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

LIGITA CHOCHLOVA

KIBERNETINIO SAUGUMO KULTŪROS PLĖTRA ŠVIETIMO SRITYJE: IKIMOKYKLINIO IR BENDROJO UGDYMO ĮSTAIGŲ PROGRAMŲ PAGRINDU

Vadovas:
Prof. Dr. Tadas Limba

VILNIUS
2022

TURINYS

TURINYS ... 2
LENTELIŲ SĄRAŠAS ... 3
PAVEIKSLŲ SĄRAŠAS ... 4
SANTRUMPOS ... 5
ĮVADAS ... 6
1. KIBERNETINIO SAUGUMO KULTŪROS TEORINIAI ASPEKTAI ... 9
1.1 Kibernetinės erdvės samprata ... 9
1.2 Kibernetinio saugumo ir informacinio saugumo diskursas ... 11
1.3 Kibernetinio saugumo kultūros samprata ... 15
1.4 Kibernetinio saugumo kultūros modeliai ... 19
1.5 Kibernetinio saugumo kultūros plėtros aspektai ... 21
2. KIBERNETINIO SAUGUMO KULTŪROS PLĖTROS IKIMOKYKLINIO IR BENDROJO UGDYMO ĮSTAIGŲ PROGRAMŲ PAGRINDU TYRIMAS ... 31
2.1 Empirinio tyrimo metodologija ... 31
2.2 Kokybinio tyrimo duomenų analizė ... 33
3. KIBERNETINIO SAUGUMO KULTŪROS PLĖTOJIMO VERTINIMAS UGDYMO PROGRAMOSE LYGINAMUOJU PAGRINDU ... 38
3.1 Informuotumo didinimo aspektas Kibernetinio saugumo įstatyme ... 38
3.2 Kibernetinio saugumo kultūros plėtojimas Kibernetinio saugumo strategijoje ... 41
3.3 Kibernetinio saugumo kultūros plėtojimo vertinimas ikimokyklinio ir bendrojo ugdymo programų pagrindu ... 44
IŠVADOS IR REKOMENDACIJOS ... 62
LITERATŪROS SĄRAŠAS ... 64
PRIEDAI ... 75
1. Kibernetinio saugumo požiūris mokyklose (CsA-S) klausimynas ... 75
2. Kibernetinio saugumo elgesys mokyklose (CSB-S) klausimynas ... 76
ANOTACIJA ... 77
ANNOTATION ... 78
SANTRAUKA ... 79
SUMMARY ... 80

LENTELIŲ SĄRAŠAS

1 lentelė. Kibernetinės erdvės definicijos tarptautinėse organizacijose Clarck (2010) ir Dunn (2013) kibernetinės erdvės komponentų pagrindu 11
2 lentelė. SETA programų raida 25
3 lentelė. Kibernetinio informuotumo didinimo mokyklų programose temos ir aspektai 27
4 lentelė. Kokybinio tyrimo eiga 33
5 lentelė. Institucijos ir jų funkcijos informuotumo didinimo aspektu 39
6 lentelė. Kibernetinio saugumo strategijos uždaviniai informuotumo didinimo aspektu 42
7 lentelė. Priešmokyklinio ugdymo programos informuotumo didinimo aspektas 47
8 lentelė. Jungtinės Karalystės kompiuterijos 6 - 7 metų ugdymo programa 48
9 lentelė. Saugaus elgesio pasiekimai informatikos bendrojo ugdymo projekto programoje. 51
10 lentelė. Informatikos ugdymo benrosios programos turinys informuotumo didinimo aspektu 52
11 lentelė. JK 11 -15 metų kompiuterijos ugdymo programos kibernetinio saugumo moduliai 53

