daugiausiai kompetencijų susijusių ne tik su skaitmeninės elgsenos žiniomis, bet ir technologinėmis. Būtent mokyklose turi būti skatinamas tinkamas požiūris į skaitmeninį raštingumą į kurio procesą turi įsitraukti visi mokytojai. Didžiausias atsakomybė, tai šviesti jauniausius mokinius diegiant įpročius kas yra tinkamas elgesys ir kritinis mąstymas siekiant jiems būti saugiems (Šimandl ir Vaniček, 2017, p. 1491).

Mokytojų, šviečiančių jaunimą, patirtis, susidaro iš išorinių, vidinių veiksnių, asmeninio požiūrio į elektroninio saugumo taisykles, apsaugos suvokimo barjerai, bei duomenų suvokimo (Šimandl ir Vaniček, 2017, p. 1492-1493).

Išoriniai veiksniai, tai dažniausiai susiję su pedagogo išoriniu pasauliu, kokia yra jo buvusi ir tobulinama dabartinė patirtis. Mokytojai turėtų šviestis patys, dalyvauti kursuose, siekiant keltis kompetencijas aktualiomis temomis susijusiomis su skaitmeniniu švietimu, taip pat bendradarbiavimu su administratoriais ar kitais informacinių technologijų specialistais, negalint išspręsti tam tikrų problemų.

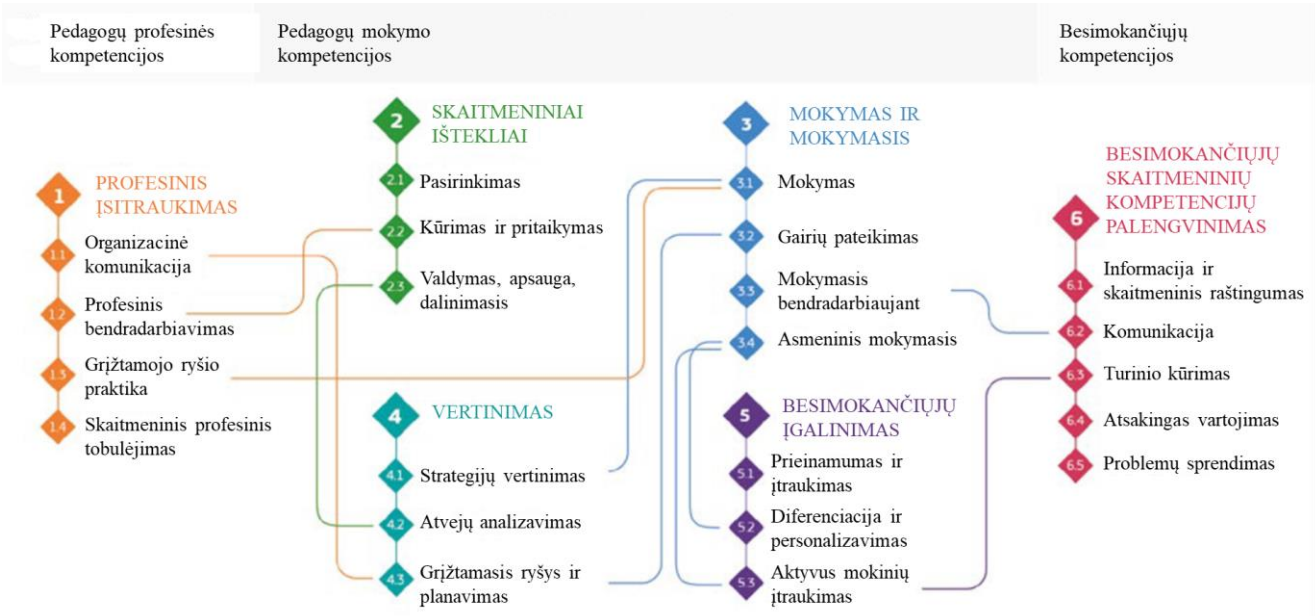
Negana to kokią patirtį mokytojas gauna iš išorinių veiksnių, tačiau yra labai svarbus jo paties požiūrį į saugumą. Vidiniai veiksniai apima jo pačio supratimą ir reagavimą į šių dienų grėsmes elektroninėje erdvėje, jo požiūrį į elektroninio saugumo taisykles ir turimus apsaugos suvokimo barjerus. Siekiant rodyti tinkamą pavyzdį, pedagogas turi ne tik nurodyti kaip reikėtų elgtis, bet ir pats rodyti pavyzdį laikydamasis numatytų taisyklių. Kai kuriais atvejais mokytojo žinių ar patirties

neturėjimas arba nesusidūrimas su kibernetinėmis problemomis gali sudaryti barjerus, kuomet pats nesielgs saugiai internete. Kitas svarbus aspektas, tai duomenų suvokimas, kuris apima žinojimą kokiais šaltiniais ar asmenimis elektroninėje galima pasitikėti, informacijos vertę – kas nutiktų, jeigu duomenys būtų prarasti, informacijos jautrumą – atskiria, kas yra jautrūs duomenys ir žino kaip juo tinkamai apsaugoti (Šimandl ir Vaniček, 2017, p. 1494).

Mokslininkas nagrinėjantis ką ne tik informacinių technologijų mokytojai turėtų žinoti apie skaitmeninį saugumą – Łukasz Tomczy (2019), pateikia keturias aktualiausias sritis: dalyko kompetencijos – suvokimas apie galimybes įtraukti informacinių technologijų dalykus mokant kitų disciplinų dalykų; metodinės kompetencijos – mokinių poreikių ir gebėjimų supratimas, siekiant įvykdyti tikslus susijusius su skaitmeniniu raštingumu; techniniai įgūdžiai – gebėjimas naudotis įrenginiais, programomis ir internetu; kompetencijos susijusios su asmeniniu ir profesiniu tobulėjimu naudojantis naujomis socialinės žiniasklaidos priemonėmis (p. 171). COVID-19 krizė ypatingai atskleidė technologijų naudojimo poreikį vykdant švietimą. Kaip pastebima 2021–2027 m. skaitmeninio švietimo veiksmų plane: „ekstremali situacija aiškiai parodė, kad visi pedagogai turi būti kompetentingi veiksmingai naudotis skaitmeninėmis technologijomis mokymo ir rengimo procese ir užtikrinti, kad visi vaikai galėtų dalyvauti skaitmeniniame švietime“ (Europos komisijos komunikatas Europos Parlamentui, Tarybai, Europos Ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui, 2020, p. 3). Šiuolaikiniame mokymo procese mokytojams iškyla pareiga pritaikyti skaitmenines technologijas mokyme, suprasti ir gebėti tinkamai valdyti įrankius.

Minėtame dokumente yra apibrėžiama visų pedagogų ir mokymo darbuotojų skaitmeninių gebėjimų įgūdžių svarba. Visų lygių pedagogų mokyme turėtų būti įtraukiami kibernetinio saugumo ir skaitmeninių įgūdžių parengimas. Vienas iš svarbių aspektų yra mokytojo tinkamas prisitaikymas prie šių dienų pasaulio ir besivystančių technologijų, gebėjimo tinkamai panaudoti skaitmeninius įgūdžius ir kūrybiškumą mokymo procese. Kita priežastis visų besimokančiųjų įtraukimas ir pagalba naudojantis elektronine erdve (Europos komisijos komunikatas Europos Parlamentui, Tarybai, Europos Ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui, 2020, p. 9).

Europos komisija identifikavus mokytojo indėlį į jaunų žmonių kibernetinio saugumo vystymą pateikė Europos skaitmeninių kompetencijų sistemą mokytojams *DigCompEdu*. Sistema skirta visų švietimo lygmenų atstovams nuo pradinio iki bendrojo švietimo, taip pat įskaitant suaugusiųjų, specialių poreikių turinčių asmenų, neformalųjį mokymą. Sistema yra siekiama sukurti bendrą pagrindą su atitinkamomis kompetencijomis švietimo teikėjams (European Framework for the Digital Competence of Educators, 2017). Kūrėjai pateikia šešias skirtingas sritis ir 22 kompetencijas (6 pav). Šios sritys apima mokytojų profesines kompetencijas, mokytojų pedagogines kompetencijas kaip technologijos integruojamos į mokymą, besimokančiojo kompetencijas – kurias turi gebėti perduoti mokytojas.



Šaltinis: išversta pagal European Framework for the Digital Competence of Educators (DigCompEdu). 2021.

6 pav. Mokytojų skaitmeninės kompetencijos

Pirmoji sritis (profesinis įsitraukimas) apimą efektyvų ir tinkamą mokyto gebėjimą naudotis technologijomis ir skaitmeninio mokymosi galimybes bendraujant ir bendradarbiaujant su kolegomis, mokiniais, tėvais ir kitais specialistais. Mokytojui svarbu gebėti vertinti individualiai ir grupėje savo mokymo praktiką, kritiškai vertinti skaitmeninių technologijų mokymo veiksmingumą ir tinkamumą.

Antroji sritis (skaitmeniniai ištekliai) apima gebėjimą pasirinkti skaitmeninius išteklius, kurti juos, pritaikyti, keisti ir valdyti. Tai apima gebėjimą suprasti asmens duomenų apsaugą pagal Europos Sąjungos Bendrąjį duomenų apsaugos reglamentą ir autorinių teisių įstatymų laikymąsi keičiant ir skelbiant skaitmeninius išteklius.

Trečioji sritis (mokymas ir mokymasis) apima skaitmeninių technologijų praktikoje planavimą, projektavimą ir naudojimą praktiniuose veiksmuose. Pagrindinis dėmesys skiriamas skaitmeninių išteklių ir metodų integravimui, skatinant skaitmeninių resursų integravimui siekiant skatinti bendradarbiavimo ir asmeninio mokymosi procesus.

Ketvirtoji sritis (vertinimas) apima konkretų skaitmeninių technologijų nagrinėjimą vertinant mokinių rezultatus ir mokymosi poreikius, siekiant visapusiškai išanalizuoti veiklos duomenis ir pateikti grįžtamąjį ryšį.

Penktoji sritis (besimokančiųjų įgalinimas) susijusi su mokymosi veiklos ir patirties kūrimu, kuris atitiktų mokinių poreikius ir leistų jiems aktyviai plėtoti savo žinias. Mokytojai naudodami skaitmenines technologijas turėtų skatindami individualizavimą skirtinguose mokymosi lygiuose ir mokymosi greityje. Tai skatina mokinius aktyviai įsitraukti į skaitmeninę veiklą, užtikrinant lygias galimybes naudotis technologijomis.

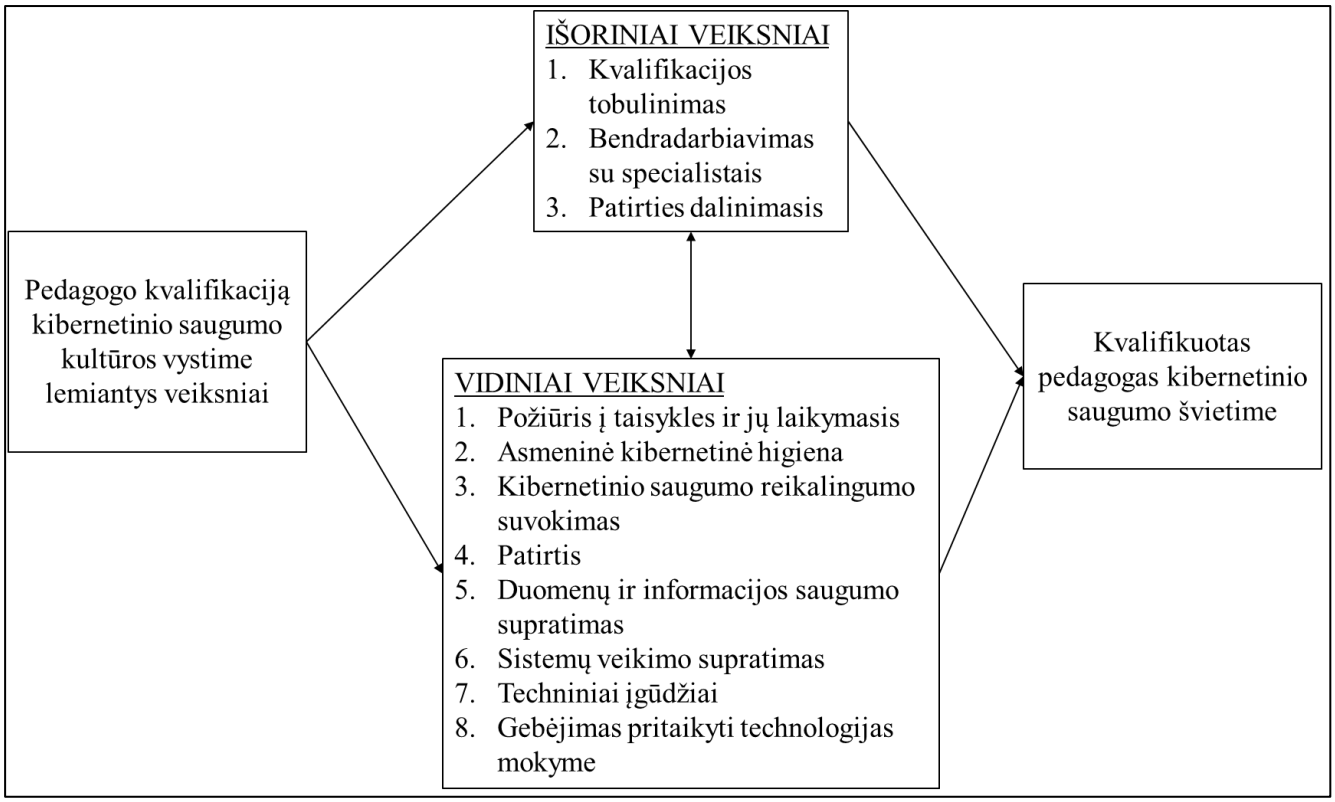
Šeštoji sritis (besimokančiųjų skaitmeninės kompetencijos palengvinimas) apima mokytojo kompetenciją skaitmeninėje srityje ir jo gebėjimą padėti mokiniams susiduriantiems su skaitmeninių įgūdžių trūkumais, jog jie galėtų saugiai naudotis elektronine erdve ir valdytų rizikas.

Mokytojai turėtų sugebėti pateikti reikiamą informacinį turinį ir skatinti medijos priemonių naudojimo raštingumą, bei integruoti veiklą, kad būtų galima spręsti skaitmenines problemas, kurti skaitmeninį turinį ir naudoti technologijas bendraujant bei bendradarbiaujant.

Europos skaitmeninių kompetencijų sistemoje mokytojų kompetencija gali būti įvertinta šešiais lygiais. A1 ir A2 lygis yra žemiausias – mokytojai paprastai yra tik pradėję naudotis technologijas, žino skaitmeninių technologijų galimybes siekiant tobulinti pedagoginę ir profesinę veiklą. B1 ir B2 lygmens mokytojai geba integruoti skaitmenines technologijas įvairias būdais ir kontekstais. C1 ir C2 – aukščiausio lygmens specialistai geba dalintis patirtimi su kolegomis, eksperimentuoti su naujoviškomis sudėtingomis technologijomis ir kurti naujus pedagoginius metodus bei vertinimo strategijas (DigComp, 2021).

Pedagogų skaitmeninė kompetencija pasireiškia ne tik gebėjimu naudoti skaitmenines technologijas mokymui tobulinti, bet ir gebėjimu jas tinkamai naudoti, valdyti duomenis, naudoti profesiniam bendravimui su kolegomis, tėvais, besimokančiais ir kitais suinteresuotais asmenimis, bei valstybės institucijomis užtikrinančiomis švietimo organizavimą ir kibernetinį saugumą. Reikalinga siekti tobulėti ne tik dėl asmeninio, bet ir kolektyvinio, organizacijos gėrio ir naujovių skatinimo.

Šių laikų mokytojas turi siekti įgauti skaitmenines kompetencijas, jog galėtų komfortiškai jaustis mokydamas jaunus žmones, kurie vejasi ir įsisavina naujų technologijų tendencijas labai greitai, tačiau panagrinėjus kiek pačio mokytojo, kaip asmens indėlis lemia ir daro įtaką mokymo procesui ir patirties perdavimui, pastebima, jog didelę įtaką daro pedagogo asmeninis požiūris, asmeninė patirtis ir suvokimas apie kibernetinį saugumą ir kylančias grėsmes. Didžiausios problemos yra tai, jog ne visuomet mokytojai žinodami taisykles kaip turėtų elgtis elektroninėje erdvėje, jų laikosi arba netgi negatyvi patirtis neskatina jų keistis. Išoriniai veiksmai, kaip savišvieta, domėjimasis naujomis tendencijomis ir kvalifikacijos kėlimas stiprina vidinius veiksnius, todėl pedagogas nuolatos būti supamas šių dviejų aspektų, kuriuos galima pavaizduoti schematiškai (žr. 7 pav.) ir turėtų savo elektroninėje rutinoje kaip įmanoma laikytis rekomenduojamų taisyklių, skatinti šviesti vaikus ir taip pat dalintis savo neigiama patirtimi pristatydami kaip jie elgėsi tam tikrose situacijose, jog jauni kibernetinės erdvės vartotojai vystytų suvokimą ir plėtotų kritinį mąstymą kaip elgtis įvairiose iškylančiose situacijose.



7 pav. Išorinių ir vidinių veiksmų įtaka pedagogo kvalifikacijai

Pedagogai ne tik patys turi būti raštingi skaitmeninėje erdvėje, tačiau taip pat jie turi būti susipažinę kokią įtaką: psichologinę, fizinę, teisinę (privatumo pažeidimai, persekiojimas) gali daryti kibernetinė erdvė ir kaip tinkamai jie galėtų suteikti pagalbą mokiniams tiek prevenciškai, tiek susidūrusiems su grėsmėmis. Šiuolaikinis mokytojas turi turėti motyvacijos suprasti esamas tendencijas elektroninėje erdvėje, siekti pritaikyti naujoves mokyme, todėl kuo yra didesnė motyvacija tobulėti ir siekti pagalvos iš išorės, tuo didesnis suvokimas papildo vidinius veiksnius ir mokymas tampa komfortišku gebant mokyti jaunimą ir suteikti reikalingą informaciją, bei padėti spręsti iškilusias problemas.

2.3.2. Tėvų ir globėjų vaidmuo vystant kibernetinio saugumo kultūrą

Siekiant gerinti mokyklinio amžiaus vaikų kibernetinės erdvės naudojimo įgūdžius ir skatinti naudojimosi kultūrą tėvai turi taip pat turi įdėti indėlį į šį procesą. Mokytojo, kaip švietėjo indėlis gali būti daugiau kaip patariamasis, rodantis pavyzdį, tačiau tėvai turi teisę individualiai stebėti kaip jų vaikai elgiasi elektroninėje erdvėje. Tirdami tėvų indėlį siekiant identifikuoti ir sumažinti jaunimo rizikas naudojant informacines technologijas Gimenez, Luengo ir Bartrina (2017) pateikia jog tėvai dažniausiai vaikų klausia ką jie veikia kol naudojasi išmaniaisiais įrenginiais, riboja naudojimosi internetu laiką, peržiūri jų naršymo istoriją, kiti susieja vaikų socialinių tinklų profilius su savuoju,

tačiau tai nėra pakankami metodai norint apsaugoti vaikus nuo kibernetinėje erdvėje kylančių rizikų (p. 538). Minėtų autorių straipsnyje yra pažymima, jog tėvai tėvų įtraukimas į kibernetinio saugumo kultūros ugdymą yra taip pat ypatingai svarbus ir mokymas turi būti pateikiamas pozityviai, o ne per gąsdinimo ar grasinimo prizmę.

2021–2027 m. skaitmeninio švietimo veiksmų plane pateikiamose 2020 m. vasario–rugsėjo mėnesiais vykusių konsultacijų dėl Skaitmeninio švietimo veiksmų plano išvadose apibrėžiama jog tėvai vykstant COVID-19 krizei atliko svarbų vaidmenį sudarant sąlygas vaikams mokytis nuotoliniu būdu. Didelį indėlį teko įdėti tėvams, auginantiems pradinių klasių vaikus, kurie veikloje negalėjo dalyvauti savarankiškai ir jiems buvo būtina tėvų pagalba. Dokumente taip pat pažymima jog „Aukštąjį išsilavinimą įgiję tėvai paprastai turėjo geresnes galimybes padėti besimokantiems asmenims, sudarydami palankią mokymosi aplinką namuose.“ (Europos komisijos komunikatas Europos Parlamentui, Tarybai, Europos Ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui, 2020, p. 7). Tai rodo, jog suaugusieji, kurie turi išsilavinimą, turi ir geresnius skaitmeninio raštingumo įgūdžius, geba suprasti technologinius ir skaitmeninėje erdvėje vykstančius procesus. Tėvų ir globėjų įsitraukimas ir kontrolės mechanizmas reikalingas stebint kokiose internetiniuose tinklapiuose ir kokias programėles jie naudoja, ar jos yra tinkamos pagal jų amžių, kokį turinį jose gali pasiekti vaikai. Svarbus stebėjimas kiek laiko praleidžiama prie naudojantis skaitmenine erdve, naudojimosi laikas padidėjo esant COVID – 19 epidemijai, kuomet mokymas vyko nuotoliniu būdu, todėl dalis tėvų į šį aspektą pradėjo žiūrėti atlaidžiau suprasdami, kad esant dideliam mokymosi krūviui, buvo leidžiama vaikams užsiimti ir norima veikla internete (Ofcom, 2021, p. 39). Pandemijos metu dalis tėvų padėjo jaunesnio amžiaus vaikams susikurti skaitmeninius ryšius su jų draugais, jog nebūtų prarastas bendravimas, tačiau taip pat yra svarbu kontroliuoti šį procesą ir žinoti su kokiais asmenimis bendrauja jų atžalos, paaiškinti apie galimus pavojus bendraujant su nepažįstamaisiais. Svarbus yra aptarimo ir refleksijos momentas su vaikais, siekiant sužinoti kaip jaunimas jaučiasi naudodamasis technologijomis, supažindinti ir mokyti kas yra sveikas ir atsakingas dalyvavimas elektroninėje erdvėje, bei atpažinti, jeigu iškyla rizikos ir vaikas susiduria su netinkamu turiniu arba yra įžeidinėjamas internetinėje erdvėje.

Mokytojai, tėvai ar globėjai yra pagrindiniai veikėjai, kurie užtikrina ir ugdo vaikų suvokimą kaip naudotis skaitmeninėmis technologijomis atsakingai ir saugiai. Tai parodo, jog abi šalys turi būti suinteresuotos būti skaitmeniškai raštingos ir domėtis kaip suteikti reikiamą informaciją ir pagalbą jaunimui. Įvairūs kursai, seminarai į kuriuos būtų įtraukti mokytojai, vaikai, bei tėvai gali padėti padidinti jaunimo supratimą ir reagavimą į pavojus ar kitas kibernetinės erdvės rizikas. Mokytojai visame šiame procese turėtų patarti ir teikti rekomendacijas, mokyti bei supažindinti su naujausiomis technologijomis, bei kylančiomis grėsmėmis. Tėvai turėtų kartu dalyvauti kibernetinėje erdvėje su

savo atžalomis ir padėti, bei kontroliuoti jų veiksmus, nustatyti reikiamas ribas, bei stebėti emocinę būklę.

2.3.3. Mokinių kibernetinio saugumo kompetencijos

Mokyklinio amžiaus vaikai nuo kuo mažesnio amžiaus turi žinoti ir suprasti savo teises. Tai įgalina jaunimą atpažinti grėsmes ir apie tai pranešti atsakingiems asmenims (tėvams, mokytojams), kurie galėtų suteikti reikiamos pagalbos ar informacijos. Būtent dėl šios priežasties mokytojų ir tėvų rolė yra labai svarbi šiame kibernetinio saugumo kultūros vystymo procese, Skaitmeninis ugdymas yra svarbus norint suprasti elektroninį pasaulį, į tai įtraukiant ir kibernetinio saugumo kultūros vystymą. 2021–2027 m. skaitmeninio švietimo veiksmų plane apibrėžiama, jog: „Mokinių įtraukimas į kompiuteriją nuo ankstyvo amžiaus, taikant novatoriškus ir motyvuojančius mokymo metodus tiek formalioje, tiek neformalioje aplinkoje, gali padėti ugdyti problemų sprendimo įgūdžius, kūrybiškumą ir bendradarbiavimo įgūdžius“ (Europos komisijos komunikatas Europos Parlamentui, Tarybai, Europos Ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui, 2020, p. 14). Tinkamas švietimas jaunimui padėtų ne tik kokybiškai pritaikyti elektroninės erdvės teikiamas galimybes, bet ir išvengti ir apsaugoti save nuo slypinčių kibernetinių grėsmių. Turi būti užtikrintas mokinių paruošimas gyvenimui ugdant skaitmenines kompetencijas, siekiant ugdyti kritinį mąstymą ir gebėjimą apdoroti neribotą informacijos kiekį. Siekiant jog jaunas vartotojas būtų nepriklausomas šiuolaikinėje visuomenėje, kurioje didelę dalį užimą informacinės technologijos, mokymo įstaigos turi įdėti didelį indėlį į šių kompetencijų ugdymą (Dobrinoiu, 2017, p. 26).