PAVEIKSLŲ SĄRAŠAS

1 pav. Magistro baigiamojo darbo struktūros schema 8
2 pav. Saugumo klausimų diskursas 12
3 pav. Informacinio, IRT ir kibernetinio saugumo sąsajos 14
4 pav. Kibernetinio saugumo kultūros lygiai 18
5 pav. Huang ir Pearlson organizacinio kibernetinio saugumo modelis 19
6 pav. Georgiadou ir kt. (2020) saugumo kultūros modelis 20
7 pav. Michalos (2020) kibernetinio saugumo kultūros modelis 21
8 pav. Informacijos saugumo elgesio profiliavimo modelis 23
9 pav. Kibernetinio saugumo informuotumo didinimo metodologija mokykloms 29
10 pav. Tyrimo loginis planas 32
11 pav. Kompiuterijos ugdymo metodologija ankstyvame amžiuje. 46
12 pav. Kibernetinio saugumo informacijos sklaida švietimo pagrindu 57
13 pav. Šiuolaikinio vaiko pasaulėvoka 58
14 pav. Europos pedagogų skaitmeninių kompetencijų sistema. 60

SANTRUMPOS

IRT - informacinių ir ryšių technologijos

ES – Europos Sąjunga

IT – informacinės technologijos

JTO – Jungtinių Tautų Organizacija

ENISA - Europos Sąjungos kibernetinio saugumo agentūra

ITU - Tarptautinė telekomunikacijų sąjunga

ISO - Tarptautinė standartizacijos organizacija

OECD -Ekonominio bendradarbiavimo ir plėtros organizacijos

PPO - Tarptautinė prekybos organizacija

UNESCO – Jungtinių Tautų Švietimo, mokslo ir kultūros organizacija

ĮVADAS

Temos aktualumas. Skaitmeninimas šiuo metu yra svarbiausia technologinė tendencija įtraukianti visuomenę globaliu mastu. ITU duomenys rodo, kad pandemija skaitmenizacijos plėtros procesą dar labiau paspartino. 2019 m. internetu naudojosi 4,1 milijardo žmonių arba 54% pasaulio gyventojų. Preliminariais ITU duomenimis, vartotojų skaičius 2021 m. išaugo 782 milijonais ir pasiekė 4,9 milijardo žmonių, arba 63% visų gyventojų. Tačiau sparti informacinės visuomenės plėtra nekoreliavo su informacinių ir ryšių technologijų (IRT) kompetencijų augimu. ITU statistikos 2018 - 2020 metų duomenimis tik 4 šalių gyventojai turėjo 80-100% pagrindinių įgūdžių reikalingų IRT srityje, tuo tarpu standartinių įgūdžių intervale nuo 80 iki 100%, neturėjo nė viena šalis. Ši kompetencijų stoka tiesiogiai įtakojo kibernetinių incidentų ir atakų rizikos augimą. „Identity Force“ duomenimis, pirmąjį 2020 m. ketvirtį kibernetinių incidentų skaičius išaugo 273% lyginant su tais pačiais duomenimis 2019 m. Europos Sąjungos (ES) 2020 metais paskelbtoje „Kibernetinio Saugumo Strategijoje“ (2020) kibernetinės erdvės saugumui teikiama didžiausia reikšmė. Strategijoje pabrėžiama ES lyderystės svarba standartų, normų ir sistemų kūrimo kibernetinėje erdvėje. Ši retorika taip pat buvo pateikta ir JAV Kibernetinio Saugumo Strategijoje (2018). Kibernetinio saugumo problematika taip pat aktualizuojama moksliniuose tyrimuose, kurie pabrėžia kibernetinės erdvės ir su ja siejamų sąvokų bei procesų apibrėžties trūkumą.

Švietimo sistemos prioritetine sritimi tampa IRT integravimas į ugdymo procesus ir ugdymo programų adaptavimas siekiant eliminuoti atotrūkį tarp sparčiai besivystančių technologinių procesų ir ugdomų kompetencijų. ES pristatė „Skaitmeninio švietimo planą (2021-2027)“, kuris turi užtikrinti tvarų ir efektyvų ES valstybių narių švietimo ir mokymo sistemų pritaikymą skaitmeniniam amžiui. Plane apibrėžiamos dvi prioritetinės sritys: skatinti didelio našumo skaitmeninio švietimo ekosistemos kūrimą ir skaitmeninių įgūdžių ir kompetencijų tobulinimas skaitmeninei transformacijai. Ekonominio bendradarbiavimo ir plėtros organizacija (OECD) pristatė PISA strategiją (2021), skirtą dokumentuoti, kaip mokiniai pasiekia ir naudoja IRT išteklius mokykloje ir už jos ribų, taip pat nustatyti, kaip mokytojai, mokyklos ir švietimo sistemos integruoja IRT į pedagoginę praktiką ir mokymosi aplinką. Ypatingai polemizuojamas vaikų saugumo klausimas naudojantis IRT ir su juo siejamų įgūdžių lavinimas. Moksliniai tyrimai šia tematika yra pradinėje vystymo stadijoje ir nėra vienareikšmių ugdymo gairių kibernetinio saugumo kurso integravimui į ugdymo programas.

Temos ištirtumas ir naujumas. Kibernetinės erdvės ir kibernetinio saugumo sampratų vienareikšmės apibrėžties trūkumas aktualizuojamas naujausiuose moksliniuose tyrimuose (Malik ir Choudhury, 2019; Cainsetal, 2021; Lahsen ir kt., 2020). Taip pat, plačiai polemizuojamas informacinio ir kibernetinio saugumo terminologijų apibrėžčių ribos (Özkan, 2019; Gcaza, von Solms, ir van Vuuren, 2015; Uchendu, Nurse, Bada ir Furnell, 2021). Šios diskusijų kryptys sąlygoja ir kibernetinio saugumo

kultūros teorinio vystymo problematiką. Atliktų mokslinių tyrimų šia tematika yra labai mažai ir jie koncentruojasi, tik organizaciniame lygmenyje. Tuo tarpu sparti skaitmenizacija ir kibernetinių grėsmių progresinis augimas reikalauja kibernetinio saugumo kultūros plėtojimo individualiame lygyje. Mokslininko Tonye (2019) teigimu švietimo sistema turi pradėti diegti kibernetinio saugumo valdymo įgūdžius ugdymo programose. Lietuvoje ši tema yra aktualizuojama ir vykdomi įvairūs informuotumo didinimo projektai, tačiau atliktų mokslinių tyrimų yra nepakankamai ir tai leidžia formuluoti tyrimo problemą:

Tyrimo problema. Kaip ikimokyklinio ir bendrojo ugdymo programos plėtoja kibernetinio saugumo kultūrą Lietuvoje?

Tyrimo objektas. Kibernetinio saugumo kultūros plėtra švietimo srityje.

Tyrimo dalykas. Ikimokyklinio ir bendrojo ugdymo programos.

Tyrimo tikslas. Įvertinti kibernetinio saugumo kultūros plėtrą švietimo srityje: ikimokyklinio ir bendrojo ugdymo programų pagrindu; pateikti su šia sritimi susijusias rekomendacijas.

Darbo uždaviniai:

1. Išanalizuoti kibernetinio saugumo kultūros teorinius aspektus.
2. Atlikti kokybinį ekspertų nuomonės tyrimą, kurio pagrindu galima vertinti kibernetinio saugumo kultūros aspektą ikimokyklinio ir bendrojo ugdymo programose ir nustatyti kibernetinio saugumo kultūros plėtojimo kryptis.
3. Išanalizuoti Lietuvos ikimokyklinio ir bendrojo ugdymo programas lyginamuoju pagrindu ir pateikti programų vystymo kryptis kibernetinio saugumo srityje.