Skaitmeninio raštingumo institutas, tarptautinis mokslinių tyrimų centras, skirtas nustatyti pasaulinius skaitmeninio intelekto ugdymo standartus, apibrėžė aštuonias sritis pagrindines skaitmeninių kompetencijų sritis, kurias vaikas turėtų įvaldyti, jog būtų saugus ir turėtų teigiamą patirtį internete. Šios sritys sudaro gebėjimą išlaikyti pozityvų asmens identitetą internete, naudotis technologijomis, sušvelninti iškylančias rizikas skaitmeninėje erdvėje, valdyti iškylančias rizikas, atpažinti ir nukreipti ar išreikšti emocijas virtualioje erdvėje, tinkamai komunikuoti ir bendradarbiauti naudojantis technologijomis, suprasti ir žinoti savo teises bei pareigas. Mokomi pagal šias disciplinas vaikai sumažino 15% riziką susidurti su pavojais internete, lyginant su tais, kurie nebuvo treniruoti. (Gegenheimer ir kt., 2019, p. 22)

Skaitmeninis raštingumas yra viena iš pagrindinių kompetencijų šiuolaikiniame pasaulyje. Tai ne tik leidžia sklandžiai gauti, dalytis, redaguoti ir archyvuoti informaciją, bet ir visapusiškai dalyvauti el. paslaugose. Skaitmeninių įgūdžių trūkumas riboja arba, kraštutiniais atvejais, trukdo dalyvauti ir visapusiškai suprasti pasaulį (Tomczy, 2019, p. 15). Tinkama šalyje veikianti sistema, visų institucijų ir organizacijų, mokytojų bendras indėlis gali padėti įgyvendinti ar palaikyti tinkamą sistemą kaip

apsaugoti vaikus ir kaip apsisaugoti jiems patiems ir būti kompetentingais šių laikų, skaitmenio pasaulio, gyventojais. Toliau bus nagrinėjama kaip viena iš daugiausiai dėmesio kibernetiniams saugumui skiriančių pasaulio šalių – JAV ir kaip Baltijos šalys užtikrina kibernetinio saugumo kultūros mokymą švietimo įstaigose.

2.4. Kibernetinio saugumo kultūros plėtros metodai ir šalių praktika

Tarptautiniu mastu šalims yra rengiamos rekomendacijos ir priemonės kurios galėtų būti pritaikytos mokant kibernetinio saugumo, tačiau kiekviena šalis skirtingai pasirinka įgyvendinti šalies vidaus politiką kaip tvarkytis ir kokias priemones reikėtų taikyti, pagrinde yra laikomasi tik pateikiamų gairių. Tai lemia skirtingų Europos šalių vaikų skaitmeninio raštingumo lygį ir pažeidžiamumo lygmenį turint skirtingas galimybes ir apribojimus. Nagrinėjama Jungtinių Amerikos Valstijų patirtį, kuri yra lyderė kibernetinio saugumo srityje ir Baltijos šalių patirtis, kurios istoriškai yra susijusios viena su kita, kibernetinio saugumo kultūros ir skaitmeninio raštingumo įgyvendinime, plačiau aptariama, kaip kiekviena šalis prisideda prie šios strategijos sričių plėtojimo, kaip įgyvendina kibernetinio saugumo mokymą.

2.4.1. Jungtinės Amerikos Valstijos

Jungtinių Amerikos Valstijų dabartinė šalies populiacija yra virš 300 milijonų, internetu naudojasi per 87% šalies gyventojų. Pagal dabartinį pasaulinį kibernetinio saugumo indeksą ši šalis yra pirmoje vietoje (Global Cybersecurity Index 2020, 2021, p 25).

1998 metais Baltųjų rūmų Kritinės insfrastruktūros apsaugos komisija nusprendė kibernetine paremtą informaciją įtraukti naują grėsmių dimensiją. Raporte apibrėžiama jog kibernetinės atakos prieš infrastruktūrą ir informacines sistemas gali reikšmingai pakenkti JAV ekonomikai ir saugumui (Lewis, 2016, p. 46). Po 2016 metų Amerikos prezidento Barack Obama paskutinio pranešimo apie esamą padėtį, buvo pradėta įgyvendinti iniciatyva „Kompiuterinis mokslas visiems“ ir paragino visas valstijas ir šalies mokyklas parengti penkerių metų planus, siekiant užtikrinti, kad visi mokiniai turėtų prieigą prie informatikos mokslų ir gautų išsilavinimą. Mokslininkai ir švietimo lyderiai parengė mokymo programas, griežtas mokytojų profesinio tobulėjimo programas, informavo švietimo politikos formuotojus remti šias programas (Tierney, Corwin, Ochsner, 2018, p. 48).

Atkreipę dėmesį į vis labiau iškylančius pavojus 2016 metais po Jungtinių Amerikos valstijų prezidento rinkimų Donald J. Trump išleido įsakymą dėl kibernetinio saugumo stiprinimo, jog reikalinga atsižvelgti vidinę kritinę infrastruktūrą, kas apimtų įvairius valdžios sektorius, įvertinti pastangas šviesti ir mokyti kibernetinio saugumo Amerikos viešojo ir privataus sektoriaus darbuotojus,

taip pat dėti indėlį į kibernetinio saugumo plėtojimą švietimo sistemoje nuo pradinio iki aukštojo mokslo (Trump White house, 2018). Tačiau Jungtinės Amerikos Valstijos siekiant švietimo pertvarkymo ir teisingumo informatikos mokslo srityje susiduria su sunkumais, dėl skirtingų valstijų politinių strategijų ir politinės valios. Todėl ne visoje šalyje yra užtikrinamas vienodas prieinamumas visų rasių ar lygmenų mokiniams (Tierney, Corwin, Ochsner, 2018, p. 59).

Amerikoje, skirtingose valstijose mokyklose yra įgyvendinami kibernetinio saugumo projektai siekiant plėtoti kibernetinę higieną, prie kurių kūrimo prisideda daug universitetų, karinių ar ne pelno siekiančių orgnizacijų. Šalyje vykdomos šios pagrindinės kibernetinio saugumo įpročių mokymo programos: (Schwartz, 2018, p. 7)

1. „Cyber.org“ mokymo programos sukurtos pedagogams ir mokiniams. Mokiniams siekiantis suteikti pagrindinių ir techninių žinių, bei įgūdžių kibernetinio saugumo temomis. Mokytojams siūlomos mokymosi programos, kurios yra reikalingos norint tinkamai pateikti informaciją mokiniams.

2. Sveiko proto pradinių – vidurinių klasių skaitmeninė pilietybė (angl. *Common Sense k-12 Digital Citizenship*). Programa įtraukia į skaitmeninio pilietiškumo mokymo programą platesnį supratimą apie privatumą, saugumą ir interneto saugumą. Visų lygių temos apima netinkamų žinučių atpažinimą, stiprių slaptažodžių kūrimą, paaiškina kaip suprasti ar svetainė, kuria naudojamasi apsaugo naudotojų asmeninę informaciją. Šia mokymo programa siekiama ugdyti jaunus žmones kaip atsakingus skaitmeninę pilietybę turinčius asmenis turinčius unikalių įgūdžių kurti ir tinkamai naudotis technologijomis (James, Weinstein, Mendoza, 2021, p. 12).

3. *Cyber Patriot* yra viena plačiausiai naudojamų JAV oro pajėgų asociacijos sukurta nacionalinė jaunimo kibernetinio švietimo programa skirta jaunimui siekiant paskatinti siekti karjeros kibernetinio saugumo, technologijų, inžinerijos matematikos disciplinų srityse, bei įgauti žinių. Vidurinių mokyklų 14 – 15 metų amžiaus mokiniams yra sukurta trijų modulių programa apimanti pavojus elektroninėje erdvėje ir kibernetinio saugumo principus. 1 modulis skirtas saugumo ir informacijos dalijimosi su šeima, draugais ir nepažįstamais asmenimis dalinimosi principų elektroninėje erdvėje mokymui. 2 modulis skirtas kompiuterių operacinių sistemų supratimo, pagrindinių kompiuterinių įgūdžių ir supažindinimas su rizikomis, tokiomis kaip sukčiavimas, kenkėjiškos programos. 3 modulis – tinklo kūrimas, kurio metu atliekamas mokomasis modeliavimas, galima stebėti kaip pasirinkti sprendimai daro įtaką sukurtam tinklui, sužinoma apie pagrindinius tinklo komponentus, kenkėjiškas programas, saugos programinę įrangą, išmokstama kaip reikia apsaugoti tinklą nuo kibernetinių grėsmių.

Sukurta interaktyvi programa žaidimų pagrindu žymiai efektyviau mokiniams padeda susipažinti ir praplėsti savo žinias kibernetinio saugumo srityje. Jaunimas ne tik supranta kaip veikia elektroninė

erdvė teoriškai, bet ir turi galimybes išbandyti ir priimti sprendimus savarankiškai ir pamatyti kaip tai gali pakeisti tam tikras įvykių sekas ir išspręsti iškylančias problemas.

4. Pradinių mokyklų kibernetinio saugumo iniciatyva. *Cyber Patriot* sukurta programa jaunesniųjų klasių mokiniams siekiant supažindinti su kibernetinio saugumo pagrindais.

5. *iSAFE* skaitmeninė pilietybė. Ne pelno siekianti organizacija sukūrė skaitmenines mokymosi programas skirtas pradinių – vidurinių mokyklų mokiniams. Programos apima privatumo, saugumo ir skaitmeninio pilietiškumo temas. Mokymo temas apibendrina plačias temas kaip skaitmeninės saugos ir saugumo, bei pateikia praktiškas gyvenimiškas situacijas, kuriose galima susidurti su rizikomis ir į ką reiktų atkreipti dėmesį.

Galima pastebėti, jog Jungtinėse Amerikos Valstijose didžiausi sunkumai su kuriais susiduriama, yra kibernetinio saugumo iniciatyvų vienodas plėtojimas visoje šalyje. Labai daug lemia atskirų valstijų ar rajonų strategijos ir politikų, bei mokyklų lyderių valios išraiška, tačiau nepaisant to atskirtis mažėja ir yra siekiama jog visų rasių jaunimas įgautų reikiamas kompetencijas.

2.5.3. Latvija

Latvijoje pagal statistikos duomenis 2021 metais šalyje gyvena virš 1 880 000 gyventojų, iš jų virš 1 670 000 yra interneto naudotojai (Kemp, 2021). Pagal dabartinį pasaulinį kibernetinio saugumo indeksą ši šalis yra penkioliktoje vietoje (Global Cybersecurity Index 2020, 2021, p. 25).

2019 metais Latvijoje pradėta formuoti formalaus švietimo kompetencijomis pagrįsta mokymo sistema. Privaloma mokymo programa yra orientuota į kompetencijų ugdymą mokantis kompleksinių dalykų. Viena iš šešių pagrindinių kompetencijų yra išskirta mokymas skaitmeninių įgūdžių (Valmane, Zarina, Badjanov, Iliško, Petrova, 2020, p. 4022). Latvijos „Nuostatuose dėl valstybinių bendrojo vidurinio išsilavinimų standartų ir bendrojo vidurinio ugdymo programų“ išskiriama kompetencija skaitmeninis raštingumas, kurios tikslas apibrėžiamas mokinio gebėjimu naudoti skaitmenines technologijas, gebėti analizuoti skaitmeninės komunikacijos naudą ir riziką, kritiškai analizuoti informacijos patikimumą žiniasklaidoje, laikytis privatumo, etikos ir teisinių reikalavimų, gebėti informaciją ir įrankius prisitaikyti prie savo poreikių ir laikytis sveikų bei saugių technologijų įpročių (Noteikumi par valsts vispārējās vidējās izglītības standartu un vispārējās vidējās izglītības programmu paraugiem, 2019).

Latvijos kibernetinio saugumo strategijoje pažymima, jog žmogaus supratimas ir elgesys yra kibernetinio saugumo pamatas. Yra svarbu užtikrinti, visi nuo sistemų ir programų kūrėjų iki vartotojų suprastų kibernetinio saugumo veikimą, bei grėsmes ir būtų kuo mažiau pažeidžiami. Strategijoje yra išskiriama jog būtina skatinti vaikų ir paauglių dalyvavimą informacinių technologijų, žaidimų ar kituose konkursuose siekiant didinti jų susidomėjimą informacinių technologijų studijomis. Iškeltas

tikslas jog Latvijos jaunimas dalyvautų bent vienoje neformalioje švietimo veikloje ar renginyje susijusiame su kibernetiniu saugumu (Informative Statement. Cybersecurity of Latvia 2019-2022, 2019, p. 17). Prie tikslų įgyvendinimo ir visuomenės informavimo prisideda sukurtas tinklapis „Drossinternet.lv“ kurio tikslas yra ugdyti ir informuoti visuomenę apie vaikų saugumą internete bei suteikiantis galimybę pranešti apie pažeidimus internete („Par mums“, 2021). Interneto tinklapyje galima rasti aktualios informacijos, bei socialinių filmukų apie galimas grėsmes internete ir kaip reikėtų elgtis, jog to išvengti. Taip pat tinklapyje galima rasti kiekvieną mėnesį leidžiamus leidinius su aktualia informacija apie esamus pažeidimus ir kaip išlikti saugiems.

Latvijos Policija yra atsakinga už saugios aplinkos kūrimą internete. Policija sukūrusi tinklapį „www.manadrosiba.lv“ kuriame galima rasti bendrą su saugumu ir interneto saugumu susijusią inforomaciją.

Latvijoje yra siekiama ugdyti jaunąją kartą skaitmeniškai raštingus, turinčius kritinį mąstymą asmenis. Tačiau atliktame tyrime, kuriame buvo aiškinamasi kaip Latvijos mokytojai supranta skaitmeninį raštingumą, buvo pateiktas pastebėjimas, jog jie į tai žiūri per siaurai ir daugiau nei penktadalis skaitmeninį raštingumą supranta kaip gebėjimą naudotis skaitmeninėmis technologijomis ir komunikacijos priemonėmis kasdieniniame gyvenime ir net trečdalis prisipažino jog jie nėra pasirengę mokiniams paaiškinti kas yra skaitmeninis raštingumas (Valmane ir kt., 2020, p. 4021).

Skaitmeninės ekonomikos ir visuomenės indekso duomenimis Latvijos gyventojų skaitmeniniai įgūdžiai yra gerokai žemesni nei likusioje Europoje. Latvija susiduria su kritine padėtimi, nes net ketvirtadalis jaunimo neturi pagrindinių įgūdžių. Straipsnio autorius pateikia kelias galimas problemas, tai trūkumas sektinų pavyzdžių, kodėl technologijos yra būtinos ir reikalingos šiuolaikiniame pasaulyje: nepakankamas su technologijomis susijusios švietimo galimybės, norint mokytis neformaliai, tai yra brangu, valstybės iniciatyvų nepakanka (Broks, 2021).

Apibendrinant Latvijos patirtį kibernetinio saugumo kultūros srityje matome, jog reikalingos švietimo reformos įgalinančios tobulinti pedagogų kvalifikaciją, jog jie gebėtų tinkamai taikyti informacines technologijas savo vykdomame darbe ir perduotų tinkamas žinias mokiniams siekiant ugdyti jų skaitmeninį raštingumą.

2.5.4. Estija

Estijoje pagal statistikos duomenis 2021 metais šalyje gyvena virš 1 330 000 gyventojų, iš jų virš 1 210 000 interneto naudotojai (Kemp, 2021). Pagal dabartinį pasaulinį kibernetinio saugumo indeksą ši šalis yra trečioje vietoje (Global Cybersecurity Index 2020, 2021, p. 15).

Pirmieji informacinės visuomenės plėtros planai buvo pradėti rengti 1994 metais. Valstybė įgijo piliečių pasitikėjimą kuriant skaitmeninę visuomenę (Aru-Chabilan, 2020, p. 63). Estija viena pirmųjų

šalių pradėjusių plėtoti nacionalinę kibernetinio saugumo strategiją 2008 metais ir atnaujinta 2019 metais. Estijos strategija turi kelis tikslus, kuriuos sudaro: visapusiškas ir gyvas visų valdžios institucijų požiūris į kibernetinį saugumą; kūrimas aukštų kibernetinio saugumo kompetencijų ir apsaugos agentūrose, kompanijose, bei visuomenėje; informacijos apsaugos sistemų reguliavimo stiprinimas; rėmimas pajėgumų vystyti tarptautinį bendradarbiavimą kibernetiniame saugume (Lewis, 2016, p. 12).

Kibernetinio saugumo taryba prižiūri visą kibernetinio saugumo strategijos įgyvendinimą Estijoje. Ekonomikos ir komunikacijos reikalų ministerija prižiūri ir koordinuoja kibernetinio saugumo įgyvendinimą valdžios institucijose, civilinėse įstaigose, įmonėse ir mokymo institucijose. Visos įstaigos įgyvendinančios strategiją turi pareigą ministerijai pateikti kasmetinius raportus apie įgyvendinimo proceso pasiekimus.

1996 metais Estijoje pradėta įgyvendinti iniciatyva „Tigro šuolis“ siekiant parengti švietimo sistemą ir visą visuomenę informacijos amžiui. Mokyklas buvo siekiama prijungti prie interneto ir aprūpinti reikalingomis priemonėmis. Iki 2000 metų beveik 70% mokytojų gavo pradinį kompiuterinį mokymą, o 15% - mokėsi išplėstiniuose kursuose (Aru-Chabilan, 2020, p. 63). Pirmasis iniciatyvos etapas apėmė infrastruktūros plėtrą, o vėliau buvo pradėtos ugdyti mokytojų ir mokinių skaitmeniniai įgūdžiai, bei siekiama sukurti standartus. Taip pat buvo remiami studentų ir mokytojų virtualaus mokymosi projektai, siekiant sukurti inovatyvius informacinius sprendimus, skirtus naudoti mokymosi procese (Aru-Chabilan, 2020, p. 64). 2006 metais buvo sujungti visi švietimo lygio pedagogai, prijungti kiti specialistai siekiant pasikeisti patirtimi, diegiant naujas tendencijas. Šio bendradarbiavimo rezultatas buvo elektroninio mokymosi medžiagos vadovo sukūrimas (Aru-Chabilan, 2020, p. 65). Šios praktikos vystymas lėmė kokybiškos medžiagos sukūrimą ir nuolatinį tobulinimą.

2013 metais Estijoje Švietimo ir mokslo ministerijos buvo atlikti esminiai informacinių technologijų organizacinės struktūros pakeitimai, siekiant sumažinti susiskaldymą, visi šios srities fondai buvo sujungti į vieną Informacinių technologijų mokymo fondą pavadinimu HITSA. Buvo suformuoti kompetencijų reikalavimai besimokantiems formaliojo ugdymo programose, mokytojams buvo padedama kaip ugdyti skirtingų dalykų kompetencijas ir visa mokomoji medžiaga buvo sujungta į valstybės finansuojamą portalą (Aru-Chabilan, 2020, p. 67). Ši patirtis rodo, kad ankstyvas technologijų pažinimas yra geriausia būdas pritraukti talentingus žmones prie informacinių technologijų (Aru-Chabilan, 2020, p. 69). Šiandien HITSA veikia kaip centrinė suinteresuotųjų šalių bendradarbiavimo platforma, tiek šalies, tiek tarptautiniu mastu. Toks visuomenės pasiruošimas, kuomet beveik viską galima padaryti internetu nesukėlė didelių nesklandumų ir COVID-19 pandemijos metu, procesai nesustojo, kuomet žmonės turėjo likti namuose, o mokiniai tęsė mokymąsi per elektronines mokyklų platformas (International Review of the Red Cross, 2020, p. 2).

Vertinant Estijos patirtį kibernetinio saugumo srityje, galima tai laikyti gerąja patirtimi, kuomet yra didelis valdžios institucijų įsitraukimas ir rėmimas programų, jog kiekviena mokykla būtų aprūpinta reikalingomis priemonėmis siekiant tobulinti mokinių skaitmeninį raštingumą. Taip pat yra labai reikšminga, jog mokytojai yra visapusiškai įtraukti į tobulinimosi ir kūrimo procesą, siekiant juos palaikyti informacijos lauke ir suteikti aktualią informaciją apie technologijas, iškylančias rizikas, bei naujausius mokymo metodus.

2.5.5. Lietuva

Lietuvoje pagal statistikos duomenis 2021 metais šalyje gyvena virš 2 710 000 gyventojų, iš jų virš 2 220 000 interneto naudotojai (Kemp, 2021). Pagal dabartinį pasaulinį kibernetinio saugumo indeksą šalis yra trečioje vietoje (Global Cybersecurity Index 2020, 2021, p. 15).

Nacionalinės kibernetinio saugumo strategijos 27 straipsnis apibrėžia kibernetinio saugumo kultūros mokymo įtraukimą į bendrojo ugdymo programas svarbą, taip pat yra minima pedagogų kvalifikacijos tobulinimo poreikis siekiant kokybiškai įgyvendinti mokymą (Lietuvos Respublikos Vyriausybės nutarimas, 2018).

Siekiant užtikrinti vaikų apsaugą susidūrus su patyčiomis arba pastebėjus kitas rizikas elektroninėje erdvėje Lietuvos Respublikos švietimo įstatymas apibrėžia apsaugą nuo smurto švietimo įstaigose, kaip ji turėtų būti įgyvendinta, taip pat 232 straipsnis numato kaip reikėtų elgtis pastebėjus patyčias ar kitą ribojamą skleisti viešąją informaciją kibernetinėje erdvėje. Šio straipsnio 1 punktas numato pastebėjus kibernetinių patyčių atvejus pranešti Lietuvos Respublikos ryšių reguliavimo tarnybai pateikiant pranešimą interneto svetainėje adresu www.draugiskasinternetas.lt arba www.svarusinternetas.lt tokią atsakomybę privalomai turi tiek smurtaujančio, tiek smurtą patiriančio nepilnamečio mokinių tėvai/ globėjai, o kiti turi tokią teisę (Lietuvos Respublikos Švietimo įstatymas, 1991). Lietuvos Respublikos ryšių reguliavimo tarnyba gavus ir įvertinus pranešimo turinį pagal poreikį informuoja kompetentingas institucijas ir taip pat turi teisę duoti nurodymus pati, siekiant pašalinti esamą informaciją arba apriboti galimybę ją pasiekti. Siekiant mažinti galimas rizikas ar patyčias elektroninėje erdvėje, Lietuvos Respublikos Švietimo, mokslo ir sporto ministerija pradėjo inicijuoti teisės aktų pakeitimus, siekiant tobulinti programas ir plėtoti kibernetinio saugumo kultūrą.

Lietuvoje Respublikos Švietimo įstatymas (1991) numato jog asmenys turi būti ugdomi kūrybiškai ir padedant įgyti kompetencijas, kvalifikaciją atitinkančią šių dienų kultūros ir technologijų lygį. Įstatyme yra įtvirtinta jog ugdymo turinys privalo būti peržiūrimas ir atnaujinamas atsižvelgiant į besikeičiančius socialinės ir kultūrinės aplinkos keliamus poreikius. Atsižvelgiant į tai, Švietimo, mokslo ir sporto ministerija 2021 metais siekdama atnaujinti bendrąsias ugdymo programas, į programų atnaujinimo gaires įtraukė skaitmeninio raštingumo kompetenciją (Lietuvos Respublikos

Švietimo, mokslo ir sporto ministro įsakymas, 2021).

Pagrindinė institucija įgyvendinanti skaitmeninio raštingumo plėtros projektus yra 2019 metais įkurta Nacionalinė švietimo agentūra, kurios veiklą koordinuoja Lietuvos Respublikos švietimo, mokslo ir sporto ministerija. Nacionalinė švietimo agentūra, įgyvendindama projektą „Mokykla 2030“ bei siekdama stiprinti mokinių skaitmeninio raštingumo gebėjimus, atnaujino informacinių technologijų mokymosi programą remdamasi DigCom modeliu, išskirdama šias kompetencijas: informacijos ir duomenų raštingumas, bendravimas ir bendradarbiavimas, skaitmeninio turinio kūrimas, saugumas, skaitmeninis mokymas ir mokymasis problemų sprendimas. Šios kompetencijos turėtų sustiprinti mokinių skaitmeninio raštingumo sugebėjimus (informatikos ugdymo paskirtis, 2021). Tuo tikslu buvo pradėti vykdyti pedagogų ir mokyklų darbuotojų rengimo projektai.

Nacionalinė švietimo agentūra, atsižvelgdama į 2021–2027 m. skaitmeninio švietimo veiksmų plano strateginius prioritetus: gerinti ir plėsti švietimą bei mokymą, diegti mišrią mokymosi sistemą, kuomet į kontaktinį mokymą būtų įtraukiamas technologijos ir nuotolinis mokymas ir siekti suteikti reikalingus skaitmeninio raštingumo įgūdžius besimokantiems, siekiant juos kuo geriau integruoti į elektroninio pasaulio sistemą (Europos komisijos komunikatas Europos Parlamentui, Tarybai, Europos Ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui, 2020, p. 3), vykdo projektines veiklas ir siekia surinkti įvairių specialistų patirtį, kaip tinkamai skleisti mokyklos bendruomenėje informaciją užtikrinančią saugią elektroninę erdvę, taip pat kuria mokomąją pagalbinę medžiagą pedagogams (Čiapienė, 2021).