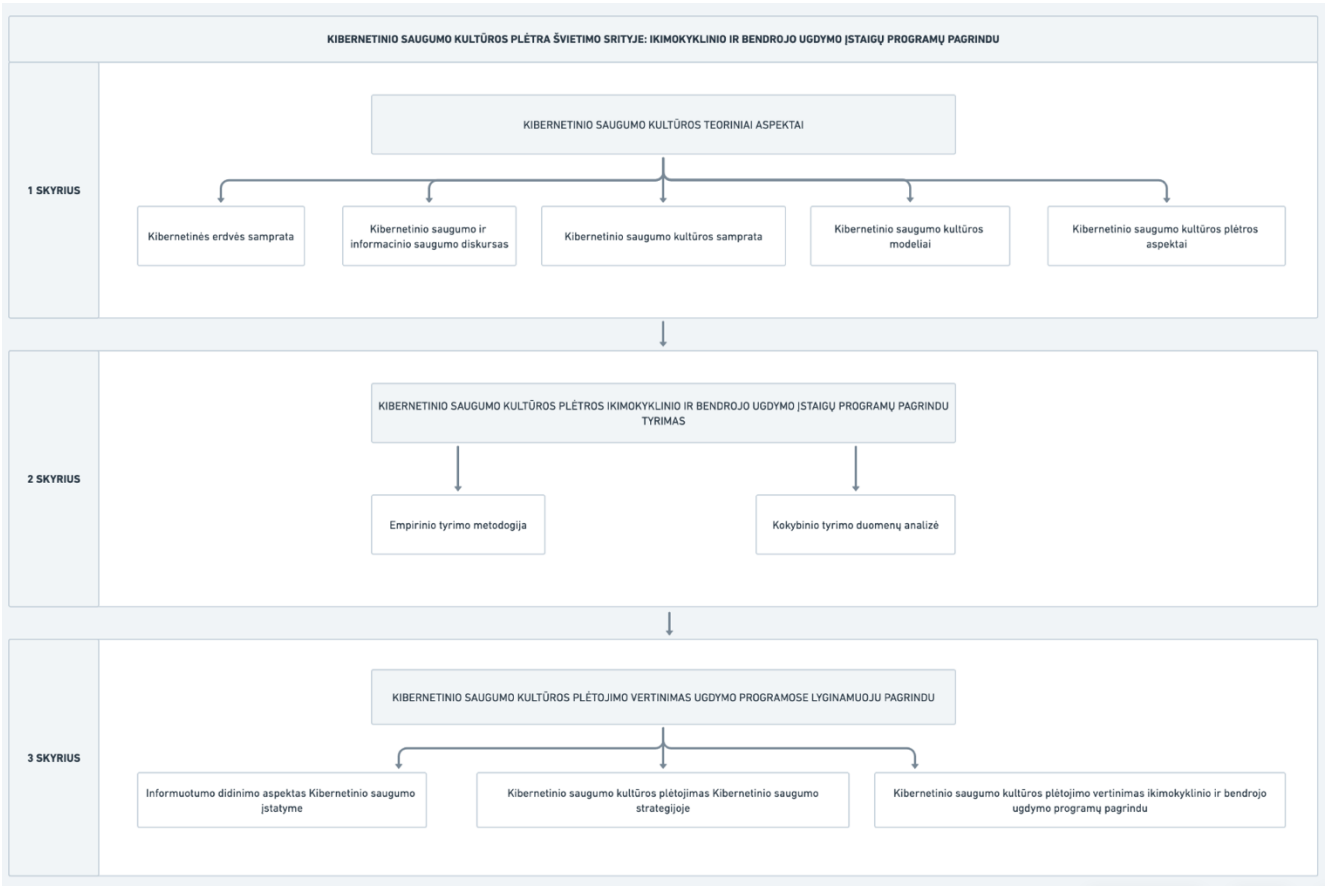
Duomenų rinkimo metodai:

1. Mokslinės literatūros sisteminimas.
2. Dokumentų kokybinio turinio (content) analizė.
3. Antrinių statistinių šaltinių analizė.
4. Pusiau struktūruotas interviu.

Duomenų analizės metodai:

1. Kokybinė turinio analizė.
2. Lyginamoji gautų duomenų analizė.

Darbo struktūra. Darbą sudarys 4 dalys (žr. 1 pav.). Pirmojoje dalyje analizuojami kibernetinio saugumo kultūros teoriniai aspektai ir problematika. Antrajame skyriuje pateikiama tyrimo metodologija ir nagrinėjami kokybinio tyrimo metu surinkti duomenys siekiant identifikuoti kibernetinio saugumo kultūros plėtojimo kryptis ugdymo programų pagrindu. Trečiojoje dalyje pateikiamas kibernetinio saugumo kultūros vertinimas ikimokyklinio ugdymo programose lyginamuoju pagrindu.



1 pav. Magistro baigiamojo darbo struktūros schema

Praktinis taikomumas. Kibernetinio saugumo kultūra skirstoma į penkis lygmenis: individualų, organizacinį, nacionalinį ir tarptautinį (Da Veiga, 2016). Individualus kibernetinio saugumo kultūros lygmuo yra esminis, tiesiogiai įtakojantis kitus keturis lygmenis. Būtent ikimokyklinio ir bendrojo ugdymo programos tiesiogiai, individualiajame lygmenyje, gali užtikrinti kibernetinio saugumo kultūros kėlimą. Šis darbas pateikia kibernetinio saugumo kultūros plėtojimo kryptis ikimokyklinio ir bendrojo ugdymo programų pagrindu, kurios gali būti integruotos į ikimokyklinio ir bendrojo ugdymo programas.

1. KIBERNETINIO SAUGUMO KULTŪROS TEORINIAI ASPEKTAI

Kibernetinė erdvė tapo informacijos ir komunikacijos globalia ekosistema. Su ja siejamos rizikos polemizuojamos tiek individualiu, tiek tarptautiniu lygiu. Reguliavimo poreikis yra naujas iššūkis valstybėms, kurių pagrindinis tikslas yra nacionalinis saugumas. Kibernetinės erdvės kontekstualumas ir kompleksiškumas įtakoja jos sampratos vystymąsi, kuri laikoma pagrindu bet kokiems tolimesniems reguliaciniams procesams.

1.1 Kibernetinės erdvės samprata

Informacinių ir ryšių technologijų konvergencija, visuotinai įdiegus interneto technologijas, įtakojo kibernetinės erdvės koncepcijos ir su ja siejamų grėsmių diskursą. Paraleliai mokslinėje literatūroje siekiama vienareikšmiškai apibrėžti kibernetinę erdvę. Mokslininkų teigimu šiuo metu nėra visuotinio konsensuso dėl kibernetinės erdvės apibrėžimo (Kramer, Starr ir Wentz 2009; Ottis ir Lorents (2010); Malik ir Choudhury 2019). Autoriaus Olagbemiro (2019) monografijoje pateikiama kibernetinės erdvės koncepcija kuriama per ekosistemos prizmę. Jo teigimu „kibernetinė erdvė nėra sritis, o veikiau socio-ekologinė ekosistema – pavyzdys dinamiškos kompleksinės adaptacinės sistemos“. Autoriai Rain Ottis ir Lorentsas (2010) kibernetinę erdvę apibrėžia kaip nuo laiko priklausomą rinkinį tarpusavyje sujungtų informacinių sistemų ir žmonių, kurie sąveikauja su šiomis sistemomis. Ozkanas ir Spruitas (2021) kibernetinei erdvei priskiria šias savybes: virtuali aplinka, kuri neegzistuoja fizine forma; tai sudėtinga aplinka dėl tarpusavyje susijungusių tinklų (tokių kaip internetas); ji turi keletą dimensijų: ją formuoja žmonės, organizacijos ir daugybė įrenginių ir tinklų, kurie yra prijungti prie kibernetinės erdvės. Clarckas (2010) ir Dunnas (2013) kibernetinę erdvę analizuoja apibrėždami jos tris komponentus: fizinį, loginį ir socialinį. Fizinis kibernetinės erdvės komponentas yra kibernetinės erdvės pagrindas – fiziniai įrenginiai iš kurių ji sukurta. Kibernetinė erdvė yra tarpusavyje sujungtų kompiuterinių sistemų erdvė, jos pagrindas yra kompiuteriai ir serveriai, superkompiuteriai ir tinklai, jutikliai ir keitikliai, internetas ir kiti tinklai bei ryšio kanalai. Ryšiai gali vykti laidais arba šviesolaidžiu, radijo bangomis arba fiziškai pernešant kompiuterinius ir saugojimo įrenginius iš vienos vietos į kitą (Clarck, 2010). Tuo tarpu loginis komponentas nėra apčiuopiamas ir įtraukia duomenis bei programinę įrangą. Loginio sluoksnio plastiškumas suteikia galimybę galutiniams vartotojams aktyviai dalyvauti jo kūrime, kuriant programas, paslaugas ir turinį, taip praplečiant loginį sluoksnį naujomis komunikacijos formomis taip sukuriant paskutinį socialinį sluoksnį. Autoriai Hathaway ir Klimburgas (2012) savo teoriniame tyrime taip pat paremia šių trijų komponentų sintezę kibernetinėje erdvėje, pabrėždami, kad kibernetinė erdvė įtraukia žmones ir jų socialinę sąveiką tinkluose papildydama techninę, programinę įrangas ir informacinių sistemų tinklus internete. Taigi remiantis teorinių tyrimų išvadomis galima teigti, kad kibernetinė erdvė yra žmonių socialinė sąveika palaikoma IRT su jų techninės priemonės.