Nacionalinė švietimo agentūra, vadovaudamasi Lietuvos Respublikos Švietimo, mokslo ir sporto ministro įsakymu dėl reikalavimų mokytojų kompiuteriniam raštingumui (Lietuvos Respublikos Švietimo, mokslo ir sporto ministro įsakymas, 2018), ir siekdama kelti visų dalykų pedagogų ir pagalbos mokiniui specialisto kompetencijas kibernetinio saugumo srityje, parengė mokytojų kvalifikacijai skirtą skaitmeninio raštingumo programų sąrašą, kurioje išskiriamos DiComp modelio pagrindinės tobulintinos kompetencijos.

Šis programų sąrašas ne tik įprasmina kibernetinio saugumo kultūros svarbą siekiant diegti žinojimą vartotojams jog jie būtų apsaugoti ir apsisaugoję, bet ir sumažina iškylančias rizikas tiek sau, tiek kitiems.

Kaip vieną iš pagrindinių kompetencijų galima išskirti saugumo kompetenciją, kuri apima gebėjimą apsaugoti savo skaitmeninę įrangą (antivirusinių programų naudojimas, slaptažodžių apsaugą ir kt.), gebėjimą apsaugoti savo ir kitų asmenų privatumą internete, gebėjimą naudotis savo asmeniniais duomenimis, bei gebėjimą atpažinti ir išvengti galimų įvairių elektroninių patyčių formų. Siekiant populiarinti kibernetinio saugumo kultūros svarbą, būtina užtikrinti, jog kiekvienas pedagogas įgytų saugumo kompetencijas ir žinotų kaip tinkamai elgtis tiek pačiam susidūrus su elektroninėmis patyčiomis, tiek kaip užtikrinti, jog mokiniai žinotų kaip elgtis ar kaip išvengti elektroninių patyčių.

Apibendrinant Lietuvos patirtį, galima daryti išvadą, jog parengtos mokymosi programų gairės ir vykdomi projektai yra išsamūs ir atitinkantys pasaulinius kibernetinio saugumo ir skaitmeninio raštingumo reikalavimus, tačiau ne vienodas teisinis sąvokų reguliavimas, kai Vyriausybės ar Kibernetinio saugumo įstatymuose vartojama kibernetinio saugumo kultūros sąvoka, o Švietimo įstatymuose vartojama skaitmeninio raštingumo sąvoka sudaro sąlygas mokytojams ne vienodai interpretuoti ugdymo turinio formulavimą tiek tobulinant asmenines kompetencijas, tiek vykdant vaikų ugdymą, kadangi vis dar trūksta metodinių rekomendacijų, mokymosi medžiagos ir praktinių patarimų rinkinio, kuriuos pedagogai galėtų naudoti ugdymo procese. Taip pat nėra aiškaus mechanizmo, kuris užtikrintų pačių pedagogų savanorišką įsitraukimą ir norą tobulinti savo kompetencijas kibernetinio saugumo ir skaitmeninio raštingumo srityje, ypač siekiant skatinti persikvalifikuoti ir tobulinti savo skaitmeninio raštingumo kompetencijas vyresnio amžiaus pedagogams.

3. KIBERNETINIO SAUGUMO KULTŪROS BENDOJO UGDYMO MOKYKLOSE VERTINIMAS

3.1. Tyrimų metodologija

Tyrimo metodika ir organizavimas. Siekiant atskleisti kibernetinio saugumo kultūros vystymą bendrojo ugdymo mokyklose pasirinktas **mišrus tyrimas**. Siekiant nustatyti esamą kibernetinio saugumo supratimo ir mokymo lygį Lietuvos bendrojo ugdymo mokyklose buvo atlikti kokybinis ir kiekybinis tyrimai. Kokybinio tyrimo metu siekiama išsiaiškinti mokytojų kompetencijų tobulinimą skaitmeninio raštingumo srityje ir mokyklų vykdomas programas siekiant stiprinti kibernetinį saugumą. Kiekybinio tyrimo metu siekiama išsiaiškinti Lietuvos mokinių naudojimąsi elektronine erdve ir supratimą apie esamas grėsmes. Siekiant tyrimo sėkmingo pritaikymo ir gautų tyrimo rezultatų bus pateiktos išvados, kurios padėtų tobulinant kibernetinio saugumo kultūrą Lietuvos bendrojo ugdymo mokyklose.

Tyrimo tikslas. Išanalizuoti kibernetinio saugumo kultūros tobulinimo galimybes Lietuvos bendrojo ugdymo mokyklose.

Tyrimo uždaviniai:

1. Įvertinti Lietuvos bendro ugdymo mokyklose vykdomą veiklą susijusią su kibernetinio saugumo kultūros ugdymu;
2. Atskleisti Lietuvos bendro ugdymo mokyklų mokinių naudojimąsi skaitmeninėmis technologijomis ir rizikų suvokimą;
3. Atlikti vertinimą parengiant rekomendacijas kibernetinės saugumo kultūros bendrojo ugdymo mokyklose tobulinimui.

Tyrimo metodai. Tyrimui atlikti bus naudojami tokie metodai:

1. Pusiau struktūrizuotas interviu. Kokybiniam tyrimui pasirinktas struktūrizuotas interviu. Tyrimu siekiama surinkti reikiamą informaciją iš specialistų, kurie tiesiogiai susiję su kibernetinio saugumo vykdomomis iniciatyvomis ir mokytojų kvalifikacijos kėlimu bendrojo ugdymo mokyklose;
2. Anketinė apklausa. Kiekybiniam tyrimui pasirinkta anketinė apklausa skirta Lietuvos mokiniams besimokantiems bendrojo ugdymo mokyklose.
3. Gautų duomenų analizė. Metodas taikomas siekiant išsiaiškinti mokytojų ir mokinių nuomonę apie vykdomų programų veiksmingumą. Pasitelkus analizės išvadas buvo rengiamos rekomendacijos siekiant tobulinti kibernetinio saugumo kultūros mokymą.

Tyrimo reprezentatyvumas.

Kokybinio tyrimo imties sudarymui pasirinkta tikslinė atranka. Pusiau struktūrizuoto interviu tyrimo dalyviai buvo atrenkami pagal šiuos kriterijus:

1. Mokyklos vykdančios mokymą pagal bendrojo ugdymo programas;
2. Specialistai tiesiogiai susiję su skaitmeninio raštingumo ir kibernetinio saugumo plėtojimu mokykloje.

Kiekybinio apklausos raštu tyrimo dalyviai atrenkami pagal šiuos kriterijus:

1. Asmenys nuo 8 iki 18 metų;
2. Mokiniai, besimokantys Lietuvos bendrojo ugdymo mokyklose.

1 etapas. Tyrimo dalyvių, atsakingų už kibernetinio saugumo kultūros vystymą ir švietimą, tyrimas. Šiame etape atliekamas kokybinis tyrimas – pusiau struktūrizuotas interviu. Interviu dalyviai specialistai susiję su kibernetinio saugumo švietimo plėtojimu. Šiuo tyrimu siekiama išsiaiškinti kokie procesai yra vykdomi siekiant vystyti kibernetinę saugumo kultūrą bendrojo ugdymo mokyklose, su kokiomis problemomis yra susiduriama.

2 etapas. Šiame etape atliekamas kiekybinis tyrimas – bendrojo ugdymo mokyklų moksleivių apklausa raštu. Tyrimu siekiama nustatyti mokinių naudojimąsi elektronine erdve, gebėjimą saugiai elgtis internete ir jų požiūrį į kibernetinio saugumo mokymą mokyklose.

3 etapas. Šiame etape bus aptariami gauti rezultatai, siekiant išsiaiškinti kaip vertinamas kibernetinio saugumo mokymas iš mokytojų ir mokinių perspektyvų.

3.2. Kokybinio tyrimo organizavimas

Kokybinio tyrimo organizavimas. Tyrime buvo pakviestos dalyvauti 10 geriausių Lietuvos mokyklų pagal žurnalo „Reitingai“ paskelbtą vertinimą ir pasirinktinai 10 mokyklų iš įvairių Lietuvos apskričių. Iš visų mokyklų tyrime sutiko dalyvauti penkios mokyklos. Tyrimas atliktas 2021 m. rugsėjo 21 – spalio 18 dienomis. Kokybinio tyrimo etapų veikla išdėstyta 2 lentelėje.

2 lentelė. Kokybinio tyrimo eiga

Etapas	Etapo veikla	Etapo tikslas
Pasirengimas	Suformuluojama tyrimo koncepcija ir tyrimo metodas. Parenkami tyrimo dalyviai remiantis viešaisiais vertinimais ir asmenine patirtimi.	Suformuluota tyrimo koncepcija; Parengtas interviu klausimynas.

2 lentelės tęsinys kitame puslapyje

2 lentelės tęsinys

Tyrimo dalyvių parinkimas	Išsiunčiami el. laiškai su tyrimo aprašymu ir įvardinimu koks yra tyrimo tikslas. Gavus atsakymą susisiekiama tiesiogiai mokyklų vadovams siekiant gauti oficialų leidimą vykdyti tyrimą.	Gautas leidimas vykdyti tyrimą iš mokyklos vadovybės.
Tyrimo vykdymas	Susisiekiama su tyrimo dalyviais, pristatomas tyrimo tikslas, organizavimo tvarka, tyrimo etika.	Surinkta informacija apie vykdomą kibernetinio saugumą mokyklose.
Duomenų analizė	Gautų duomenų sisteminimas, apibendrinama gauta informacija.	Rezultatų interpretavimas, vertinimas ir gautos išvados.

Tyrimo etika. Kokybinio tyrimo tikslas buvo išsiaiškinti institucijos vykdomą veiklą, todėl iš pradžių buvo gautas mokyklų vadovų leidimas dalyvauti tyrime. „...bendra tyrimų etikos ypatybė susijusi su institucijų ar organizacijų, kuriose planuojama vykdyti tyrimus, leidimo gavimu.“ (Kardelis, 2016, p. 81). Pasirinktų mokyklų vadovams buvo išsiųstas el. laiškas su tyrimo tikslu, siekiniais siekiant gauti leidimą vykdyti tyrimą. Dėl esančių COVID-19 apribojimų su mokyklos vadovais nebuvo susitikta, o gavus leidimą, jie paskyrė atsakingus asmenis, kurie atsakė į pateiktus klausimus (arba tai padarė patys).

Visi tyrimo dalyviai struktūrizuotame interviu dalyvavo savo valia ir savanoriškai. Siekiant išsaugoti tyrimo dalyvių anonimiškumą tyrime nėra atskleidžiamos organizacijos tyrimo dalyvių vardai, pavardės ir pareigybės, nes daugumoje mokyklų šias pareigybes užima vienas žmogus, todėl tyrimo dalyviams buvo priskirti kodai (žr. 3 lent.).

3 lentelė. Tyrimo dalyvių grupė

Kodas	Mokykla
TD1	Lietuvos sveikatos mokslų universiteto gimnazija
TD2	Marijampolės „Ryto“ pagrindinė mokykla
TD3	Vytauto Didžiojo universiteto licėjus SOKRATUS
TD4	Dusetų Kazimiero Būgos gimnazijos
TD5	Vytauto Didžiojo universiteto Ugnės Karvelis gimnazija

Tyrimo dalyvių apklausos analizė.

Tyrimo dalyviams buvo užduoti 8 klausimai:

1. Kokia Jūsų mokymo įstaigoje yra vykdoma šviečiamoji veikla susijusi su kibernetiniu saugumu? Jeigu tai, kaip ji yra vykdoma?
2. Kaip yra kreipiamas dėmesys į mokinių ir mokytojų skaitmeninio raštingumo ir kibernetinio saugumo kompetencijų tobulinimą? Kaip kompetencijos yra tobulinamos?
3. Ar mokykloje turite mokytoją ar pagalbos mokiniui specialistą skaitmeniniam raštingumui?
4. Jeigu turite specialistą arba mokytoją. Kokia darbuotojo vykdoma veikla? Ar mokytojas (-ai) ar specialistas (-ai) yra įgiję nustatytas kompetencijas pagal LR Švietimo ir mokslo ministro 2018 m. birželio 25 d. įsakymą Nr. V-598 „Dėl reikalavimų mokytojų ir pagalbos mokiniui specialistų skaitmeninio raštingumo programoms aprašo patvirtinimo“?
5. Jeigu mokytojo ar specialisto neturite. Ar būtų poreikis tokį specialistą turėti?
6. Ar turite mokykloje patvirtintą tvarką susijusią su smurto ir patyčių prevencija? Ar tvarkoje yra apibrėžiama smurto forma – „kibernetinės patyčios“?
7. Ar mokykla dalyvauja „Draugiškas internetas“ siūlomose programose?
8. Kokias kitas iniciatyvas susijusias kibernetinio saugumo kultūra mokykla vykdo? Įvardinkite vykdomas iniciatyvas.

3.3. Kokybinio interviu tyrimo rezultatai

Toliau nagrinėjami tyrimo dalyvių atsakymai į klausimus.

1. Kokia Jūsų mokymo įstaigoje yra vykdoma šviečiamoji veikla susijusi su kibernetiniu saugumu? Jeigu tai, kaip ji yra vykdoma?

Keturi iš penkių tyrimo dalyvių pasidalino, jog šviečiamoji veikla yra integruota į informacinių technologijų pamokas ir vykdoma klasės valandėlių metu. TD3 pastebėjo, jog veikla sistemingai mokykloje nebuvo vykdoma, tačiau planuoja kibernetinio saugumo temas įtraukti į klasės valandėlių turinį kviečiant specialistus. Kitas tyrimo dalyvis TD2 paminėjo jog <*Europos kibernetinio saugumo mėnesiui visada skiriame bent keletą renginių, stengiamės atkreipti mokytojų ir mokinių dėmesį į pavojus susijusius su interneto vartojimu. Renginius įtraukiame į mokyklos mėnesio veiklos planą*.>, trečiasis tyrimo dalyvis TD5 taip pat pastebėjo, jog <*Esant ypatingiems atvejams, kviečiami specialistai iš kitų organizacijų pravesti užsiėmimus tam tikrų klasių koncentrams, kuriems ši tema yra ypač aktuali*.>.

Pastebėtina, jog tyrimo dalyviai paminėjo, jog kibernetinio saugumo mokymo dalykai yra įtraukti į informacinių technologijų dalykus ir tik po periodiškai kai kurios temos aptariamos per klasės

valandėles, tačiau tik iškilus problemai yra gilinamasi ir kviečiami specialistai pravesti užsiėmimą tikslinei grupei. Tai leidžia teigti jog visų mokinių supratimo lygis gali labai skirtis priklausomai nuo klasės auklėtojo kompetencijos, nes dažniausiai klasės valandėlių temos yra pasirenkamos individualiai, taip pat yra sklaidos trūkumas, kuomet specialistų informacija yra pateikiama tik mažai grupei.

2. Kaip yra kreipiamas dėmesys į mokinių ir mokytojų skaitmeninio raštingumo ir kibernetinio saugumo kompetencijų tobulinimą? Kaip kompetencijos yra tobulinamos?

Tyrimo dalyviai paminėjo, jog pagal poreikį yra sudaromos sąlygos dalyvauti kvalifikacijos tobulinimo programos susijusiomis su skaitmeniniu raštingumu, į kibernetinio saugumo kompetencijų žinias yra mažiau gilinamasi. Du tyrimo dalyviai paminėjo jog mokyklose yra organizuojamos ar planuojamos organizuoti metodinės popietės kurių metu mokytojai dalinasi savo patirtimi. Skaitmeninio raštingumo trūkumai ypatingai išryškėjo paskelbus Lietuvoje karantiną ir uždarius mokyklas, kaip teigia TD 2 <*Skaitmeninis mokytojų ir mokinių raštingumas labai stipriai išaugo pandemijos kontekste, kai reikėjo perorganizuoti ugdymą į nuotolinį. Kartu mokėmės, suradome vieningą nuotolinio mokymosi platformą (Google meet), daug padėjo informatikos mokytojai...*>.

Vis dar pastebimas poreikis kelti mokytojų skaitmeninio raštingumo kompetencijas, jog jie jautųsi komfortiškai ir gebėtų pritaikyti technologijas savo vedamų pamokų, tiek kontaktinio, tiek nuotolinio mokymo, metu. Taip pat nė vienas respondentas nepaminėjo, jog jų mokykloje būtų vertinamas skaitmeninio raštingumo lygis, o į kvalifikacijos kėlimo kursus mokytojai gali dalyvauti pagal išreikštą poreikį. Iškyla rizika, jog ne visi mokytojai, kuriems yra reikalingas skaitmeninio raštingumo mokymai, pateikia savo kandidatūras.

3. Ar mokykloje turite mokytoją ar pagalbos mokiniui specialistą skaitmeniniam raštingumui?

4. Jeigu turite specialistą arba mokytoją. Kokia darbuotojo vykdoma veikla? Ar mokytojas (-ai) ar specialistas (-ai) yra įgiję nustatytas kompetencijas pagal LR Švietimo ir mokslo ministro 2018 m. birželio 25 d. įsakymą Nr. V-598 „Dėl reikalavimų mokytojų ir pagalbos mokiniui specialistų skaitmeninio raštingumo programoms aprašo patvirtinimo“?

5. Jeigu mokytojo ar specialisto neturite. Ar yra poreikis tokį specialistą turėti?

Šių trijų, aukščiau pateiktų klausimų atsakymai bus apibendrinti bendrai.

Tyrimo dalyviai atskleidė jog mokytojo ar specialisto, įgijusio kompetencijas pagal LR Švietimo ir mokslo ministro 2018 m. birželio 25 d. įsakymą Nr. V-598 „Dėl reikalavimų mokytojų ir pagalbos mokiniui specialistų skaitmeninio raštingumo programoms aprašo patvirtinimo“ neturi. Du tyrimo dalyviai paminėjo jog tokias funkcijas atlieka inžinierius kompiuteriams, informatikos mokytojas.

Vienas tyrimo dalyvis TD 5 pateikė jog <*Švietimo pagalbos specialistai yra dalyvavę 8 akademinių valandų konferencijoje "Vaikų naudojimasis internetu: moksliniai rezultatai ir praktinės įžvalgos. Specialistai yra įgiję reikiamas kompetencijas skaitmeninio raštingumo srityje*.>. Pasidomėjus ar toks specialistas būtų reikalingas, visi tyrimo dalyviai sutiko, kad tokia atskiro specialisto pareigybė arba kompetenciją įgijęs mokytojas padėtų gerinti mokinių kibernetinio saugumo suvokimą ir įgūdžius.

Apibendrinant galima įžvelgti, jog mokyklose trūksta specialistų, kurie būtų įgiję tinkamas kompetencijas siekiant stiprinti mokinių žinias. Mokytojai ir specialistai dažniausiai dalyvauja pavieniuose mokymuose norint pagilinti ir atnaujinti savo žinias.

6. Ar turite mokykloje patvirtintą tvarką susijusią su smurto ir patyčių prevencija? Ar tvarkoje yra apibrėžiama smurto forma – „kibernetinės patyčios“?

Visi tyrimo pateikė jog jų mokykloje yra patvirtinta tvarka susijusi su smurto ir patyčių prevencija.

Keturios iš penkių mokyklų su kibernetinėmis patyčiomis tvarkosi individualiai, užpildant pranešimus ir pranešant atsakingiems asmenims, tik viena iš mokyklų savo tvarkoje turi apsibrėžusi pranešimo užpildymą tinklapyje www.draugiskasinternetas.lt. Vienas iš tyrimo dalyvių, kurio mokykloje į smurto ir patyčių prevenciją įtraukta kaip elektroninės patyčio ir nenumatyta tvarka kaip su jomis kovoti, TD 3 paminėjo jog <*Šiuo metu tvarka yra atnaujinama, tad vertingas patarimas, įtraukti ir kibernetinių patyčių klausimą*>.

Mokyklos bendruomenė dažniausiai yra antri namai mokiniams ir kuriant gerbūvį mokiniams yra būtina pastebėti jeigu mokiniai susiduria su patyčiomis. Mokyklos turėtų tiksliai apsibrėžti kaip jie turėtų tvarkytis su skaitmeninėje erdvėje patiriamu pavojumi. Mokykla neturėtų kibernetinio pobūdžio patyčių pasilikti tvarkyti ir reaguoti tik savo viduje, reikėtų būti atsakingai informuoti tarnybas, kurios atsakingos elektroninės erdvės tvarkymą, jog būtų pradėtas tyrimas ir būtų surasti skriaudėjai arba žeidžianti ar daranti žalą informacija pašalinta ir būtų užkardytas plitimas, kuris galimai galėtų pasiekti ir kitus vartotojus. Taip pat pastebėtina, kadangi tokie atvejai Lietuvos mokyklose atsitinka nedažnai, reagavimo ir suvaldymo praktikų patirtį mokyklos turėtų dalintis tarpusavyje.

7. Ar mokykla dalyvauja „Draugiškas internetas“ siūlomose programose?

Trys iš penkių tyrimo dalyvių pateikė, jog jų mokykla nedalyvauja „Draugiškas internetas“ siūlomose programose. Du tyrimo dalyviai pateikė, jog mokykla yra įsitraukusi į programą ir naudojosi tinklapyje siūloma informacija šviečiant vaikus ir pristatant temas susijusias su internetiniu saugumu.

„Draugiškas internetas“ yra viena pagrindinių platformų siūlančių ir pateikiančių mokymo turinį, bei praktikas kaip geriau integruoti technologijas į pamokų turinį, bei kaip veiksmingai paruošti temas

siekiant mokinius supažindinti su kibernetiniu saugumu, todėl šios platformos populiarumas tarp mokyklų turėtų augti.

8. Kokias kitas iniciatyvas susijusias kibernetinio saugumo kultūra mokykla vykdo? Įvardinkite vykdomas iniciatyvas.

Vienas iš tyrimo dalyvių pateikė jog jų mokykloje nėra plačiai vykdoma veikla susijusi su kibernetinio saugumo švietimu ir paminėjo jog sudarant mokymo planus, bus stengiamasi įtraukti aktualias temas mokiniams. Kiti tyrimo dalyviai pateikė skirtingus atsakymus kokia veikla vykdoma siekiant stiprinti kibernetinio saugumo kultūrą, TD1 paminėjo, jog visa atsakomybė yra perleista informacinių technologijų mokytojams, kurie skatina mokinius dalyvauti įvairiuose konkursuose. Kitas tyrimo dalyvis TD5 paminėjo, jog tokios temos dažniausiai įtraukiamos ir pristatomos per pažintinę – kultūrinę veiklą, kuomet supažindinama su saugaus interneto naudojimo klausimais, TD 4 paminėjo, jog yra vykdoma <*Prevencinių klipų, filmų apie kibernetinį saugumą žiūrėjimas ir aptarimas, policijos atstovų paskaitos kibernetinio saugumo klausimais...*>. TD2 pabrėžė jog yra mokykloje ganėtinai rimtai žiūri į galimas grėsmes, su kuriomis mokiniai gali susidurti skaitmeninėje erdvėje, todėl mokykloje <*Vykdome prevencinius pokalbius, klasių valandėles, integruojame saugesnio interneto temas įvairių dalykų pamokose, organizuojame renginį* „*Saugaus interneto savaitė*“>, taip pat ši mokykla siekdama skleisti naudingą informaciją savo interneto svetainėje pateikia aktualias nuorodas mokiniams ir tėvams, kaip reikia būti saugiems skaitmeninėje erdvėje ir kaip reikia elgtis susidūrus su grėsmėmis.

Kaip pastebima, jog ne visos mokyklos aktyviai prisideda prie kibernetinio saugumo kultūros vystymo, dauguma iniciatyvų priklauso nuo mokyklos valdžios palaikymo. Kai kuriose mokyklose tai paliekama tam tikrų dalykų mokytojų (dažniausiai informacinių technologijų) atsakomybei supažindinti vaikus su esamomis grėsmėmis. Labai pagirtina, jog visi yra mokyklų, kurios stengiasi integruoti skaitmeninio raštingumo temas ne tik informacinių technologijų ar klasės valandėlių temas.