Tarptautinės organizacijos taip pat aktyviai įsitraukia į kibernetinės erdvės sampratos problematikos plėtojimą pateikdamos savo kibernetinės erdvės apibrėžtis. Jungtinių tautų organizacija (JTO) kibernetinę erdvę ir jos saugumą analizuoja per IRT saugumo prizmę, siekiant sukurti normatyvinę sistemą, skirtą elgsenos formavimui naudojant IRT ir užtikrinti IRT aplinkos stabilumą tarptautiniu lygiu (United Nations, 2021). NATO savo operacijose pasitelkia šį apibrėžimą: „globali sritis, susidedanti iš visų tarpusavyje susijungusių ryšių, informacijos technologijų ir kitų elektroninių sistemų, tinklų ir jų duomenų, įskaitant tuos kurie yra atskirti arba nepriklausomi, kurie apdoroja, saugo ar perduoda duomenis“ (NATO, 2020). Taip pat, organizacija išskiria tris kibernetinės erdvės komponentus: fizinį, loginį ir kibernetinės personos. Autorių Clarcko (2010) ir Dunno (2013) kibernetinės erdvės modulio socialinis komponentas NATO yra tiksliai apibrėžiamas ir įvardijamas kaip kibernetinė persona. Europos Sąjungos kibernetinio saugumo agentūra (ENISA) pateikia šią apibrėžtį: „kibernetinė erdvė reiškia saitų ir ryšių rinkinį tarp objektų, kurie pasiekiami per apibendrintą telekomunikacijų tinklą, ir pačių objektų rinkinį, kurie turi sąsajas, leidžiančias nuotoliniu būdu valdyti, prieigą prie duomenų arba dalyvauti valdymo veiksmuose kibernetinėje erdvėje“ (ENISA, 2016). Šiuo apibrėžimu ENISA nedetalizuoja atskirų kibernetinės erdvės segmentų, juos apibendrindama kaip objektus, kurie sąveikaują tinklų pagrindu. Tarptautinė telekomunikacijų sąjunga (ITU) kibernetinę erdvę apibrėžia kaip: „vartotojus, tinklus, įrenginius ir visą programinę įrangą, procesus, saugomą arba perduodamą informaciją, taikomąsias programas, paslaugas ir sistemas, kurie gali būti tiesiogiai arba netiesiogiai prijungti prie tinklų“ (ITU, 2008). Tarptautinė standartizacijos organizacija (ISO) teigia, kad kibernetinė erdvė yra sudėtinga aplinka, atsirandanti dėl žmonių, programinės įrangos ir paslaugų sąveikos internete, palaikoma visame pasaulyje paskirstytų fizinių IRT įrenginių, kurie yra prijungti prie tinklų (ISO, 2012). ISO ir ITU apibrėžimai įtraukia tiek individą, tiek informacijos ir ryšių tinklus, kurių sąveikos sąlyga yra laikomas prisijungimas prie tinklų. OECD semantikoje vartojamas terminas „skaitmeninis“, kuris jų teigimu pabrėžia organizacijos ekonominę ir socialinę veiklos sritį (OECD, 2022). Tuo tarpu „kibernetinis“ yra siejamas su informacinėmis technologijomis (IT), tarptautiniu saugumu ir teisinėmis priemonėmis siekiant šį saugumą užtikrinti. Tarptautinė prekybos organizacija (PPO) taip pat neįtraukia kibernetinės erdvės savo terminologijoje, apibrėždami elektroninę prekybą tik elektroninių priemonių naudojimu. Jungtinių Tautų švietimo, mokslo ir kultūros organizacija (UNESCO) kibernetinei erdvei analizuoti pasitelkia šią sampratą: virtualus pasaulis, skirtas skaitmeninei ar elektroninei komunikacijai, susijęs su pasauline informacine infrastruktūra (UNESCO, 2003). UNICEF savo tyrimuose ir terminologijoje vartoja žodį „skaitmeninis“, akcentuojamas tik vaikų kibernetinis saugumas (UNICEF, 2018). Pateiktų kibernetinės erdvės definicijų tarptautinėse organizacijose analizė Clarckas (2010) ir Dunnas (2013) kibernetinės erdvės komponentų pagrindu išdėstyta 1 lentelėje.

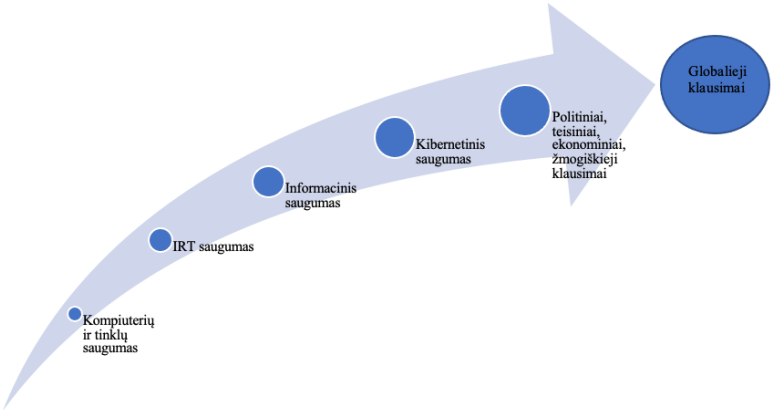
1 lentelė. Kibernetinės erdvės definicijos tarptautinėse organizacijose Clarck (2010) ir Dunn (2013) kibernetinės erdvės komponentų pagrindu

Tarptautinė organizacija	Fizinis aspektas	Loginis aspektas	Socialinis aspektas
OECD	-	-	-
PPO	-	-	-
UNESCO	✓	-	✓
UNICEF	-	-	-
JTO	✓	✓	
NATO	✓	✓	✓
ENISA	✓	✓	-
ITU	✓	✓	✓
ISO	✓	✓	✓

Remiantis analizės rezultatais galima teigti, kad tarptautinės organizacijos taip pat neturi konsensuso dėl vienareikšmės kibernetinės erdvės apibrėžties. Fizinis ir loginis kibernetinės erdvės komponentai yra įtraukiami į visas organizacijų pateiktas kibernetinės erdvės sampratas. Tačiau trečiasis, socialinis aspektas, identifikuojamas tik keturiuose apibrėžimuose. Galima daryti prielaidą, kad būtent šis aspektas reikalauja platesnės analizės. Taip pat svarbu pabrėžti, kad trijų organizacijų (OECD, PPO, UNICEF) vartojama semantika neįtraukia žodžio „kibernetinis“. OECD ir UNICEF vietoje jo naudoja terminą „skaitmeninis“, o PPO „elektroninės priemonės“. Taigi galima daryti išvadą, kad kiekviena organizacija remiasi savo veiklos sritimi formuodama savo žodyną ir politiką. Tačiau atsižvelgiant į kibernetinės erdvės globalumą ir su ja siejamą problematiką, ji įtraukia visas sritis. Kibernetinės erdvės apibrėžimas reikalauja tarpdisciplininės analizės, įtraukiant žmogaus teisių, techninių, saugumo, teisinių, ekonominių ir kt. disciplinų specialistus.

1.2 Kibernetinio saugumo ir informacinio saugumo diskursas

Nacionalinis ir tarptautinis dėmesys bei žiniasklaidos eskalacija kibernetinės erdvės saugumo klausimais įtakojo kibernetinio saugumo prioretizavimą. Autorius Ghernaouti (2013) pateikė besivystantį saugumo klausimų diskursą tarptautinėje bendruomenėje (žr. 2 pav.).