Apibendrinant kokybinio tyrimo gautus rezultatus, pastebima jog daugumoje mokyklų skaitmeninio raštingumo tobulinimo ir kibernetinio saugumo kultūros temos yra pateikiamos daugiausiai tik informacinių technologijų pamokose, kitų dalykų mokytojai šias temas linkę pristatyti pasyviau. Mokyklose nėra mokytojų skaitmeninio raštingumo kompetencijų tobulinimo sistemos. Mokyklos siekia padėti pedagogams išspręsti su technologijomis susijusias problemas dažniausiai tik pastebėjus tam tikrus trūkumus ar prasidėjus krizėms, kas šiuolaikinių technologijų pasaulyje nėra pakankamai, siekiant užtikrinti kokybišką skaitmeninio raštingumo ugdymą. Pastebima, jog mokyklos dažnu atveju palieka patiems mokytojams spręsti koks yra jų skaitmeninių kompetencijų kėlimo poreikis, nors mokytojai turi būti skatinami kelti savo kompetencijas ir gebėti įtraukti skaitmenines

technologijas į vedamų pamokų turinį siekiant pateikti informaciją mokiniams kuo įvairesniais būdais. Kita išryškėjusi problema, jog mokyklos neturi specialistų, kurie būtų parengti pagal skaitmeninių kompetencijų sąrašą ir gebėtų tinkamai suteikti reikiamą pagalbą mokiniams siekiant tobulinti jų žinias.

Dauguma mokyklų kibernetinių patyčių atvejus sprendžia kaip ir kontaktinių patyčių atvejus, tačiau elektroninėje erdvėje vykstantys veiksmai gali būti nebūtinai susiję tik su toje mokykloje esančiais mokiniais, taip pat mokyklos administracijai gali būti sunku užtikrinti, jog žalingas turinys būtų pašalintas, todėl kiekviena mokykla turėtų būti atsakinga pranešti apie įvykusius atvejus Ryšių reguliavimo tarnybai.

Mokyklose dažniausiai vyksta pavieniai projektai susiję su kibernetiniu saugumu, o mokinių pagrindinė informacija apie kibernetinį saugumą yra ta, kuri įtraukta į informacinių technologijų ugdymo turinį. Tokį mokyklų iniciatyvų pasiskirstymą lemia, jog kiekvienai mokyklai individualiai yra paliekama nuspręsti, kiek norima įsitraukti į kibernetinio saugumo kultūros plėtrą, nėra sukurtos vienos metodinės bazės, kurios padėtų ir prisidėtų prie pamokų turinio kūrimo ir tobulinimo, o daug pavienių, kurios neduoda apčiuopiamos naudos.

3.4. Kiekybinio tyrimo organizavimas

Kiekybinio tyrimo apklausos modeliavimas. Tyrimo pasirinktas instrumentas – apklausa raštu. „Skiriamasis tokių apklausų bruožas – klausimų ir atsakymų procesas yra tik respondento valioje, t. y. kai klausimynas pildomas savarankiškai netarpininkaujant <...> apklausos vykdytojui“ (Gaižauskienė ir Mikėnė, 2014, p. 71). Tyrimo dalyviai į klausimus atsakinėjo savarankiškai, jiems tinkamu metu ir patogioje aplinkoje. Taip tikimasi, jog tyrimo dalyviai labiau įsigilino į klausimus ir juos atsakinėjo nuoširdžiau.

Tyrimo metu buvo siekiama sužinoti koks mokinių dalyvavimo kibernetinėje erdvėje dažnumas, ar jie yra aktyvūs socialinių tinklų naudotojai, kaip mokiniai suvokia skaitmeninėje erdvėje esančias rizikas ir kaip jie yra mokomi kibernetinio saugumo mokyklose. Pagal šiuos tikslus tyrimo klausimai buvo sugrupuoti į 5 temas (žr. 4 lent.)

4 lentelė. Tyrimo klausimų grupės ir tikslai

Eil. Nr.	Grupė	Tikslas
1.	Socialiniai – demografiniai tiriamųjų duomenys	Nustatyti tiriamųjų lytį, amžių ir gyvenamąją vietovę.

4 lentelės tęsinys kitame puslapyje

4 lentelės tęsinys

2.	Dalyvavimas kibernetinėje erdvėje	Išsiaiškinti koks procentas mokinių naudojasi išmaniosiomis technologijomis ir kiek laiko praleidžia elektroninėje erdvėje.
3.	Socialinių tinklų naudojimas	Išsiaiškinti kokia yra mokinių socialinių tinklų naudojimosi kultūra ir suvokimas.
4.	Kibernetinių rizikų suvokimas	Išgryninti kaip jaunimas supranta kibernetines rizikas, ką laiko pagrindinėmis grėsmes skaitmeniniam saugumui.
5.	Kibernetinio saugumo kultūros mokymas	Nustatyti kaip mokiniai yra mokomi kibernetinio saugumo kultūros savo mokyklose.

Tyrimo imtis. Siekiant, jog tyrimo imtis būtų reprezentatyvi, imties tūris buvo apskaičiuotas Ingos Gaižauskienės ir Svajonės Mikėnės pateikta formule (Gaižauskienė ir Mikėnė, 2014, p. 42)

$$n = \frac{t^2 N p(1-p)}{\Delta^2 N + t^2 p(1-p)};$$

Čia: n – imties tūris;

N – populiacijos dydis;

t – stjudento koeficientas;

p – numatomas pasiskirstymas;

Δ - paklaida.

Remiantis Švietimo valdymo informacinės sistemos statistiniais duomenimis 2020-2021 metų mokinių skaičius besimokančiųjų pagal bendro ugdymo programas, kurias sudaro pradinis, pagrindinis, vidurinis mokymas yra 327024 tūkst. (Švietimo valdymo informacinė sistema, 2021). Patikimumas pasirinktas 95%, kaip teigia Gaižauskienė ir Mikėnė (2014): „Paprastai yra naudojamas 95 proc. patikimumo lygmuo kaip kompromisinis pasirinkimas, užtikrinantis toleruotiną patikimumą bei optimalų imties dydį. “ (p. 40). Įvertinus, kokia respondentų skaičiaus galima sulaukti, buvo pasirinkta 5% paklaida.

Atlikus skaičiavimus pagal aukščiau pateiktą formulę gautas tyrimo imties dydis – 384 tyrimo dalyviai.

Kiekybinio tyrimo eiga. Siekiant pasiekti didesnį tyrimo dalyvių skaičių buvo pasirinktas klausimyno pildymas tiesiogiai internetinėje svetainėje. Klausimynas buvo patalpintas į internetinį puslapį www.manoaplkausa.lt. Anketinės apklausos nuoroda buvo pasidalinama socialiniuose

tinkluose, nevyriausybinėse organizacijos, bei su mokytojais, kurie tiesiogiai dirba su vaikais besimokančiais bendrojo ugdymo mokyklose. Tyrimas vyko 2021 m. spalio 19 – lapkričio 19 dienomis. Tyrimas buvo vykdomas iki kol buvo surinkta 384 atsakymai į klausimyną. Iš viso buvo surinkti 386 klausimynai. Anketos kūrimo pasirinktyse nebuvo galima patvirtinti klausimyno, jeigu bent vienas klausimas neatsakytas, todėl visos anketos buvo tinkamos tolimesnei analizei. Kokybinio tyrimo etapų veikla išdėstyta 5 lentelėje.

5 lentelė. Kiekybinio tyrimo eiga

Etapas	Etapo veikla	Etapo tikslas
Pasirengimas	Suformuluojama tyrimo koncepcija ir tyrimo metodas. Parengiamas anketinės apklausos klausimynas, įkeliamas į internetinę platformą.	Parengtas apklausos klausimynas.
Tyrimo vykdymas	Siunčiama klausimyno nuoroda viešaisiais tinklais.	Surinkta informacija apie mokinių kibernetinio saugumo ir rizikų supratimą.
Duomenų analizė	Gautų duomenų sisteminimas, apibendrinama gauta informacija.	Rezultatų interpretavimas, vertinimas ir gautos išvados.

Tyrimo etika. Siekiant užtikrinti sklandų ir saugų tyrimą, buvo laikomasi tyrimo etikos principų. Prieš dalyvaudami apklausoje, tyrimo dalyviai buvo supažindinti su tyrimo tikslu, jo viešinimu ir anonimiškumo užtikrinimu. Tyrimo dalyviams nebuvo daromas tiesioginis ar netiesioginis spaudimas dalyvauti apklausoje, todėl tyrimo dalyviai turėjo laisvą galimybę apsispręsti dėl dalyvavimo apklausoje. Siekiant užtikrinti dalyvių anonimiškumą, visi duomenys yra pateikiami tik apibendrintai, o klausimyno atsakymų rezultatai yra prieinami tik tyrėjui. Anketoje iš asmeninių duomenų buvo prašoma pateikti kokios asmuo yra lyties, amžiaus ir kokio dydžio gyvenvietėje gyvena, šie duomenys buvo reikalingi siekiant pastebėti tendencijas kaip skiriasi kibernetinio saugumo ir rizikų suvokimas skirtingų grupių asmenų.

Duomenų analizės metodai. Duomenų analizei ir apdorojimui buvo naudojama statistinės analizės programos SPSS 26.0 versija. Duomenų apipavidalinimui ir grafiniam pateikimui buvo naudojama MS Office paketo programa MS Exel. Siekiant nustatyti ar tarp kintamųjų yra statistinis ryšis, buvo pasirinkti statistinės duomenų analizės metodai::

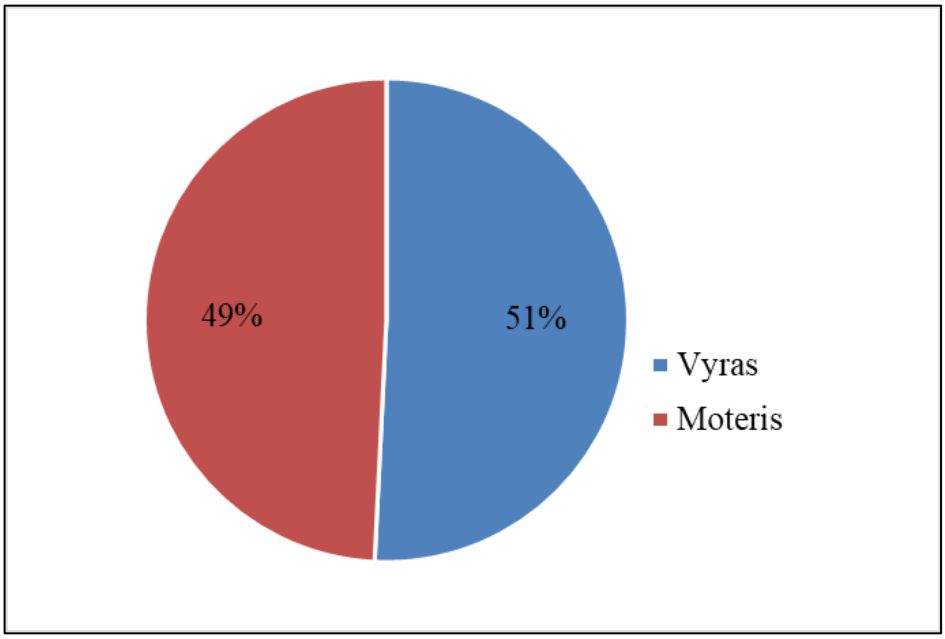
1. Pirsono ksi-kvadrato ($\chi 2$) testas – nominalinių ir ordinalinių kintamųjų bei nominalinių kintamųjų tarpusavio priklausomybei tikrinti;
2. Fišerio tikslusis testas – kur buvo netinkamas Pirsono $\chi 2$ testas.

Duomenų analizei pasirinkta vienoda $\alpha=0.05$ reikšmingumo lygmens reikšmė.

2.1. Kiekybinės apklausos raštu tyrimo rezultatai

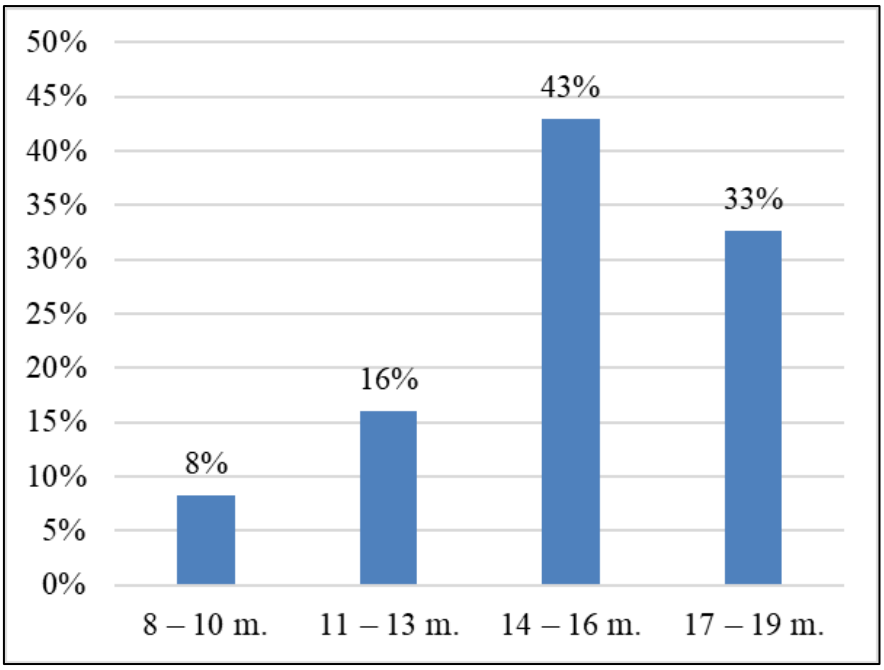
Tyrimo socialiniai demografiniai duomenys.

Tyrime dalyvavo 386 Lietuvos bendrojo ugdymo mokyklose besimokančių mokinių. Iš jų 196 (51%) vaikinų ir 190 (49%) merginų (8 pav.)



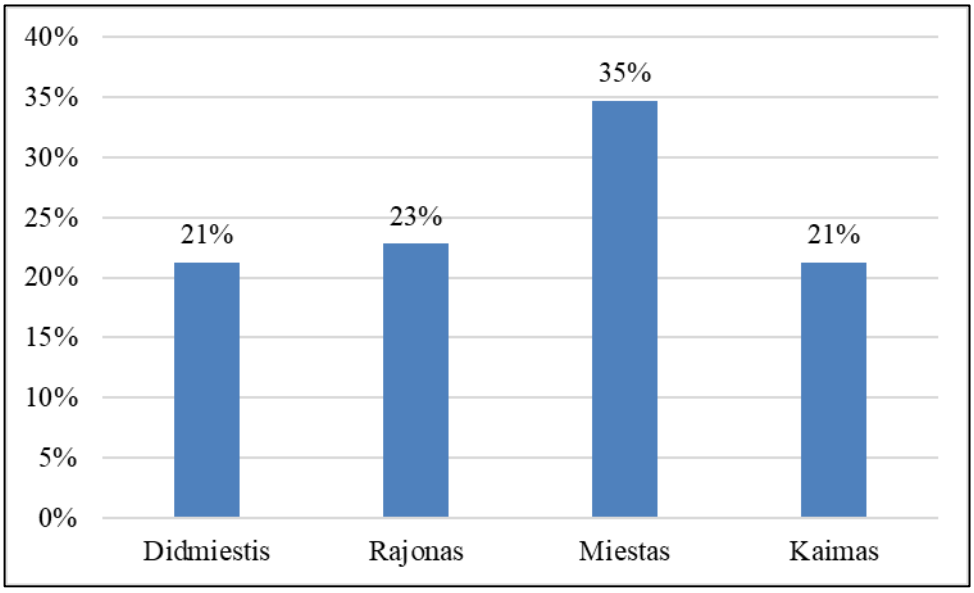
8 pav. Tyrimo dalyvių lytis

Tyrimo dalyviams buvo užduotas klausimas apie jų amžių. Kaip pateikta diagramoje (9 pav.), amžius buvo suskirstytos atsižvelgiant į ugdymo pakopas: pradinis (8 – 10 m.), pagrindinis (11 – 16 m.), vidurinis (17 – 19 m.) ugdymas. Pagrindinio ugdymo pakopos amžiaus grupė buvo išskaidyta į dvi amžiaus grupes dėl tikslesnio tolimesnių tyrimo rezultatų. Daugiausia apklaustųjų buvo 14 – 16 metų – 166 (43%). 126 (33%) buvo 17 – 19 metų jaunimas. Mažiau atsakiusiųjų buvo 11 – 13 metų – 62 (16%) ir 8 – 10 metų – 32 (8%) amžiaus mokinių. Tokį tyrimo dalyvių pasiskirstymą galėjo lemti jog vyresni mokiniai daugiau laiko praleidžia naudodamiesi elektroniniais įrenginiais ir šių amžiaus grupių atstovams apklausa internete buvo lengviau prieinama.



9 pav. Tyrimo dalyvių amžius

Kiek dėmesio skirtingose Lietuvos vietovėse yra dėmesio skiriama kibernetinio saugumo mokymui siekiant nustatyti kibernetinio saugumo mokymo lygį skirtingose Lietuvos vietovėse tyrimo dalyvių buvo prašoma nurodyti jų gyvenamąją vietovę. Tyrimo dalis gyvenanti: didmiesčiuose sudaro 21% (N=82), rajonuose – 23% (N=88), miestuose 35% (n=134), kaimo vietovėse – 21% (N=82) (10 pav.).

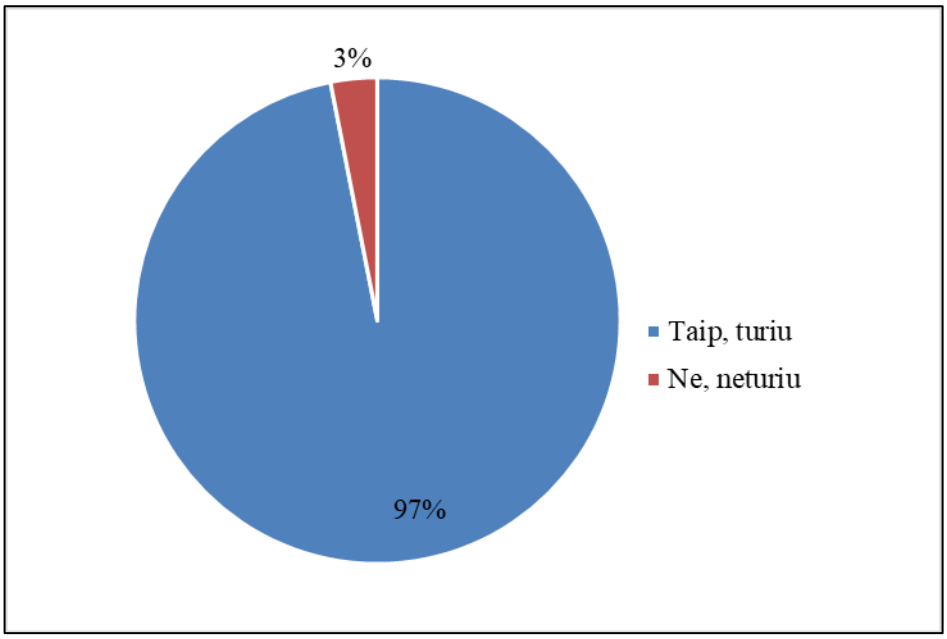


10 pav. Gyvenamoji vieta

Atliekant tyrimą buvo siekiama išsiaiškinti kiek procentų jaunimo turi priėjimą prie elektroninės erdvės ir kiek iš jų turi savo asmeninius įrenginius, kuriais naudojasi.

Pirmasis užduotas klausimas buvo siekiant išsiaiškinti kiek mokyklinio amžiaus vaikų turi savo asmeninius telefonus, kuriais naudojasi. 97% (N=370) pateikė jog turi savo asmeninį įrenginį, 3% (N=12) atsakiusiųjų 8 – 10 metų (8 tyrimo dalyviai) ir 11 – 13 metų (4 tyrimo dalyviai), kurie paminėjo jog savo asmeninių telefonų neturi (11 pav.).

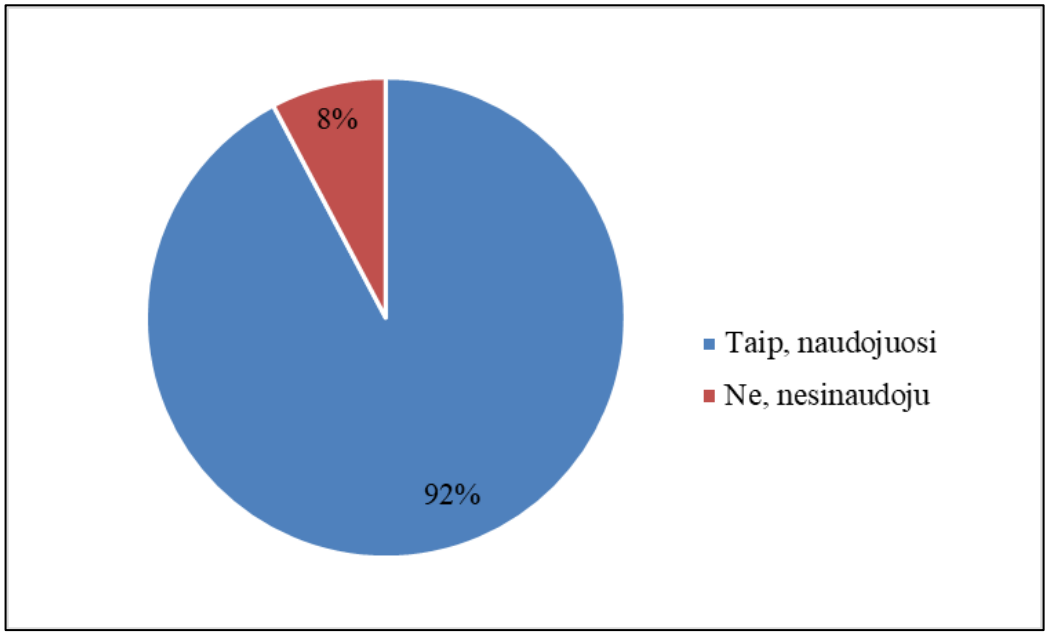
Didelė dalis jauno amžiaus vaikų pradeda naudotis išmaniaisiais įrenginiais. Didelė dalis tėvų pasirenka leisti vaikams turėti asmeninius telefonus, tai vienas galimas iš tėvų kontrolės momentų, kuomet jie nori jog jų vaikai būtų lengviau pasiekiami. Naudodami savo asmeninius telefonus, mokiniai lengvai gali patekti į skaitmeninę erdvę ir tai tik dar kartą įrodo koks yra svarbus jų kuo ankstesnis supažindinimas su tinkama elgsena kibernetinėje erdvėje.



11 pav. Ar turite savo asmeninį išmanųjį telefoną kuriuo naudojatės?

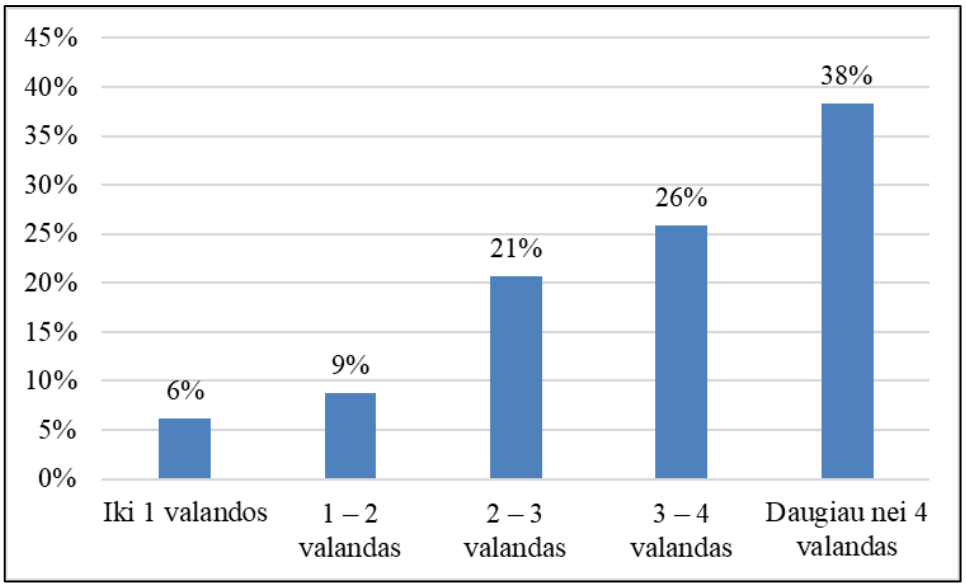
Paklausus mokinių ar naudojasi kompiuteriu, buvo gauti rezultatai (12 pav.) jog 92% (N=356) naudojasi. Dalis mokinių – 8% (N=30) pateikė, jog nesinaudoja kompiuteriu, tačiau turi savo asmeninius išmaniuosius telefonus. Iš atsakiusiųjų, kurie nesinaudoja kompiuteriu 27% (N=8) 8 – 10 (arba 2% nuo bendros imties) metų grupės mokiniai buvo paminėję, jog taip pat neturi savo asmeninio telefono. Tai yra jauniausiųjų grupė, todėl daug priežasčių, gali lemti jog tėvai vis dar riboja prieigas prie elektroninės erdvės arba stengiasi naudojimąsi kontroliuoti.

Vertinant apklausos rezultatus, galima daryti išvadą, jog vis daugiau mokinių naudojasi išmaniaisiais įrenginiais nepriklausomai nuo jų amžiaus, o tai sudaro terpę susidurti su kibernetinėmis grėsmėmis.



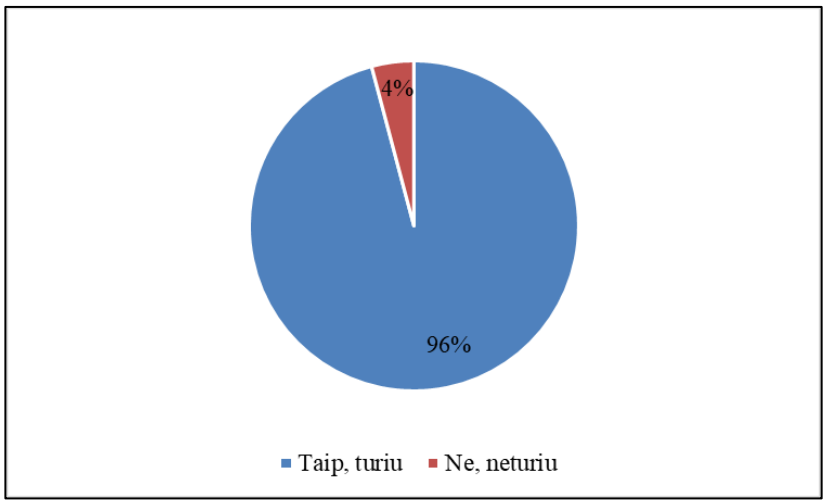
12 pav. Mokinių naudojimasis kompiuteriu

Trečiuoju klausimu buvo siekiama nustatyti kiek vidutiniškai tyrimo dalyviai praleidžia laiko naudodamiesi išmaniaisiais įrenginiais ir ar mokinių amžius turi įtakos praleidžiamam prie išmaniųjų įrenginių laikui. Daugiausiai tyrimo dalyviai paminėjo, jog naudodamiesi išmaniaisiais įrenginiais vidutiniškai per dieną praleidžia daugiau nei 4 valandas – 38% (N=148). Daugiau negu penktadalis mokinių (56%) elektroninėje erdvėje kiekvieną dieną vidutiniškai praleidžia nuo 1 iki 4 valandų: 9% (N=34) nuo 1 iki 2 valandų, 21% (N=80) nuo 2 iki 3 valandų, 26% (N=100) nuo 3 iki 4 valandų. Didžioji dalis atsakiusiųjų, kurie praleidžia naudojantis išmaniaisiais įrenginiais iki 1 valandos – 6% (N=24) yra mokiniai 8 – 10 metų grupėje (13 pav.). Buvo siekiama išsiaiškinti, ar praleidžiamas laikas prie išmaniųjų įrenginių priklauso nuo mokinių amžiaus, tačiau nustatyta, kad tarp mokinių amžiaus ir praleidžiamo laiko prie išmaniųjų įrenginių ($\chi 2=1.665$, df=1, p=0.472) statistiškai reikšmingų skirtumų nėra, tai rodo, kad skirtingo amžiaus mokiniai naudodamiesi išmaniaisiais įrenginiais praleidžia panašų laiko tarpą.



13 pav. Laikas praleidžiamas naudojantis išmaniaisiais įrenginiais

Tyrimo metu buvo klausiama ar mokiniai turi susikūrę savo socialinių tinklų profilius. Absoliuti dauguma tyrimo dalyvių 96% (N=370) patvirtino jog yra prisiregistravę prie bent vieno iš socialinių tinklų. 4 % (N=16) neturinčiųjų socialinių tinkle profilių, priklauso 8 – 10 amžiaus grupei. Buvo siekiama nustatyti, ar socialinių tinklų kūrimas priklauso nuo mokinių amžiaus (14 pav.) Svarbu pabrėžti, jog dauguma socialinių tinklų turi amžiaus apribojimus ir profilio kūrėjas turėtų būti vyresnis negu 13 metų amžiaus, todėl iš pateiktų tyrimo rezultatų galima teigti jog 21% (N=78) (skaičiuojant nuo bendros imties 20%) mokinių profiliuose yra pakeitę savo tikrąjį amžių, jog anketa būtų patvirtinta ir jie galėtų naudotis socialiniu tinklu. Vertinant statistinį ryšį tarp kintamųjų ($\chi 2=1.687$, df=1, p=0.352), matoma, kad statistiškai reikšmingo skirtumo tarp socialinių tinkle turėjimo ir amžiaus nėra ir nepriklausomai nuo mokinių amžiaus, didžioji dauguma mokinių turi socialines paskyras, net jeigu tai reiškia, kad jie pažeidžia tinklapių vidines nuostatas.

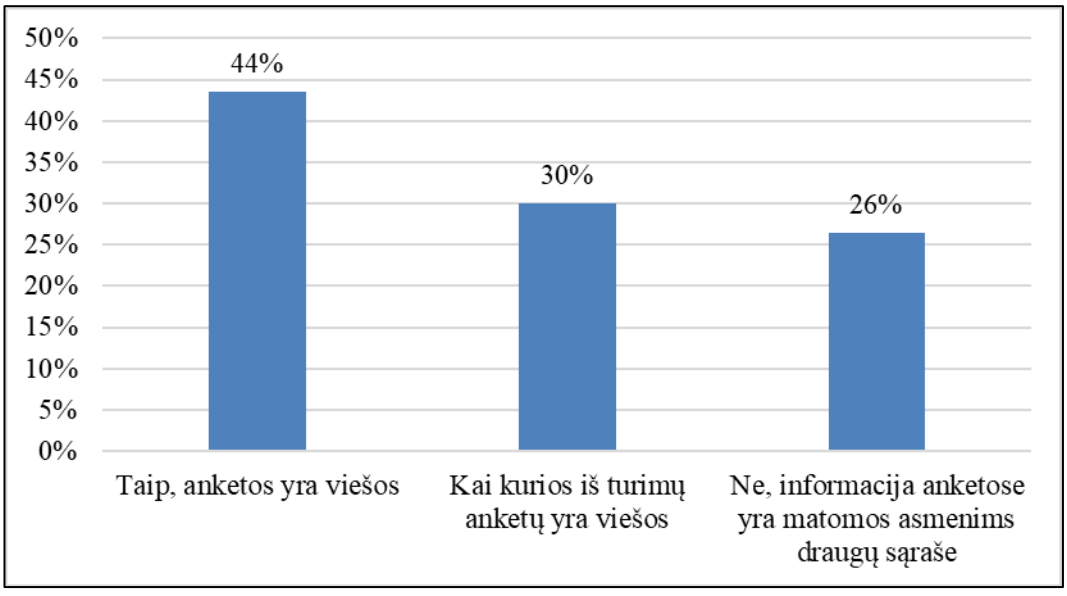


14 pav. Socialinių tinklų profilio turėjimas

Norint išsiaiškinti kaip tyrimo dalyviai saugo savo informaciją, kurią skelbia socialiniuose tinkluose, nuo pašalinių asmenų, buvo paklausta ar jų profilių anketos yra viešos. 44% (N=168) mokiniai paminėjo, jog jų informacija yra vieša ir pasiekiama, bei ją gali peržiūrėti visi vartotojai, kurie ir nėra jų draugų sąraše. 30% (N=116) atsakė, jog tik kai kurių turimų socialinių tinklų anketų yra viešos. 26% (102) pateikė, jog priėjimas prie jų asmeninio profilio duomenų yra apribotas ir yra matomas tik asmenims esantiems jų draugų sąraše (15 pav.)

Diferenciacijos tarp lyties ir viešai prieinamų anketų nepastebėta, labai panašus procentas atsakiusiųjų vaikinų ir merginų pateikė jog jų profiliai yra atviri. Pagal amžių išsiskiria, jog viešos anketos vyrauja pas 14 – 16 metų mokinius. Šios amžiaus grupės jaunimas dauguma yra nauji socialinių tinklų erdvės vartotojai, todėl jie dažniau gali susidurti su sutarties sutikimo rizikomis, kuomet pradėdami valdyti savo paskyras, jie nežino kaip tinkamai jas reikėtų apsaugoti ir nusistatyti tinkamus privatumo nustatymu.

Pastebimas stiprus statistinis ryšis tarp mokinių amžiaus ir jų socialinių tinklų apsaugos, tyrime galima pamatyti, kad vyriausiųjų klasių mokiniai (amžiaus grupė 17 – 19 metų) yra labiau linkę laikyti savo informaciją pasiekiamą tik asmenims esantiems jų draugų sąraše ($\chi 2=1.887$, df=1, p=0.724), tuo tarpu 14 – 16 amžiaus mokiniai, galėdami oficialiai užsiregistruoti socialiniuose tinkluose, dažniau nepaiso privatumo politikos ir savo profilius palieka atvirus.



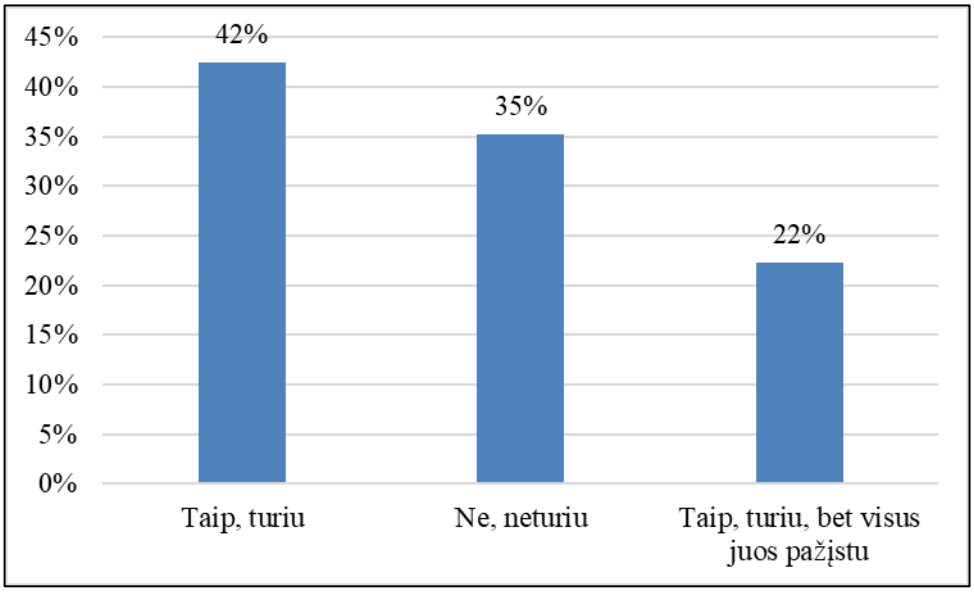
15 pav. Socialinių tinklų profilių prieinamumas

Viena iš socialiniuose tinkluose išskiriamų rizikų yra kontaktinės rizikos. Norint išsiaiškinti kokį dėmesį mokiniai skiria atsirinkdami ką priimti į savo draugų grupę buvo aiškinamasi ar jie turi platformose draugų, kurių nepažįsta ir nebuvo sutikę gyvai. Iš visų atsakiusiųjų didžiausią dalį – 42%

(N=164) sudaro vartotojai, kurie savo paskyrose yra priėmę į draugus asmenis, kurių nepažįsta ir su jais dalinasi savo skelbiama informacija. 35% (N=136) pateikė, jog visi asmenys esantys jų draugų sąraše yra jiems pažįstami, o 22% (N=86) mokiai kai kurių asmenų iš savo draugų sąrašo nėra sutikę gyvai, bet visi jiems yra pažįstami (16 pav.).

14 – 16 metų amžiaus grupės mokiniai statistiškai patikimai dažniau ($\chi2=1.887$, df=1, p=0.052) socialiniuose tinkluose bendravo su asmenimis, kurių nepažįsta ir su kuriais nebuvo susitikę gyvai, lyginant su 17 – 19 metų mokiniais (atitinkamai 68% ir 41%). Tuo tarpu tarp 8 – 10 (p=0.201) ir 11 – 13 (p=0.352) metų amžiaus mokinių reikšmingų skirtumų nenustatyta.

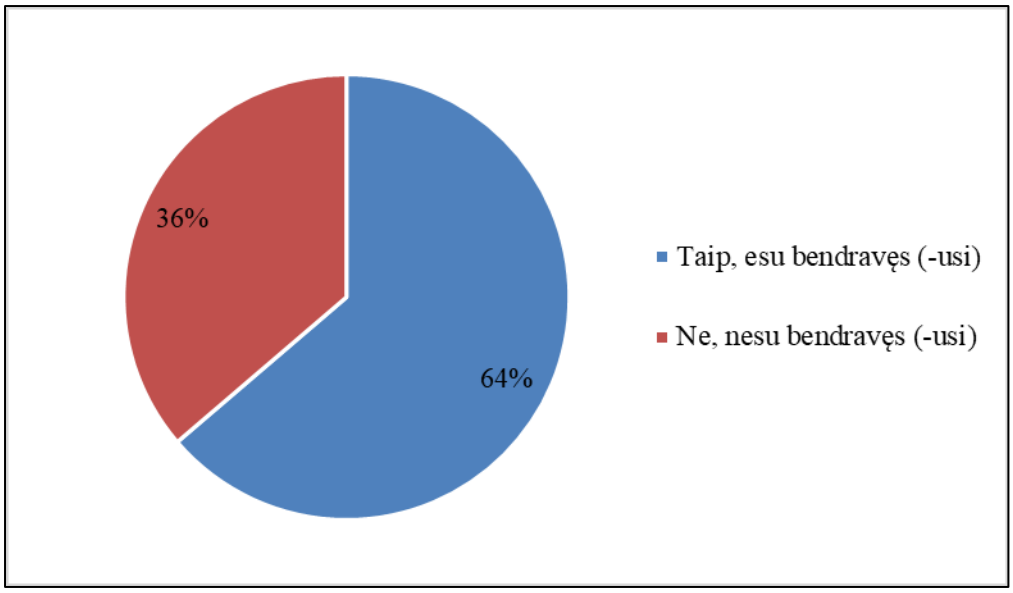
Tokie rezultatai rodo, kad būtent 14 – 16 metų amžiaus mokiniai turi didžiausią tikimybę susidurti su kibernetinėmis grėsmėmis, bendraudami su jiems nepažystamais asmenimis.



16 pav. Ar socialinių tinklų platformose turite draugų, kurių nepažįstate ir nesate sutikę gyvai?

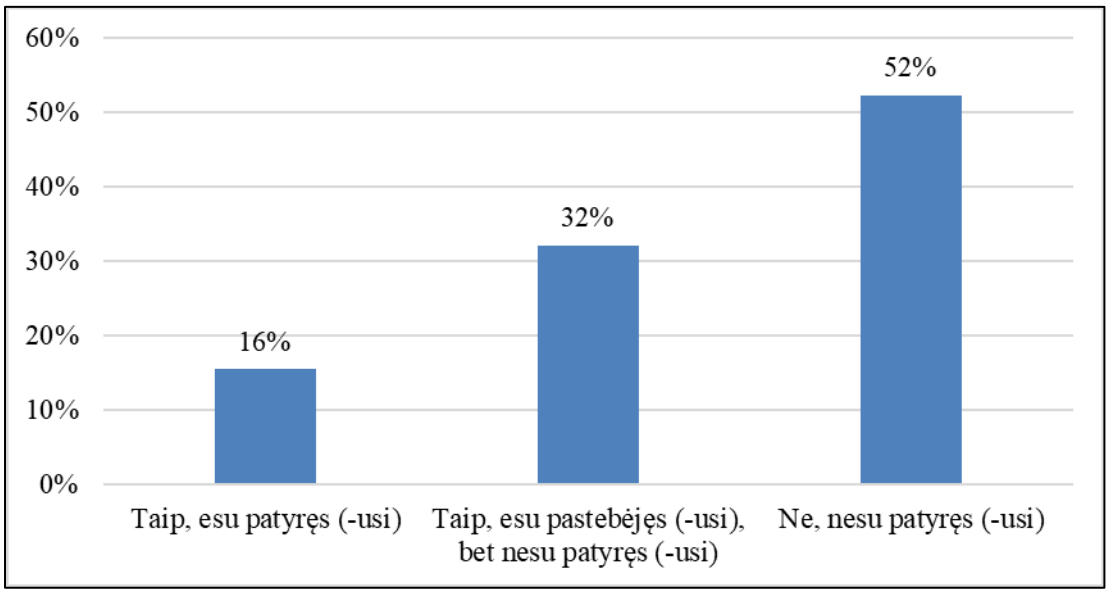
Siekiant išsiaiškinti mokinių kontaktinių rizikų suvokimą buvo prašoma pažymėti ar kada nors tyrimo dalyviai buvo bendravę su asmeniu elektrinėje erdvėje, kurio niekada nebuvo sutikę gyvai. 64% (N=246) pažymėjo, jog su asmenimis, kurių nėra sutikę gyvai bendrauti yra tekę, o 36% (N=140) niekada nėra to darę (17 pav.).

Statistiškai dažniau su nepažystamais asmenimis bendraudavo merginos ($\chi2=1.925$, df=1, p=0.788), negu vaikinai ($\chi2=1.651$, df=1, p=0.412), todėl galima daryti prielaidą, kad būtent merginos turi didesnę tikimybę susidurti grėsmėmis internetinėje erdvėje, kadangi jos labiau linkusios nepaisyti galimų kontaktinių rizikų.



17 pav. Ar kada nors esate bendravę su asmeniu elektroninėje erdvėje, kurio niekada nebuvote sutikę gyvai?

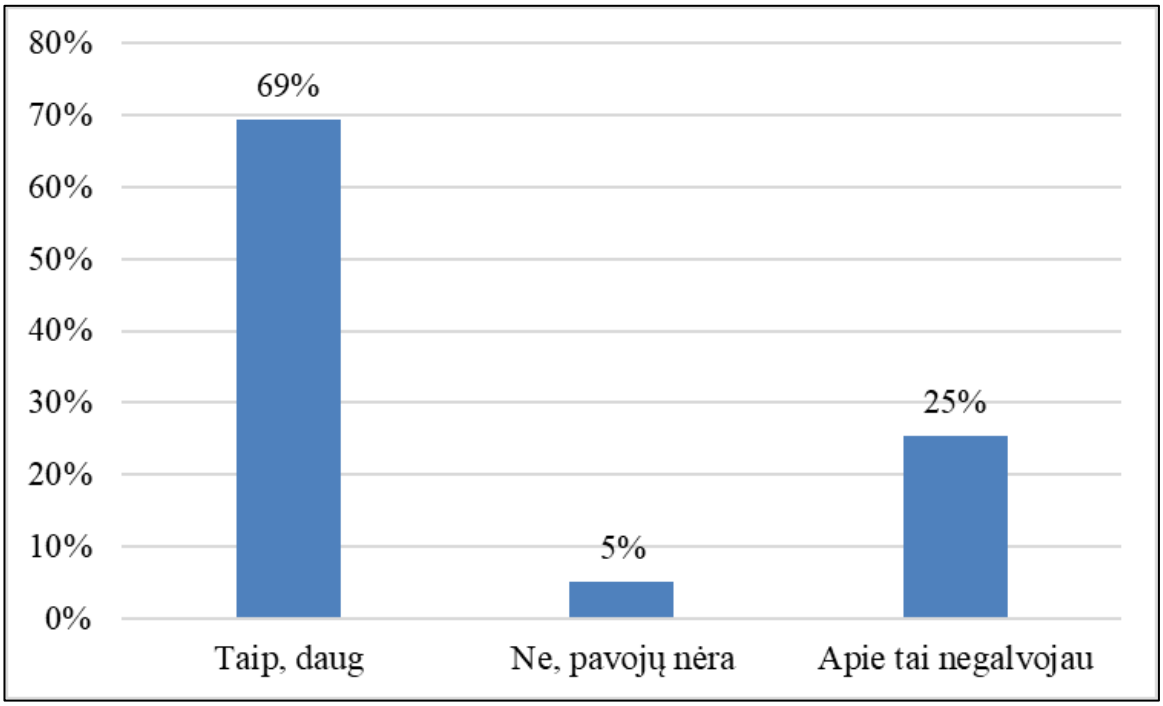
Kibernetinėje erdvėje jaunimas gali susidurti su viena iš emociškai galinčių paveikti kontaktinių ir elgesio rizikų – patyčios, kuomet yra nutaikytas tiesioginis poveikis asmeniui siekiant jį pašiepti, įbauginti ar kaip kitaip paveikti. Paklausus tyrimo dalyvių ar jie yra susidūrę su šiuo reiškiniu, 16% (N=60) yra patyrę patyčias elektroninėje erdvėje, 32% (N=124) buvo pastebėję, kuomet patyčias patiria elektroninėje erdvėje kiti. Daugiau negu pusė 52% (N=202) pažymėjo, jog šio reiškinio nėra patyrę (18 pav.).



18 pav. Ar esate pastebėję/ patyrę elektroninių patyčių socialiniuose tinkluose, naudodami bendravimo platformas?

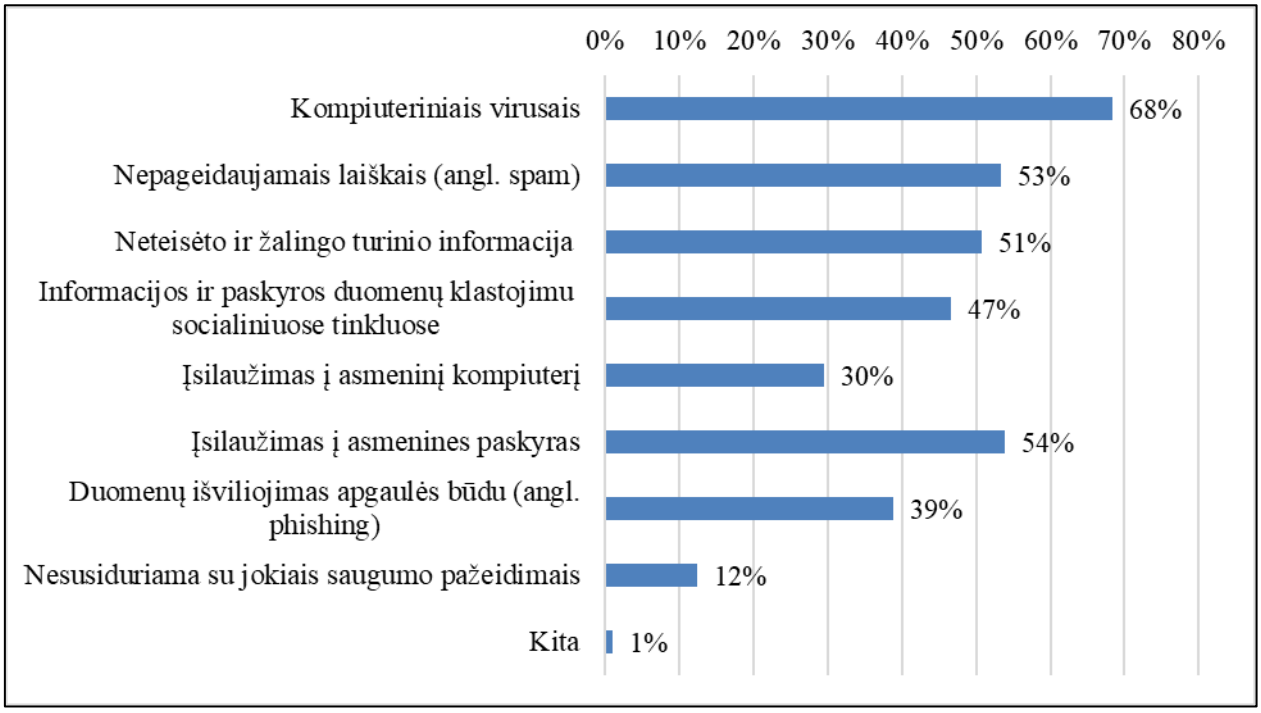
Siekiant sužinoti kaip mokiniai vertina ar kibernetinėje erdvėje yra daug pavojų, jų buvo prašoma pažymėti savo nuomonę. Didžioji dauguma – 69% (N=268) tyrimo dalyvių teigia, jog elektroninėje erdvėje yra daug pavojų, jog pavojų nėra mano 5% (N=20), o apie tai nėra galvoję ketvirtadalis atsakiusiųjų mokinių – 25% (N=98) (19 pav.).

Atsižvelgiant į tyrimo rezultatus, pastebimos tendencijos, jog nepriklausomai nuo mokinių amžiaus, visi supranta, jog internetinėje erdvėje egzistuoja įvairaus lygio pavojai, kas sąlygoja, jog mokiniai ganėtinai sąmoningai vertina galimybes susidurti su kibernetinėmis grėsmėmis.



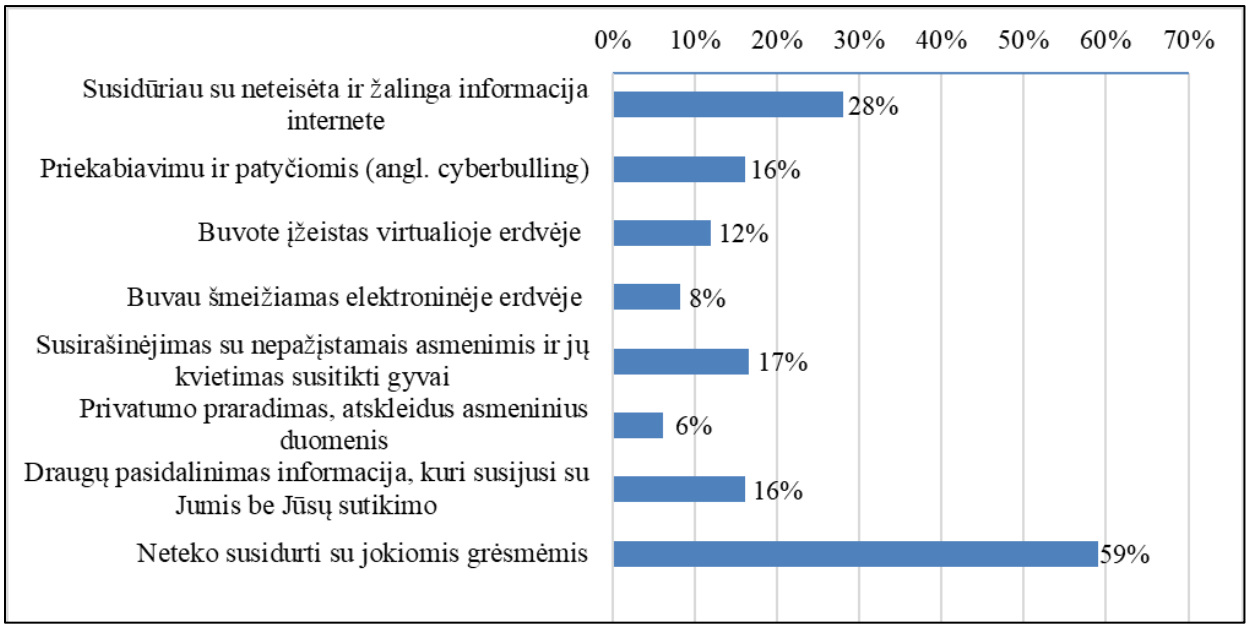
19 pav. Kaip manote, ar elektroninėje erdvėje yra daug pavojų

Siekiant sužinoti kokias kibernetines grėsmes pastebi mokiniai, jų buvo klausiama su kokiomis kibernetinėmis grėsmėmis dažniausiai susiduriama elektroninėje erdvėje. Atsakydami į šį klausimą, mokiniai galėjo pasirinkti kelis atsakymus, taip pat mokiniai galėjo įrašyti, kokios, jų nuomone, gali būti grėsmes internete. 68% (N=264) tyrimo dalyvių atsakė, jog viena didžiausių kibernetinių grėsmių yra kompiuteriniai virusai. Panašus procentas: 54% (N=208) mano jog yra susiduriama su duomenų išviliojimu apgaulės būdu, 53% (N=206) – nepageidaujamais laiškais ir 51% (N=196) – neteisėto ir žalingo turinio informacija. Jaunimas manoma, jog rečiau susiduriama su šiais pažeidimais: informacijos ir paskyros duomenų klastojimu socialiniuose tinkluose – 47% (N=180), duomenų išviliojimu apgaulės būdu – 39% (N=150), įsilaužimu į asmeninius kompiuterius – 30% (N=114). Manančiųjų, jog kibernetinėje erdvėje nėra susiduriama su jokiais saugumo pažeidimais – 12% (N=48). 1% (N=4) teigė, jog galimos tokios grėsmės, kaip duomenų bazės nutekėjimas ar informacijos praradimas (20 pav.).



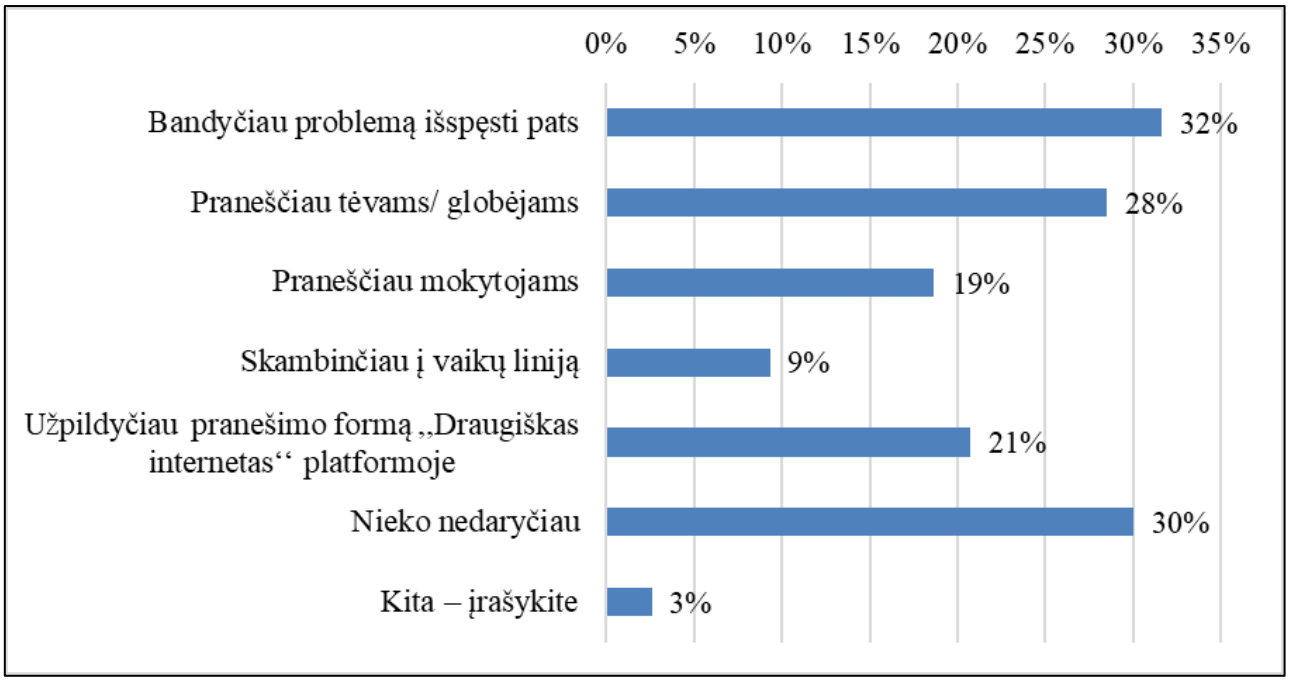
20 pav. Kaip manote, su kokiais tinklų ir informacijos saugumo pažeidimais internete susiduriama dažniausiai?

Paklausus su kokiomis grėsmėmis mokiniai susidūrė asmeniškai 28% (N=108) mokinių susidūrė su neteisėta ir žalinga informacija, 17% (N=64) bendravo su nepažįstamais asmenimis ir gavo jų kvietimą susitikti gyvai, 16% (N=62) patyrė priekabiavimą ir patyčias, bei buvo pasidalinama informacija susijusia su jais pačiais be jų sutikimo, 12% (N=46) buvo bent kartą įžeisti virtualioje erdvėje. Kiek mažiau: 8% (N=32) mokinių buvo šmeižiami kibernetinėje erdvėje, o 6% (N=24) buvo praradę privatumą atskleidus jų asmeninius duomenis. Daugiau negu pusė tyrimo dalyvių – 59% (N=228) su jokiomis grėsmėmis kibernetinėje erdvėje nėra susidūrę. (21 pav.)



21 pav. Su kokiomis grėsmėmis Jums asmeniškai yra tekę susidurti?

Pastebėjus patyčias, neteisėtą turinį elektroninėje erdvėje dauguma mokinių – 32% (N=122) bandytų problemas spręsti patys. Tačiau čia kyla grėsmė, jog ketinant imtis iniciatyvos patiems ir apginti save ar kitus ir sprendžiant problemas elektroninėje erdvėje savarankiškai, tokie veiksmai gali sukelti pavojų ginančiajam, nes jis patys galėtų tapti patyčių auka. 30% (N=116) tyrimo dalyvių išliktų pasyvūs ir nedarytų nieko. Aktyviai nereaguodami į situaciją mokiniai apsaugotų savo nuo galimų grėsmių, tačiau tai gali sukelti pasekmes patyčias patiriančiam asmeniui, nes jis gali pats bijoti kreiptis pagalbos arba taip nėra užkertamas kelias plisti neteisėtai informacijai internete ir ji galimai pasieks didesnę dalį vartotojų. Svarbu pastebėti, jog daugiausia pasirinkusiųjų atsakymą „nedaryčiau nieko“ buvo tarp 14 – 16 metų mokinių – 64% visų apklaustųjų toje mažiaus grupėje, o atsižvelgiant į tai, kad šio amžiaus mokiniai yra vieni aktyviausių socialinių tinklų naudotojų, kyla didelė grėsmė, jog patyčios gali būti nesustabdytos laiku dėl mokinių atsainaus požiūrio į jas. 28% (N=110) tyrimo dalyvių praneštų apie pastebėtą neteisėtą informaciją ar veiką tėvams/ globėjams. 21% (N=80) užpildytų anoniminę anketą svetainėje „Draugiškas internetas“, 19% (N=72) apie įvykį praneštų mokytojams, o 9% (N=36) skambintų į „Vaikų liniją“. Atsakymą „kita“ pasirinkę tyrimo dalyviai paminėjo, jog stebėtų situaciją ir bandytų suprasti kodėl tokia situacija kilo, bei rasti galimus problemų sprendimo būdus, kiti paminėjo, jog kreiptųsi į policiją ar užpildytų pranešimą „E. policija“ portale (22 pav.).

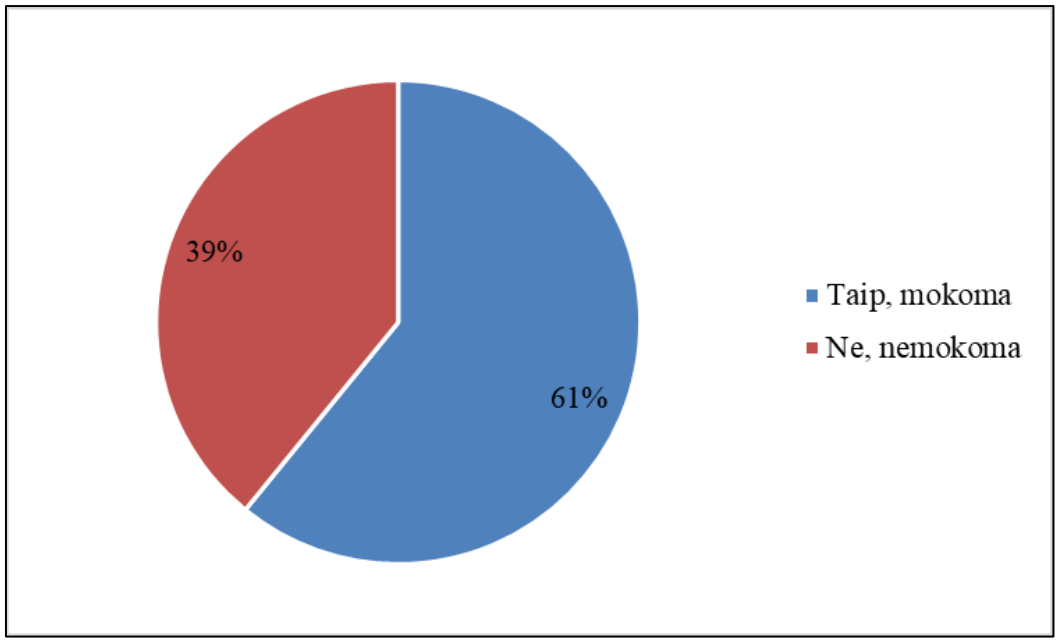


22 pav. Kaip elgėtės/ elgtumėtės pastebėjus patyčias, neteisėtą turinį elektroninėje erdvėje?

Mokinių buvo klausiama ar jų mokyklose yra mokoma skaitmeninio saugumo. 61% (N=235) atsakiusiųjų pateikė jog yra mokoma skaitmeninio saugumo. 39% (N=151) atsakė, jog tokio pobūdžio mokymas nėra vykdomas (23 pav.).

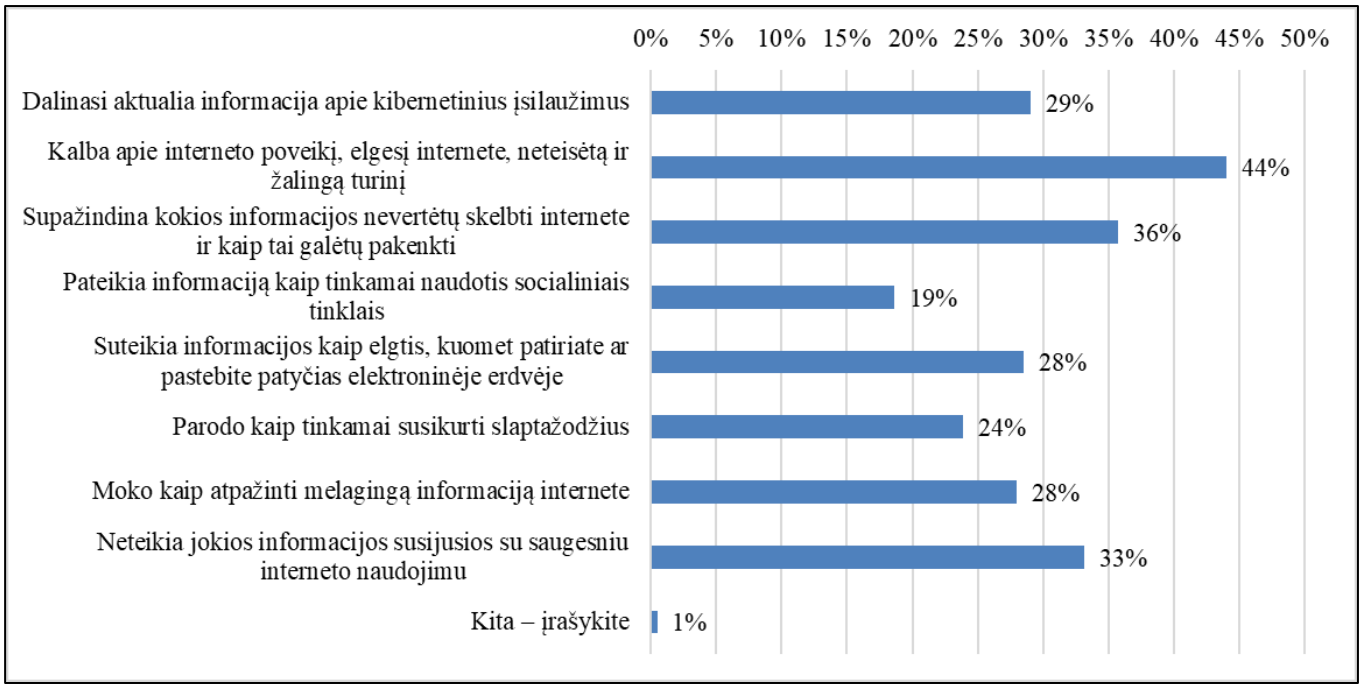
Net 82% (N=125) visų atsakiusiųjų, jog tokio pobūdžio mokymas nevykdomas, buvo tarp 14 – 19 metų amžiaus mokinių. Tokie tyrimo rezultatai leidžia daryti prielaida, jog dabar mokyklos didžiausią dėmesį skaitmeninio saugumo srityje skiria jaunesnio amžiaus mokiniams, kurie taps atsakingesni vartotojai, tuo tarpu vyresnio amžiaus mokinių rizikos internetinėje erdvėje galimai kyla dėl neskiriamo dėmesio jų skaitmeninio saugumo mokymui ir saugaus elgesio internete propagavimui.

Taip pat buvo bandoma išsiaiškinti, ar skaitmeninio saugumo mokymai priklauso nuo mokinių gyvenamosios vietovės, tačiau nustatyta, kad tarp skaitmeninio saugumo mokymų ir mokinių gyvenamosios vietovės, jei mokiniai gyvena ir mokosi kaime ($\chi2=0.125$, df=1, $p=0.652$), miesto rajone ($\chi2=0.264$, df=1, $p=0.764$), mieste ($\chi2=0.394$, df=1, $p=0.781$) ir didmiestyje ($\chi2=0.097$, df=1, $p=0.832$) statistiškai reikšmingų skirtumų nėra, ir nepriklausomai nuo gyvenamosios vietovės, mokiniams suteikiamos vienodos mokymosi sąlygos.



23 pav. Ar mokykloje yra mokoma skaitmeninio saugumo?

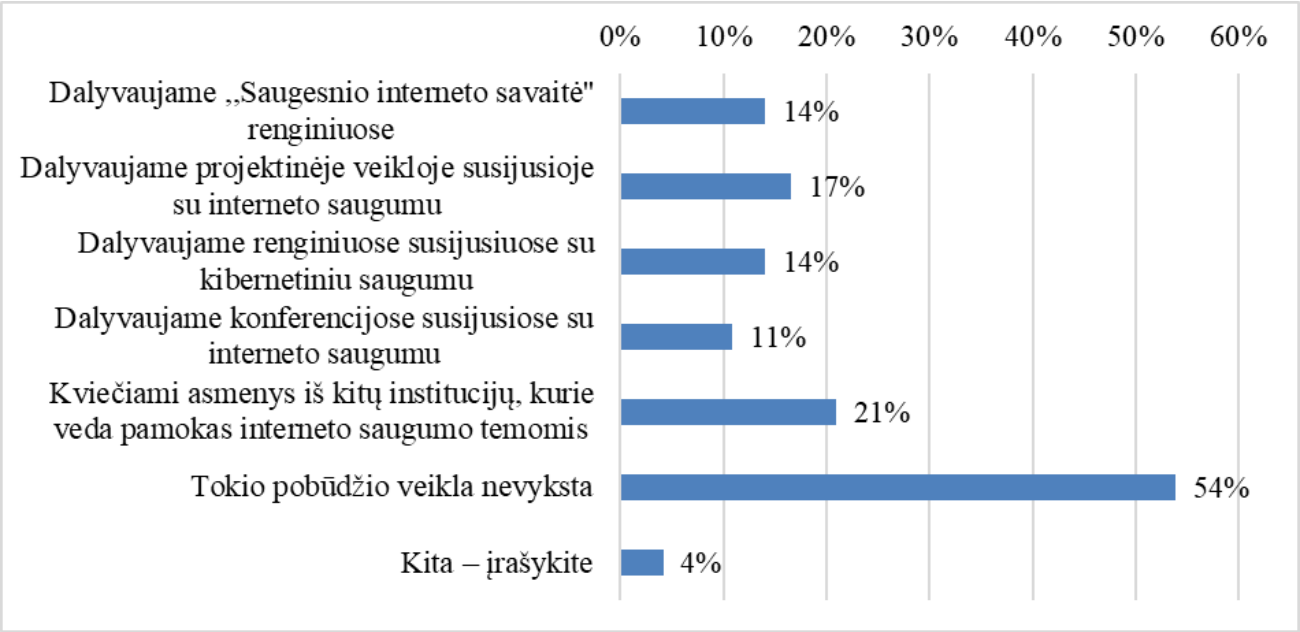
Norint sužinoti kaip mokytojai prisideda prie skaitmeninio saugumo ugdymo mokinių buvo klausiama kokios pobūdžio informacijos jie sulaukia. Daugiausiai, 44% (N=171) mokinių, teigė jog mokykloje yra kalbama apie interneto poveikį, elgesį internete, neteisėtą ir žalingą turinį. 36% (N=139) tyrimo dalyvių yra supažindinami su rekomendacijomis kokios informacijos nereikėtų skelbti internete ir kaip tai galėtų daryti įtaką jiems asmeniškai. 29% (N=112) jaunimui yra pateikiama aktuali informacija apie kibernetinius įsilaužimus. Kiek mažiau, 28% (N=108), paminėjo, jog juos yra mokoma kaip atpažinti melagingą informaciją internete, tiek pat procentų mokinių pateikė, jog jiems suteikiama informacija kaip jie turėtų elgtis susidūrus su patyčiomis elektroninėje erdvėje. 24% (N=93) mokinių yra suteikiama informacija kaip reikėtų tinkamai susikurti slaptažodžius. Mažiausiai mokinių – 19% (N=72) gauna informacijos ir rekomendacijų kaip turėtų tinkamai naudotis socialiniais tinklais. 33% (N=128) tyrimo dalyvių pateikė, jog jokios informacijos susijusios su saugesniu interneto naudojimu iš mokytojų nesulaukia (24 pav.).



24 pav. Kaip mokytojai padeda Jums saugiau naudotis skaitmenine erdve?

Mokyklose, kuriose mokiniai turi su kibernetinio saugumo mokymu susijusias veiklas, buvo klausiama kokia veikla yra vykdoma. 21% (N=81) tyrimo dalyvis pažymėjo jog į mokyklą yra kviečiami asmenys iš kitų institucijų, kurie veda pamokas interneto saugumo temomis. 17% (N=64) mokinių dalyvauja projektinėse veiklose susijusiose su interneto saugumu. 14% (N=54) dalyvauja „Saugesnio interneto savaitė“ renginiuose ir dalyvauja renginiuose susijusiuose su kibernetiniu saugumu. Kiek mažiau – 11% (N=43) dalyvauja projektinėje veikloje. Daugiau negu pusė 54% (N=208) mokinių atsakė jog jokia veikla susijusi su kibernetinio saugumo mokymu jų mokyklose nėra vykdoma. 4% (N=16) pasirinkę atsakymą „kita“ paminėjo, jog kibernetinio saugumo temos yra paliečiamos per informacinių technologijų pamokas, kiti jog yra vedama pamoka vieną kartą per metus, bendraujama su kibernetinio saugumo komandomis, vykdo apklausas (25 pav.).

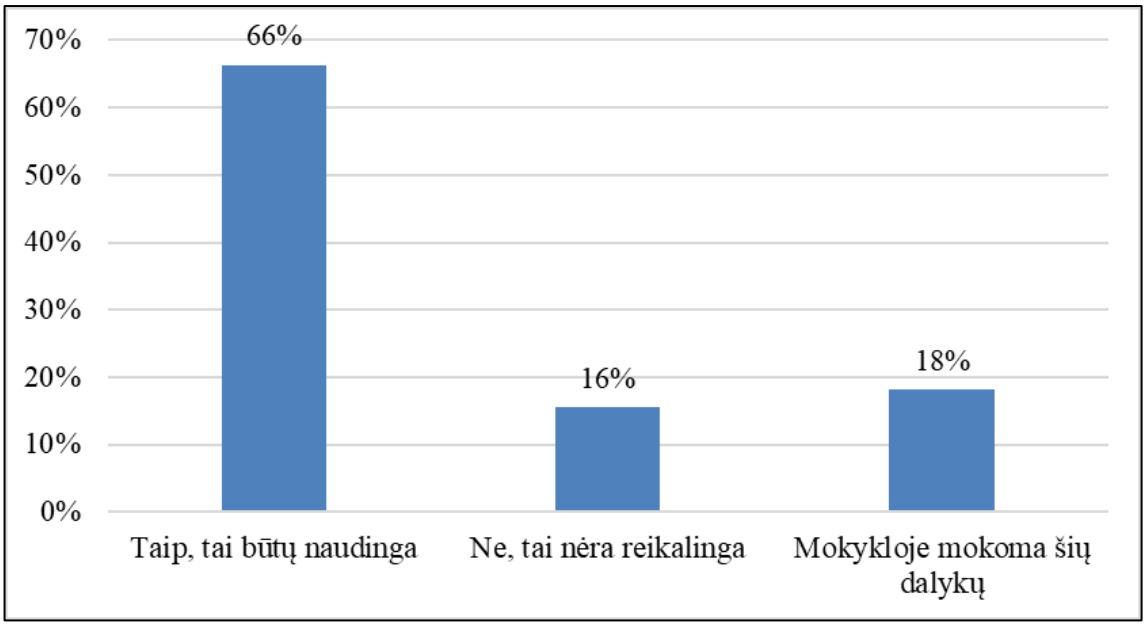
Iš pateiktų atsakymų matoma, jog dalyje mokyklų ganėtinai aktyviai yra stengiamasi plėtoti kibernetinio saugumo kultūrą mokinių tarpe, juos įtraukiant į įvairias veiklas ir taip plečiant bendrą suvokimą, žinias ir ugdant patirtį. Tačiau vis dar daugiau negu pusė mokinių tokio pobūdžio mokymo neturi, todėl jiems kyla grėsmė neatpažinti ir susidurti su galimomis iškylančiomis kibernetinėmis rizikomis.



25 pav. Jeigu mokykloje vykdomas kibernetinio saugumo mokymas, kokia veikla yra vykdoma?

Paklausus mokinių ar jie mano jog yra reikalinga, jog jie būtų mokomi kibernetinio saugumo mokyklose, kurio metu būtų supažindinami su internetinėmis ir techninėmis grėsmėmis, bei kaip jie turėtų elgtis 66% (N=256) tyrimo dalyvių patvirtino jog toks mokymas jiems būtų naudingas. 18% (N=70) paminėjo jog šių temos yra aiškinamos pamokų metu. 16% (N=60) mano, jog tai nėra reikalingos mokymosi temos (26 pav.). Vertinant mokinių nuomone atsižvelgiat į jų amžių, 8-10 m. amžiaus grupė ($\chi2=0.354$, df=1, p=0.650), 11-13 m. amžiaus grupė ($\chi2=0.225$, df=1, p=0.664), 14-16 m. amžiaus grupė ($\chi2=0.487$, df=1, p=0.773) ir 17-18 m. amžiaus grupė ($\chi2=0.257$, df=1, p=0.732), statistiškai nei vienoje amžiaus grupėje reikšmingų skirtumų pastebėta nebuvo ir skirtingos amžiaus grupės turėjo panašią nuomonę, o tai leidžia teigti, jog kibernetinio saugumo poreikis ir jo svarbos suvokimas visiškai nepriklauso nuo mokinių amžiaus.

Mokyklose vis plačiau yra mokoma saugaus elgesio internetinėje erdvėje, tačiau kibernetinio saugumo mokymas ir kultūros plėtojimui reikalingas platesnis supratimas kaip veikia sistemos, su kokiomis rizikomis galima susidurti neturint reikiamų žinių ir kaip reikėtų elgtis susidūrus su problema. Todėl galima teigti, jog mokyklose yra nepakankamai dėmesio skiriama kibernetinio saugumo kultūros ugdymui.



26 pav. Ar manote, jog būtų naudinga jog mokykloje mokytų kibernetinio saugumo, kurio metu būtų supažindinama kaip saugiai naudotis elektronine erdve, bei įvairiomis technologinėmis grėsmėmis?

Apibendrinus pastebima jog Lietuvos mokiniai yra aktyvūs kibernetinės erdvės naudotojai, kurių didžioji dauguma naudojasi išmaniaisiais įrenginiais daugiau nei 3 valandas per dieną. Taip pat dauguma jų yra socialinių tinklų vartotojai. Tai yra ganėtinai didelis laiko tarpas, kurio metu naršydami, bendraudami potencialiai gali susidurti su įvairiomis grėsmėmis.

Didelė dalis mokinių savo paskyrų nustatymuose yra suteikę prieigą peržiūrėti visą savo turinį vartotojams nesantiems jų draugų sąraše, taip pat tarp savo kontaktų turi asmenų, kurių nepažįsta ir gyvai niekada nėra matę, tačiau su tokiais asmenimis bendravę socialinė erdvėje, tai gali iššaukti kontaktines ir elgesio rizikas, kuomet asmeninė informacija apie juos yra pasiekiama dideliam ratui asmenų. Tai patvirtina, ir tai jog 16% yra patyrę patyčias, o 32% jas buvo yra pastebėję . Atsižvelgiant į tai, Galima teigti jog mokyklos ir tėvai įdeda yra per mažą indėlį formuojant tinkamą mokinių elgesį ir taip neapsaugodami jų elektroninėje erdvėje.

Didžioji dauguma mokinių sutinka jog skaitmeninėje erdvėje yra daug pavojų. Įvardindami su kokiais pažeidimais galima susidurti dažniausiai, pirmoje vietoje įvardino kompiuterinius virusus, o antroje vietoje dažniausiai paminėtas atsakymas yra įsilaužimas į asmenines paskyras. Tai sukelia privatumo paradoksą, kuomet jaunimas supranta galimą įsilaužimą į paskyrą kaip grėsmę, bet nesuvokia, jog reikia saugoti socialinių tinklų paskirose esančią informaciją nuo trečiųjų šalių.

Galima teigti jog mokyklinio amžiaus vaikams nėra suteikiama pakankamai informacijos kaip jie turėtų reaguoti į pažeidimus kibernetinėje erdvėje, todėl trečdalis iš jų liktų pasyvūs ir matydami

rizikas nedarytų nieko, o kitas trečdalis bandytų problemą spręsti patys, kas gali lemti jų tapimą patyčių auka.

Daugelyje Lietuvos mokyklų yra mokoma skaitmeninio raštingumo, kurio metu mokiniai yra supažindinami su aktualiomis temomis kaip tinkamai elgtis elektroninėje erdvėje. Nepaisant to galima teigti jog mokyklose šios temos yra pagrinde su koncentruotos į informacinių technologijų pamokas, nes daugiau negu pusė mokinių nedalyvauja jokioje projektinėje veikloje, kurios metu būtų supažindinami su kibernetiniu saugumu plačiau. Patys mokiniai pritaria, jog yra reikalingas toks mokymas, kuris praplėstų jų žinias ir žinojimą kaip atsakingai naudotis įrenginiais, juos apsaugoti ir patiems išlikti saugiems.

IŠVADOS

1. Mokslininkai identifikuoja, jog silpniausia kibernetinio saugumo grandis yra vartotojai ir žmogiškos klaidos, būtent tai gali sukelti didelį pavojų prarandant informacijos prieinamumą, vientisumą ir konfidencialumą. Kibernetinio saugumo kultūra turėtų būti suprantama kaip besikeičianti ir prisitaikanti prie naujausių procesų sistema siekiant vystyti žmonių supratimą ir tobulinant jų įgūdžius siekiant užkirsti kelią vis naujoms atsirandančioms grėsmėms.

2. Kibernetinė saugumo kultūra yra neatsiejama nuo keturių lygmenų: tarptautinio, nacionalinio, organizacinio ir individualaus. Tarptautinė kibernetinė saugumo kultūra apima bendro saugumo kultūros kūrimo procesą siekiant numatyti gaires šalims, jog jų kuriamos sistemos atitiktų pasaulines tendencijas. Nacionalinė kibernetinė saugumo kultūra numato reguliavimą šalies lygmeniu ir užtikrina bendrus saugumo standartus, bei remia šalies gyventojų švietimo iniciatyvas. Organizacinė kibernetinė saugumo kultūra atsižvelgia kaip apsaugoti savo vidinę infrastruktūrą ir sistemas, bei kaip apsaugoti vartotojus, klientus ar suinteresuotus asmenis. Individuali kibernetinio saugumo kultūra apima asmenines žmogaus žinias ir žinojimą, kaip elgtis ir reaguoti iškilus grėsmėms.

3. Naudodamiesi skaitmenine erdve, ieškant informacijos, bendraujant ar pramogaujant, vartotojai gali susidurti su šiomis pagrindinėmis rizikomis: kontaktinėmis, turinio, elgesio ir sutikimų. Neturint reikiamų skaitmeninio raštingumo sugebėjimų ir supratimo kaip reikėtų reaguoti į esamas grėsmes, vartotojai gali nukentėti asmeniškai patiriant finansinių nuostolių, psichologinių ar emocinių sutrikimų, prarasti savo asmeninius duomenis ar pakenkti savo reputacijai, Ypatingai tai yra pavojinga vaikams, kuomet jų asmenybės tik formuojasi ir tokie susidūrimai gali daryti įtaką jų tolimesnio gyvenimo perspektyvoms ar pasirinkimams.

4. Asmeninė kibernetinė higiena ir tinkamai veikianti kibernetinio saugumo sistema gali užkardyti galimus pavojus elektroninėje erdvėje. Prie to turėtų prisidėti valdžios institucijos palaikydamos ir skatindamos iniciatyvas susijusias su kibernetiniu saugumu, dalintis patirtimi su kitomis šalimis, turi būti tinkamai veikianti vidinė teisinė bazė, kuri numatytų kontrolės ir užkardymo priemones. Šalyje turi būti veikiančios institucijos užtikrinančios operatorių ir kitų veikėjų veikiančių internetinėje erdvėje kontrolę. Siekiant sėkmingai plėtoti kibernetinio saugumo kultūrą, tai turi būti daroma per mokymo prizmę, pedagogams suteikiant reikiamų kompetencijų, kurias jie tinkamai galėtų perduoti mokiniams.

5. Siekiant užtikrinti kibernetinio saugumo mokymą mokyklų vadovybė turi palaikyti ir skatinti šį dalyką įtraukti į visų dalykų pamokas, todėl atsakomybė tenka ne tik informacinių technologijų mokytojams. Mokytojai turėtų būti kvalifikuoti ir turėti tinkamus skaitmeninio raštingumo įgūdžius, kuriuos tinkamai perduotų besimokantiesiems. Pedagogo kvalifikaciją turėtų

sudaryti vidiniai veiksniai, kurie apimtų jo asmeninius sugebėjimus ir supratimą, bei išoriniai veiksniai, kurie padėtų stiprinti profesines ir dalykines kompetencijas.

6. Šalys kibernetinio saugumo mokymą savo viduje organizuojasi skirtingai, tam įtakos turi politinė sistema, ekonominė padėtis ir švietimo organizavimas. Jungtinės Amerikos Valstijos, turėdamos daug iniciatyvų ir kuriamų programų, susiduria su skirtingų valstijų politika ir programų ar iniciatyvų palaikymu plėtojant kibernetinio saugumo kultūrą šalyje, todėl nėra vienodo priėjimo prie mokymo. Latvijoje reikalingos švietimo reformos, kurios sujungtų specialistus ir valdžios institucijas siekiant kelti mokytojų kvalifikaciją ir paruošiant juos, jog būtų tinkamai mokomi mokiniai. Vienas iš geriausiai veikiančių pavyzdžių, kaip turėtų būti plėtojama skaitmeninis raštingumas yra Estija. Šalyje yra didelis valdžios ir mokslo institucijų įsitraukimas, bei mokytojų įtraukimas į tobulinimo ir kūrimo procesą siekiant tinkamai plėtoti kibernetinį saugumą.

7. Lietuvoje yra sukurta teisinė sistema, tačiau ji veikia tik iš dalies. Dauguma mokytojų neturi tinkamų skaitmeninio raštingumo įgūdžių, o kvalifikacijos tobulino kursuose dalyvauja pasirinktinai. Mokyklose, kaip patvirtina mokyklų atstovai ir mokiniai, su kibernetiniu saugumu susijusios temos yra dėstomos daugiausia tik informacinių technologijų pamokose, kas yra nurodyta pagal sudarytas mokymo programas, o papildomi projektai yra vykdomi mokyklų ar mokytojų iniciatyva, kas lemia mažą mokinių įsitraukimą.

8. Mokiniai yra aktyvūs kibernetinės erdvės naudotojai ir aktyvūs socialiniuose tinkluose, nors didelė dalis supranta kas yra internetinėje erdvėje slypinčios grėsmės, dalis vis tiek nėra atsargūs valdydami savo duomenis ir nežino kaip tinkamai reikėtų reaguoti į grėsmes. Dauguma mokinių pritaria, jog jiems yra reikalingas kibernetinio saugumo mokymas, kuris praplėstų jų žinias ir žinojimą, kaip tinkamai elgtis ir būtų ugdoma jų kibernetinė higiena, bei formuotųsi tinkama kultūra.

REKOMENDACIJOS

1. Švietimo mokslo ir sporto ministerijai įvesti mokytojams metinį skaitmeninio raštingumo testavimą, siekiant įvertinti skaitmeninės kompetencijos pagal Europos Sąjungos skaitmeninių kompetencijų sistemos numatytą lygmenį siekiant atrasti trūkstamas kompetencijas, bei sudaryti kvalifikacijos kėlimo planą, jog būtų pasiektas tinkamas lygmuo ir mokytojas jaustųsi komfortiškai taikydamas skaitmenines technologijas mokymosi procese, bei suteikdamas informaciją mokiniams kaip tinkamai elgtis kibernetinėje erdvėje. Pirmasis mokytojų įvertinimo etapas turėtų būti informacinių technologijų mokytojams, kurie tiesiogiai yra susiję su kompiuterinių technologijų mokymu. Antrasis rekomenduotinas etapas turėtų būti visų likusiu mokytojų vertinimas, siekiant nustatyti skaitmeninio raštingumo lygį ir padėti jiems tobulinti savo įgūdžius skaitmeniniame raštingume ir kibernetinės kultūros vystyme.

2. Visi mokytojai, nepriklausomai nuo jų mokomos srities privalo nuolatos tobulinti savo skaitmeninį raštingumą mokydamiesi patys, spręsdami iškylančias problemas mokyklose ir identifikuotus pastebėjimus ar išmoktas pamokas dalindamiesi su savo mokyklos bendruomene ar dalindamiesi gerąja patirtimi su kitomis mokyklomis. Švietimo mokslo ir sporto ministerija ir mokyklos turi užtikrinti pedagogų švietimą ir nusimatyti periodinį kibernetinio saugumo žinių atnaujinimą.

3. Vykdant švietimo reformas ir pokyčius mokytojų kompetencijos turėtų būti nuosekliai peržiūrimos, jog jų kvalifikacija atitiktų naujausias tendencijas ir būtų teikiama aktuali informacija mokiniams.

4. Švietimo mokslo ir sporto ministerijai rekomenduojama sudaryti aukštųjų mokymo institucijų, susijusių su kibernetiniu saugumu, specialistų ir mokytojų darbo grupę siekiant kurti inovacijas skaitmeninio raštingumo mokymo tobulinimo srityje, skatinti juos dalintis gerąja patirtimi ir spręsti iškilusias problemas. Sudaryti visų lygių švietimo atstovams galimybes siūlyti iniciatyvas iš jų perspektyvos, nes dirbdami su vaikais, jie yra vieninteliai, kurie mato realią situaciją, koks yra kibernetinio saugumo kultūros lygmuo jaunų žmonių tarpe.

5. Švietimo mokslo ir sporto ministerijai rengiant bendrojo ugdymo programas ir gaires (rekomendacijas), daugiau dėmesio skirti tiksliai išskiriant kibernetinio švietimo kultūros esmines kryptis ir užduotis atsižvelgiant į poreikį vystyti mokinių skaitmeninį raštingumą, saugų elgesį socialiniuose tinkluose, bei stiprinti technines žinias ir ugdyti kritinį mąstymą.

6. Mokykloms stiprinti bendradarbiavimą su privačiuoju sektoriumi ir didžiosiomis informacinių technologijų kompanijomis, bei kibernetinio saugumo specialistais siekiant ugdyti

informacinių technologijų ir skaitmeninio raštingumo kompetencijas mokinių tarpe, mokinant juos su šiuolaikinius poreikius atitinkančiomis programomis ir užduotimis.

7. Mokykloms įtraukti tėvus į kibernetinio saugumo kultūros ugdymą teikiant rekomendacijas kaip bendrauti su vaikais ir gauti grįžtamąjį ryšį, kuomet jie naudojasi elektronine erdve, kaip apsaugoti vaikus skaitmeninėje erdvėje, kokius saugumo nustatymus jie turėtų nusimatyti, bei supažindinti tėvus kaip jie galėtų kelti savo skaitmeninio raštingumo kompetencijas.

LITERATŪRA

1. Aiken. G. M. (2019). Cybersecurity and productivity: has a cybersecurity culture gone too far?'' *ASBBS Proceedings,* 26(2), 13-22, Prieiga per internetą: https://www.proquest.com/openview/d0b2ea6de6bfa532593821326e913495/1?pq-origsite=gscholar&cbl=2030636;

2. Alnatheer, M. A. (2014). A Conceptual Model to Understand Information Security Culture. *International Journal of Social Science and Humanity*, 4(2), 104-107. Prieiga per internetą: https://www.researchgate.net/publication/271295163_A_Conceptual_Model_to_Understand_Information_Security_Culture;

3. Ani, U. D., He, H. ir Tiwari, A. (2018). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology,* 21(9), 1-34. Prieiga per internetą: 10.1108/JSIT-02-2018-0028;

4. Aronovich, A. (2018). *Why Educating Your Employees on Cyber Intelligence And Security Will Reduce Risk*. Prieiga per internetą: https://www.cybintsolutions.com/employee-education-reduces-risk/;

5. Aru-Chabilan, H. (2020).Tiger Leap for digital turn in the Estonian education. *Educational media international*. 57(1), 61–72. Prieiga per internetą: https://doi.org/10.1080/09523987.2020.174485;

6. Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T. ir Shadbolt, N. (2018). Third part tracking in the mobile ecosystem. *Computers and Society*, 1-9. Prieiga per internetą: https://arxiv.org/abs/1804.03603

7. Broks, A. (2021). *Digital illiteracy looming over Latvia: here's how progressive IT companies can help*. Prieiga per internetą: https://blog.twino.eu/digital-illiteracy-looming-over-latvia-heres-how-progressive-it-companies-can-help/;

8. Čiapienė, G. (2021). *Idėjos ugdymui: kaip atskleisti saugesnio interneto temas*. Prieiga per internetą: https://www.nsa.smm.lt/2021/01/04/idejos-ugdymui-kaip-atskleisti-saugesnio-interneto-temas/;

9. Cross, M. (2014). *Social media security: Laveraging social network while mitigating risk*. Rockland: Sungress. Prieiga per internetą: https://web-p-ebscohost-com.skaitykla.mruni.eu/ehost/detail/detail?vid=14&sid=4777f5fa-a69c-47b1-a063-36064c24b85f%40redis&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=486636&db=e000xww;

10. da Veiga, A. (2016). Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument. *SAI Computing Conference*, 1006-1015. Prieiga per internetą: 10.1109/SAI.2016.7556102;

11. da Veiga, A., Astakhova, L. V., Botha, A. ir Herselman, M. (2020). Defining organisational information security culture – Perspectives from academia and industry. *Computers & Security*, 1-52. Prieiga per internetą: https://doi.org/10.1016/j.cose.2020.101713;

12. Dean, B. (2021). *Social Network Usage & Growth Statistics: How Many People Use Social Media in 2021?*. Prieiga per internetą: https://backlinko.com/social-media-users#social-media-usage-stats;

13. DiComp. (2021). *Educators – DigCompEdu.* Prieiga per internetą: http://www.digcomptest.eu/index.php?pg=quadro

14. Dobrinoiu, M. (2017). Need for Education on Cybersecurity. *Int'l J. Info. Sec. & Cybercrime*, 25, 25-32. Prieiga per internetą: https://heinonline.org/HOL/LandingPage?handle=hein.journals/ijisc6&div=7&id=&page=;

15. Enescu, S. (2019). The concept of cybersecurity culture. *International Scientific Conference "Strategies XXI"*, 176-183. Prieiga per internetą: https://www.proquest.com/openview/417f00c36521a0471400cf3aac4d9ef3/1.pdf?pq-origsite=gscholar&cbl=2026346;

16. European Commission. (2017). *European Framework for the Digital Competence of Educators (DigCompEdu). Assessing Educators' Digital Competence*. Prieiga per internetą: https://ec.europa.eu/jrc/sites/default/files/digcompedu_leaflet_en-2017-11-14.pdf;

17. European Union Agency for Network and Information Security (ENISA). (2017). *Cyber Security Culture in organisations.* Prieiga per internetą: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations;;

18. Europos komisijos komunikatas Europos Parlamentui, Tarybai, Europos Ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. 2021–2027 m. skaitmeninio švietimo veiksmų planas Švietimo ir mokymo pritaikymas prie skaitmeninio amžiaus, *Eur-Lex*. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52020DC0624;

19. Flick, U. (2014). *The SAGE Handbook of Qualitative Data Analysis*. SAGE. Prieiga per internetą: https://dx-doi-org.skaitykla.mruni.eu/10.4135/9781446282243.n6;;

20. Frey, B. B. (2018). *The SAGE Encyclopedia of Educational Research, Measurement, and Evaluation*. SAGE. Prieiga per internetą: https://dx-doi-org.skaitykla.mruni.eu/10.4135/9781506326139;

21. Gaižauskienė, I. ir Mikienė, S. (2014). *Socialinių tyrimų metodai: apklausa*. Vilnius: Mykolo Romerio universitetas;

22. Gcaza, N. ir von Solms, R. (2017). Cybersecurity culture: An Ill-defined Problem. *Conference: IFIP World Conference on Information Security Education,* 98-109. Prieiga per internetą: https://www.researchgate.net/publication/316713566_Cybersecurity_Culture_An_Ill-Defined_Problem;

23. Gegenheimer, S., Rubinstein, J., Azoulay, A., Bogdan-Martin, D., Ba, B., Lee, Y., Cichy, M., Ekholm, B., Georgieva, K., Granryd, M., Jarque, C. M., Kidron, B. B., Lovett, A., Al Mansoori, H. O., Martin, K., Mitchell, P., Mittal, S. B., Ndege, S., O'Brien, D., Al Ruwais, A. B. S. ir Yafang, S. (2019). Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online. *Broadband Commission*. Prieiga per internetą: https://www.broadbandcommission.org/publication/child-online-safety/;

24. Gimenez, A. M., Luengo J. A. ir Bartrina J. (2017). What are young people doing on Internet? Use of ICT, parental supervision strategies and exposure to risks. *Electronic Journal of Research in Educational Psychology*, 15(3), 533-552. Prieiga per internetą: 10.14204/ejrep.43.16123;

25. Google support (2021). *Age-restricted content*. Prieiga per internetą: https://support.google.com/youtube/answer/2802167?hl=en#zippy=%2Cmonetization-and-age-restrictions;

26. Governance Experts Measure Culture, Cybersecurity Strategy, and ESG (2019). *NACD Directorship,* 45(5), 49-51. Prieiga per internetą: https://web-p-ebscohost-com.skaitykla.mruni.eu/ehost/detail/detail?vid=7&sid=4777f5fa-a69c-47b1-a063-36064c24b85f%40redis&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=138678897&db=f5h;);

27. Hattingh, M. (2021). *The Dark Side of YouTube: A Systematic Review of Literature*. Adolescences. Prieiga per internetą: 10.5772/intechopen.99960;

28. Hindsa, J., Williamsb, E. J. ir Joinson, A. N. (2020). It wouldn't happen to me" : Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies,* 143, 1-14. Prieiga per internetą: https://www-sciencedirect-com.skaitykla.mruni.eu/science/article/pii/S1071581920301002;

29. Informatiko ugdymo paskirtis https://nsasmm-my.sharepoint.com/personal/cezary_taraskievic_nsa_smm_lt/_layouts/15/Doc.aspx?sourcedoc={9fc59f1d-f246-4b67-aac5-ed94d1998ade}&action=view&wd=target%281.%20Informatikos%20ugdymo%20paskirtis.one%7Cc2a9b4bc-5967-494f-8a20-4bfc89397589%2F1.%20Informatikos%20ugdymo%20paskirtis%7C365252cd-a302-4aa3-be81-2e7f1fe8eec8%2F%29;

30. *Informative Statement. Cybersecurity of Latvia 2019-2022* (2019). Prieiga per internetą: https://www.mod.gov.lv/sites/mod/files/document/Cybersecurity%20Strategy%20of%20Latvia%202019_2022.pdf;

31. International Review of the Red Cross (2020) Interview with Prime Minister Jüri Ratas of Estonia. *Digital technologies an war,* 102(913), 1-7. Prieiga per internetą: https://doi.org/10.1017/S181638312000034X;

32. ITU (2021). *Global Cybersecurity Index 2010.* Prieiga per internetą: https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/

33. Johnson, J. (2021). *Internet penetration rate worldwide 2021, by region.* Prieiga per internetą: https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/;

34. Johnson, J. (2021). *Worldwide digital population as of January 2021*. Prieiga per internetą: https://www.statista.com/statistics/617136/digital-population-worldwide/;

35. Jungtinių tautų Generalinės asamblėjos 2003 m. sausio 31 d. rezoliucija 57/239. *Creation of a global culture of cybersecurity.* Prieiga per internetą: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf;

36. Kardelis, K. (2016) *Mokslinių tyrimų metodologija ir metodai*. Mokslo ir enciklopedijų leidybos centras;

37. Katz, F. H. (2018). Breadth vs. Depth: Best Practices Teaching Cybersecurity in a Small Public University Sharing Models. *The Cyber Defense Review* , 3(2), 65-71. Prieiga per internetą: https://www.jstor.org/stable/26491224;

38. Kemp, S. (2021). *Digital 2021: Estonia data reportal.* Prieiga per internetą: https://datareportal.com/reports/digital-2021-estonia?rq=estonia;

39. Kemp, S. (2021). *Digital 2021: Latvia data reportal.* Prieiga per internetą: https://datareportal.com/reports/digital-2021-latvia;

40. Kemp, S. (2021). *Digital 2021: Lithuania data reportal.* Prieiga per internetą: https://datareportal.com/reports/digital-2021-lithuania?rq=lithuania;

41. Lewis, J. A. (2016). Advanced Experiences in Cybersecurity Policies and Practices. An Overview of Estonia, Israel, South Korea, and the United States. *IDB-DP*-457, 1-62. Prieiga per internetą: https://publications.iadb.org/en/advanced-experiences-cybersecurity-policies-and-practices-overview-estonia-israel-south-korea-and;

42. *Lietuvos Respublikos Seimo 2018 m. birželio 27 d. įstatymas Nr. XIII-1299 „Lietuvos Respublikos Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas.* Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/15e540727ac211e89188e16a6495e98c;

43. *Lietuvos Respublikos Švietimo ir mokslo Ministro 2018 m. birželio 25 d. įsakymas Nr. V-598 „Dėl Švietimo ir mokslo ministro 2007 m. kovo 29 d. įsakymo Nr. ISAK-555 „Dėl reikalavimų*

mokytojų kompiuterinio raštingumo programoms patvirtinimo‘‘ pakeitimo. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/599d489078af11e89188e16a6495e98c?jfwid=q8i88m58y2;

44. *Lietuvos Respublikos Švietimo įstatymas*. (1991). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.1480/asr;

45. *Lietuvos Respublikos Švietimo, mokslo ir sporto ministro 2021 m. rugpjūčio 6 d. įsakymas Nr. V-1468 ,,Dėl švietimo, mokslo ir sporto ministro 2019 m. lapkričio 18 d. įsakymo Nr. V-1317 ,,Dėl bendrųjų programų atnaujinimo gairių patvirtinimo‘‘ pakeitimo‘‘*. Prieiga per internetą: https://www.smm.lt/uploads/lawacts/docs/3107_d412c146;0a217d7572efcd4e86d1d5c3.pdf;

46. *Lietuvos Vyriausybės nutarimas dėl Lietuvos Respublikos Kibernetinio saugumo įstatymo įgyvendinimo, 2018 m. rugpjūčio 13 d. Nr. 818 (Galiojanti suvestinė redakcija nuo 2021 m. sausio 1 d.).* Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr;

47. LKŽ. *Kultūra.* Prieiga per internetą: http://www.lkz.lt/?zodis=kult%C5%ABra&lns=-1&les=-1&id=17246460000;

48. Loishyn, A. A., Hohoniants, S., Ya.Tkach, M., Tyshchenko, M. H., Tarasenko, N. M. ir Kyvliuk, V. S. (2021). Development of the Concept of Cybersecurity of the Organization. *EM Journal*, 10(3), 1447-1453. Prieiga per internetą: https://web-s-ebscohost-com.skaitykla.mruni.eu/ehost/pdfviewer/pdfviewer?vid=0&sid=5f2c0de0-ba55-4687-aa41-7c4bda731cee%40redis;

49. LRT.lt (2021) Paskelbti geriausių mokyklų ir universitetų reitingai – lyderiai pozicijų neužleidžia. Prieiga per internetą: https://www.lrt.lt/naujienos/lietuvoje/2/1407118/paskelbti-geriausiu-mokyklu-ir-universitetu-reitingai-lyderiai-poziciju-neuzleidzia;

50. Martellozzo, E., Monaghan, A., Davidson, J. ir Adler, J. (2020). Reaserching the Affects That Online Pornography Has on U.K. Adolscents Aged 11 to 16. *Research Article*, 1-15. Prieiga per internetą: https://doi-org.skaitykla.mruni.eu/10.1177/2158244019899462;

51. Miguel, C. S., Morales, K. ir Ynalve, M. A. (2020). Online Victimization, Social Media utilization and Cyber crime prevention measures. *Asia-Pacific Social Science Review,* 20(4), 123-135. Prieiga per internetą: http://apssr.com/volume-20-no-4/online-victimization-social-media-utilization-and-cyber-crime-prevention-measures/;

52. *Ministru kabineta noteikumi Nr. 416 Noteikumi par valsts vispārējās vidējās izglītības standartu un vispārējās vidējās izglītības programmu paraugiem*, Prieiga per internetą: https://likumi.lv/ta/id/309597;

53. Mishra, L., Gupta, T. ir Sheree, A. (2020). Online teaching-learning in higher education during lockdown period of COVID-19 pandemic. *International Journal of Educational Research*, 1, 1-8. Prieiga per internetą: https://doi.org/10.1016/j.ijedro.2020.100012;

54. NACD Directorship (2019). Leading Minds of Governance ,, Governance Experts Measure Culture, Cybersecurity Strategy, and ESG. *NACD Directorship*, 45(5), 49-50. Prieiga per internetą: https://web-p-ebscohost-com.skaitykla.mruni.eu/ehost/detail/detail?vid=4&sid=0c03a4e3-eaf4-48e8-a96b-2ae2873921c5%40redis&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=138678897&db=f5h;

55. National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity version 1.1*. Prieiga per internetą: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf;

56. Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya S. ir Hancock G. M. (2020). Holistic cyber hygene education: Accounting for the human factors, *Computers & Security*, 92: 1-6. Prieiga per internetą: https://doi.org/10.1016/j.cose.2020.101731;

57. Ofcom. (2021). *Ofcom Children and parents: Media use and attitudes report.* Prieiga per internetą: https://www.ofcom.org.uk/__data/assets/pdf_file/0025/217825/children-and-parents-media-use-and-attitudes-report-2020-21.pdf;

58. *Par mums*. Prieiga per internetą: https://drossinternets.lv/lv/info/par-mums;

59. Pătrașcu, P. (2019). Promoting Cyber Culture through Education. *The International Scientific Conference eLearning and Software for Education*, 2, 273-279. Prieiga per internetą: https://www.proquest.com/openview/8887f8408411a1f3a6069ccb4532c2f3/1?pq-origsite=gscholar&cbl=1876338;

60. Paul, C. ir PorcheI. R. (2012). Toward a U.S. Army Cyber Security Culture. *International Journal of Cyber Warfare & Terrorism*, 1(3), 70-80. Prieiga per internetą: 10.4018/ijcwt.2011070105;

61. Paul, F. (2020). *Why build a cybersecurity culture?*. Prieiga per internetą: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/why-build-a-cybersecurity-culture;

62. Paziuk, A. ir Mitsik, V, (2019). Global cybersecurity culture in the international disclosure: values and principles. *National Academy of Managerial Staff of Culture and Arts Herald*, 2, 103-107. Prieiga per internetą: 10.32461/2226-3209.2.2019.175488;

63. Presthus, W. ir Vatne, D. M. (2019). A Survey on Facebook Users and Information Privacy. *Procedia Computer Science*, 164, 39-47. Prieiga per internetą: https://www-sciencedirect-com.skaitykla.mruni.eu/science/article/pii/S187705091932191X;

64. Ragab D. (2019). Teaching digital citizens in today's world: Research and insights behind the Common Sense K–12 Digital Citizenship Curriculum. *San Francisco, CA: Common Sense Media*. 1-

59. Prieiga per internetą: https://www.researchgate.net/publication/337447543_Teaching_Digital_Citizens_in_Today%27s_World_Research_and_Insights_Behind_the_Common_Sense_K-12_Digital_Citizenship_Curriculum;

65. Reilly, C. A. (2021). Reading risk: Preparing students to develop critical digital literacies and advocate for privacy in digital spaces. *Computers and Composition*. 61, 1-13. Prieiga per internetą: https://www-sciencedirect-com.skaitykla.mruni.eu/science/article/pii/S8755461521000293;

66. Sarokin, D. (2019). *5 Components of Multimedia.* Prieiga per internetą: https://smallbusiness.chron.com/5-components-multimedia-28279.html;

67. Schwartz, S. (2018). Schools Teach ‚cyber hyhiene' to compat phishing, identity theft. *Education Digest*, 84(1), 4-8. Prieiga per internetą: https://web-s-ebscohost-com.skaitykla.mruni.eu/ehost/detail/detail?vid=6&sid=2d26468f-4615-4c0d-b0a4-b9bda9c58ce7%40redis&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=131039568&db=trh;

68. Šimandl, V. ir Vaníček, J. (2017). Influences on ICT teachers knowledge and routines in technical e-safety context. *Telematics and Informatics*, 34, 1488-1502. Prieiga per internetą: https://www-sciencedirect-com.skaitykla.mruni.eu/science/article/pii/S0736585317301806;

69. Tierney, W. G., Corwin, Z. B. ir Ochsner, A. (2018). *Diversifying Digital Learning: Online Literacy and Educational Opportunity*. Baltimore : Johns Hopkins University Press. Prieiga per internetą: https://web-p-ebscohost-com.skaitykla.mruni.eu/ehost/detail/detail?vid=4&sid=b0e43ae8-0dda-4cfe-a648-b3b5253283e0%40redis&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=1619068&db=e000xww;

70. Tomczy, L. (2019). What Do teachers Know About Digital Safety?. *Computers in the Schools*, 3(36): 167-187. Prieiga per internetą: https://www.researchgate.net/publication/335134277_What_Do_Teachers_Know_About_Digital_Safety;

71. Trum White House (2018). *President Trump Unveils America's First Cybersecurity Strategy in 15 Years Trump white house*. Prieiga per internetą: https://trumpwhitehouse.archives.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/;

72. Tziarras, Z. (2014).The Security Culture of Global and Multileveled Cybersecurity. *Cyber-Development, Cyber-Democracy and Cyber-Defense. Challenges, Opportunities and Implications for Theory, Policy and Practice,* Chapter 13, 319-335. Prieiga per internetą: https://www.researchgate.net/publication/261986826_The_Security_Culture_of_a_Global_and_Multileveled_Cyber_Security;

73. Valmane, L., Zariņa, S., Badjanov, J., Iliško, D. ir Petrova, M. (2020). Empowering digital and media literacy of primary school teachers in Latvia. *12th International Conference on Education and New Learning Technologies*, 4022-4029. Prieiga per internetą: https://www.researchgate.net/publication/343421342_EMPOWERING_DIGITAL_AND_MEDIA_LITERACY_OF_PRIMARY_SCHOOL_TEACHERS_IN_LATVIA;

74. Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G. ir Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, 128, 1-11. Prieiga per internetą: https://doi.org/10.1016/j.dss.2019.113160;

75. von Solms, R. ir van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102. Prieiga per internetą: https://www-sciencedirect-com.skaitykla.mruni.eu/science/article/pii/S0167404813000801.

Valavičiūtė R. (2021). *Kibernetinio saugumo kultūros vystymas Lietuvos bendrojo ugdymo mokyklose* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas.

ANOTACIJA

Magistro baigiamajame darbe išanalizuota kibernetinio saugumo kultūros vystymo reikalingumas siekiant ugdyti mokinių tinkamą elgesį skaitmeninėje erdvėje. Pirmame skyriuje nagrinėjama kibernetinio saugumo kultūros samprata ir esminiai bruožai. Antrame skyriuje yra nagrinėjama kibernetinio saugumo kultūros teorinis konceptas, apžvelgiamos skaitmeninėje erdvėje dažniausiai kylančios rizikos, su kuriomis dažniausiai gali susidurti vartotojai. Nagrinėjama kibernetinio saugumo ekosistema ir kokią naudą duoda tinkama kibernetinė higiena, koks turėtų būti mokytojų ir tėvų įsitraukimas į ugdymą. Skyriuje apžvelgiamos kitų šalių praktikos vystant kibernetinio saugumo kultūrą ugdymo įstaigose. Trečiame skyriuje pateikiami kokybinis ir kiekybinis tyrimai. Kokybiniu tyrimu atskleidžiama koks yra mokyklų įsitraukimas į mokytojų kvalifikacijos kėlimą susijusį su kibernetiniu saugumu ir kaip yra vykdomas mokymas bei kultūros plėtra. Kiekybiniu tyrimu atskleidžiami mokinių dalyvavimo elektroninėje erdvėje ypatumai, rizikos suvokimas ir koks jų požiūris į mokykloje vykdomą kibernetinio saugumo mokymą. Skyriuje pateikiamos tyrimų išvados ir apibrėžiamos esminės problemos, kurios daro įtaką siekiant tinkamai plėtoti kibernetinę saugumo kultūrą bendrojo ugdymo mokyklose.

Pagrindiniai žodžiai: kibernetinio saugumo kultūra, kibernetinio saugumo mokymas, skaitmeninio raštingumo vystymas.

Valavičiūtė R. (2021). *Development of cybersecurity culture in the Lithuanian general education schools* (master thesis). Vilnius: Mykolas Romeris University.

ANNOTATION

Master‘s thesis analyses necessity of cybersecurity culture in order to foster an appropriate behaviour of school children in the cybernetic space. Chapter 1 looks into the understanding of cybersecurity culture and most common features. Chapter 2 delves into the theoretical concept of cybersecurity culture, goes through most common risks encountered by the users in the cyber space. It also explores the ecosystem of cybersecurity and what benefits cyber hygiene gives as well as the role of parents and teachers in the education. Chapter overviews best practises of other countries in implementing cybersecurity culture in learning institutions. Chapter 3 provides research in quality and quantity. Quality research displays schools‘ involvement in exceling connected with cybersecurity and how training and spreading of this culture is implemented. Quantity research shows peculiarities of student’s presence in the cyberspace, understanding of risks and approach to cybersecurity training in schools. Chapter provides findings of research and defines critical issues that influence appropriate development of cybersecurity culture in general education schools.

Key words: cybersecurity culture, cybersecurity education, development of digital literacy.

Valavičiūtė R. (2021). *Kibernetinio saugumo kultūros vystymas Lietuvos bendrojo ugdymo mokyklose* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas.

SANTRAUKA

Kibernetinio saugumo kultūros ugdymo magistro baigiamojo darbo tema yra aktuali Švietimo mokslo ir sporto ministerijai, mokykloms, mokytojams ir tėvams, siekiant ugdyti mokinius, kaip atsakingus skaitmeninės erdvės vartotojus. Daugelis mokslininkų kibernetinę saugumo kultūrą apibrėžia kaip būtiną ugdyti aspektą šių dienų pasaulyje. Kibernetinė saugumo kultūra vis dar yra ganėtinai naujas objektas, kurio mokymo sistema yra labai skirtingai suprantama, todėl buvo iškelta pagrindinė darbo problema – kaip galėtų būti tobulinama Kibernetinio saugumo kultūra bendrojo ugdymo mokyklose? Darbo objektas. Kibernetinio saugumo kultūros vystymas Lietuvos bendrojo ugdymo mokyklose. Šio darbo tikslas teoriškai ir empiriškai ištirti kibernetinio saugumo kultūros vystymą Lietuvos bendrojo ugdymo mokyklose. Darbo uždaviniai: išnagrinėti kibernetinio saugumo kultūros sampratą, pateikti kibernetinio saugumo kultūros teorinį konceptą, išanalizuoti užsienio šalių patirtį, plėtojant kibernetinio saugumo kultūrą, atlikti tyrimą siekiant identifikuoti kibernetinio saugumo kultūros tobulinimo galimybes Lietuvoje. Darbo metodai: mokslinės literatūros analizė, lyginamoji literatūros analizė, duomenų vizualizacija, kokybinė turinio analizė, kiekybinė turinio analizė.

Empirinio tyrimo metu buvo iškelta hipotezė: Lietuvos bendrojo ugdymo mokyklose nepakankamai dėmesio skiriama į mokinių kibernetinio saugumo kultūros ugdymą. Atlikus kokybinį ir kiekybinį tyrimus ši hipotezė buvo patvirtinta. Mokyklose mokytojai susiduria su skaitmeninio raštingumo trūkumu, kas daro įtaką mokymui, taip pat mokyklos neturi vienos sistemos, kuri užtikrintų kokybišką mokymą ir stiprintų mokinių gebėjimus. Mokiniai būdami aktyvūs skaitmeninės erdvės vartotojai susiduria paradoksu, kuomet suvokdami grėsmes vis tiek naudojasi internetu neįvertindami rizikos. Pagrindiniai aspektai padedantys stiprinti kibernetinį saugumą siekiant išvengti žmogiškųjų klaidų ugdant mokinius yra mokytojų kompetencijų stiprinimas, tėvų įtraukimas ir kritinio mąstymo ugdymas, kuris padėtų suformuoti jaunų žmonių tinkamą elgesį skaitmeninėje erdvėje.

Magistro baigiamojo darbo pabaigoje pateikiamos išvados bei siūlymai dėl kibernetinio saugumo kultūros tobulinimo bendrojo ugdymo mokyklose.

Valavičiūtė R. (2021). *Development of cybersecurity culture in the Lithuanian general education schools* (master thesis). Vilnius: Mykolas Romeris University.

SUMMARY

Topic of the master‘s cybersecurity culture development is relevant to the Ministry of education, science and sport, schools, teachers and parents in order to educate students as responsible users of the cyber space. A few scientists define cybersecurity culture as a crucial aspect of education in the modern world. Cybersecurity remains a fairly new subject with its teaching system interpreted differently, therefore the main proposition of the thesis – how could cybersecurity culture be improved in public schools. Object of the thesis: Development of cybersecurity culture in the Lithuanian general education schools. Objective of the thesis: Theoretical and empirical research of development of cybersecurity culture in the Lithuanian general education schools. Tasks: look into concept of cybersecurity culture, provide theoretical philosophy of cybersecurity culture, analyse experience of foreign countries in developing cybersecurity culture, conduct research in order to identify opportunities for excellence of developing cybersecurity culture in Lithuania. Methods of thesis: analysis of scientific literature, comparative analysis of literature, visualization of data, qualitative analysis, quantitative analysis.

During the empirical research a hypothesis was presented: Lithuanian public schools pay not enough attention to cybersecurity education of students. Qualitative and quantitative research confirmed this hypothesis. Teachers in schools face lack of cyber literacy which in turn negatively impacts teaching. Also, schools lack a unified system to strengthen abilities of students. Being active participants in the cyber space face a paradox when they understand the threats without understanding the risks. Main aspects in avoiding human error in strengthening cybersecurity culture are improving competences of teachers, participation of parents and development of critical thinking which in turn would help to form an appropriate behaviour of youth in the cyber space.

Ending of the master’s thesis provides conclusions and motions in regards of excelling cybersecurity culture in the general education schools.

PRIEDAI

1 priedas

KIEKYBINIO TYRIMO KLAUSIMYNAS

Laba diena,

Esu Mykolo Romerio universiteto, viešojo valdymo ir verslo fakulteto, Kibernetinio saugumo valdymo magistro studijų studentė – Rūta Valavičiūtė. Magistro baigiamajame darbe atlieku tyrimą ir kviečiu Jus dalyvauti apklausoje, skirtoje išsiaiškinti Jūsų supratimą apie skaitmeninį saugumą elektroninėje erdvėje. Tik Jūsų atsakymų dėka pavyks gauti objektyvius tyrimo rezultatus, kurie padės identifikuoti problemas ir prisidėti prie kokybiškesnio kibernetinio saugumo kultūros vystymo bendrojo ugdymo mokyklose.

Maloniai prašau atsakyti į visus anketos klausimus.

Apklausa anoniminė, todėl užtikrinu Jūsų atsakymų anonimiškumą (rezultatai bus panaudoti tik apibendrintai).

Jūsų amžius	Jūsų lytis:
□ 8 – 10 m.; □ 11 – 13 m.; □ 14 – 16 m.; □ 17 – 19 m.	□ Vyr. □ Mot.
Gyvenamoji vieta	
□ Didmiestis; □ Miesto rajonas □ Miestas; □ Kaimas.	

1. Ar turite savo asmeninį išmanųjį telefoną kuriuo naudojatės?

□ Taip, turiu;

□ Ne, neturiu.

2. Ar naudojatės kompiuteriu?

□ Taip, naudojuosi;

□ Ne, nesinaudoju.

3. Kiek vidutiniškai valandų per dieną naudojatės internetu??

 Iki 1 valandos

 1 – 2 valandas;

 2 – 3 val;

 3 – 4 val;

 Daugiau nei 4 val.

4. Ar turite socialinio tinklo profilį (pvz. Facebook, Instagram, Tik Tok ir pan)

 Taip, turiu;

 Ne, neturiu.

5. Ar jūsų socialinių tinklų anketos yra viešos?

*Viešos anketos – anketos, kurių turinį gali peržiūrėti visi vartotojai, kurie yra ne tik draugų sąraše.

 Taip, anketos yra viešos;

 Kai kurios iš turimų anketų yra viešos;

 Ne, informacija anketose yra matomos asmenims draugų sąraše.

6. Ar socialinių tinklų platformose turite draugų, kurių nepažįstate ir nesate sutikę gyvai?

 Taip, turiu;

 Ne, neturiu;

 Taip, turiu, bet visus juos pažįstu.

7. Ar esate pastebėję/ patyrę elektroninių patyčių socialiniuose tinkluose, naudodami bendravimo platformas?

 Taip, esu patyręs (-usi);

 Taip, esu pastebėjęs (-usi), bet nesu patyręs (-usi);

 Ne, nesu patyręs (-usi).

8. Ar kada nors esate bendravę su asmeniu elektroninėje erdvėje, kurio niekada nebuvote sutikę gyvai?

 Taip, esu bendravęs (-usi);

 Ne, nesu bendravęs (-usi).

9. Kaip manote, ar elektroninėje erdvėje yra daug pavojų?

 Taip, daug;

 Ne, pavojų nėra;

 Apie tai negalvojau;

10. Kaip manote, su kokiais tinklų ir informacijos saugumo pažeidimais internete susiduriama dažniausiai? (daug galimų variantų)

- Kompiuteriniais virusais;
- Nepageidaujamais laiškais (angl. spam);
- Neteisėto ir žalingo turinio informacija (rasizmas, pornografija ir pan.)
- Informacijos ir paskyros duomenų klastojimu socialiniuose tinkluose (pateikiama melaginga, netiksli informacija);
- Įsilaužimas į asmeninį kompiuterį;
- Įsilaužimas į asmenines paskyras;
- Duomenų išviliojimas apgaulės būdu (angl. phishing);
- Nesusiduriama su jokiais saugumo pažeidimais;
- Kita – įrašykite.

11. Su kokiomis grėsmėmis Jums asmeniškai yra tekę susidurti? (daug galimų variantų)

- Susidūriau su neteisėta ir žalinga informacija internete (pvz. diskriminacinio, pornografinio, smurtinio pobūdžio informacija);
- Priekabiavimu ir patyčiomis (angl. cyberbulling);
- Buvote įžeistas virtualioje erdvėje (pvz. socialiniuose tinkluose pravardžiuojamas po paskelbtu įrašu ar nuotrauka);
- Buvau šmeižiamas elektroninėje erdvėje (pvz. buvo viešai ar pokalbių platformose paskelbta informacija apie Jus, kuri nėra tiesa);
- Susirašinėjimas su nepažįstamais asmenimis ir jų kvietimas susitikti gyvai;
- Privatumo praradimas, atskleidus asmeninius duomenis;
- Draugų pasidalinimas informacija (pvz. nuotraukomis ar įrašais), kuri susijusi su Jumis be Jūsų sutikimo;
- Neteko susidurti su jokiomis grėsmėmis;
- Kita – įrašykite.

12. Kaip elgėtės/ elgtumėtės pastebėjus patyčias, neteisėtą turinį elektroninėje erdvėje? (daug galimų variantų)

- Bandyčiau problemą išspęsti pats (pvz. rašydamas žinutes patyčių kurstytojui);
- Praneščiau tėvams/ globėjams;
- Praneščiau mokytojams;
- Skambinčiau į vaikų liniją;
- Užpildyčiau pranešimo formą „Draugiškas internetas“ platformoje;
- Nieko nedaryčiau;
- Kita – įrašykite;

13. Ar mokykloje yra mokoma skaitmeninio saugumo? (Kaip tinkamai elgtis internete, kaip susikurti ir valdyti asmeninį profilį, su kokiomis rizikomis galima susidurti internetinėje erdvėje ir kaip elgtis su jomis susidūrus)

- Taip, mokoma;
- Ne, nemokoma.

14. Kaip mokytojai padeda Jums saugiau naudotis skaitmenine erdve? (daug galimų variantų)

- Dalinasi aktualia informacija apie kibernetinius įsilaužimus;
- Kalba apie interneto poveikį, elgesį internete, neteisėtą ir žalingą turinį;
- Supažindina kokios informacijos nevertėtų skelbti internete ir kaip tai galėtų pakenkti.
- Pateikia informaciją kaip tinkamai naudotis socialiniais tinklais (kaip susikurti profilį, kaip tinkamai nusistatyti saugumo nustatymus);
- Suteikia informacijos kaip elgtis, kuomet patiriate ar pastebite patyčias elektroninėje erdvėje;
- Parodo kaip tinkamai susikurti slaptažodžius;
- Moko kaip atpažinti melagingą informaciją internete;
- Neteikia jokios informacijos susijusios su saugesniu interneto naudojimu;
- Kita – įrašykite.

15. Jeigu mokykloje vykdomas kibernetinio saugumo mokymas, kokia veikla yra vykdoma? (daug galimų variantų)

- Dalyvaujame „Saugesnio interneto savaitės renginiuose“;
- Dalyvaujame projektinėje veikloje susijusioje su interneto saugumu (pvz. piešinių konkursai, edukaciniai žaidimai saugaus interneto temomis);
- Dalyvaujame renginiuose susijusiuose su kibernetiniu saugumu;
- Dalyvaujame konferencijose susijusiose su interneto saugumu;
- Kviečiami asmenys iš kitų institucijų, kurie veda pamokas interneto saugumo temomis;
- Tokio pobūdžio veikla nevyksta;
- Kita – įrašykite.

16. Ar manote, jog būtų naudinga jog mokykloje mokytų kibernetinio saugumo, kurio metu būtų supažindinama kaip saugiai naudotis elektronine erdve?

- Taip, tai būtų naudinga;
- Ne, tai nėra reikalinga;
- Mokykloje mokoma šių dalykų.