Šaltinis: adaptuota pagal Ghernaouti, 2013

2 pav. Saugumo klausimų diskursas

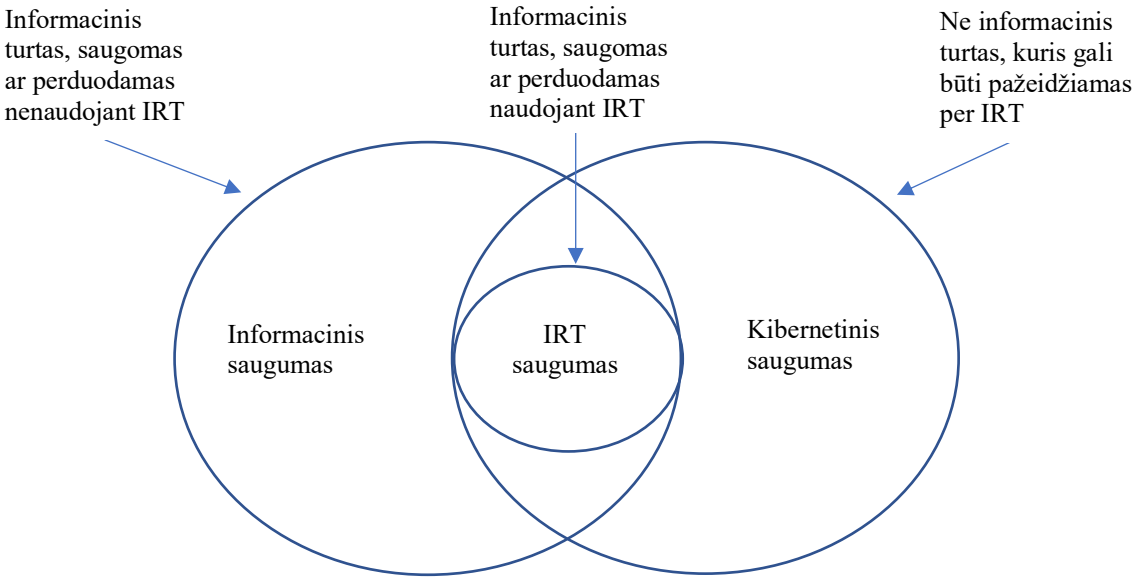
Kibernetinio saugumo svarba yra aktualizuojama teikiant jam prioritetą informacinio, IRT, kompiuterių ir tinklų saugumo atžvilgiu. Šią tendenciją taip pat atspindi ir Google žiniatinklio paieškos rezultatai, kurie rodo, kad nuo 2016 metų „kibernetinio saugumo“ (angl. cyber security) termino paieška išaugo keletą kartų, kai tuo tarpu „informacinio saugumo“ (angl. information security) termino paieška išliko be didesnių pokyčių (Google Trends, 2022). Kibernetinės erdvės saugumo klausimai taip pat pabrėžiami ir Europos Sąjungos Kibernetinio Saugumo Strategijoje (2020), kuri išreiškia poreikį, kad kiekvienas, kuris naudojasi internetu, prisidėtų prie globalios, atviros, stabilios ir saugios kibernetinės erdvės. Ši retorika taip pat pateikta ir JAV Kibernetinio Saugumo Strategijoje. Pasaulinio ekonominio forumo „Pasaulinėje rizikos ataskaitoje 2021“ konstatuojama, kad „verslo, vyriausybės ir namų ūkių kibernetinio saugumo infrastruktūra ir (arba) priemonės yra pranoktos arba atgyvenusios dėl vis sudėtingesnių ir dažnesnių kibernetinių nusikaltimų, sukeliančių ekonominius sutrikimus, finansinius nuostolius, geopolitinę įtampą ir/ arba socialinius nestabilumus“. Kibernetinės atakos turi tiek trumpalaikį, tiek ilgalaikį ekonominį poveikį skirtingiems ūkio subjektams nuostolių ir išlaidų prasme (Gañán, Ciere ir van Eeten, 2017). Taigi saugumo klausimai, susiję su kibernetine erdve, reikalauja koordinuotų ir sutelktų nacionalinės ir tarptautinės visuomenės, vyriausybių ir privataus sektoriaus pastangų. EBSCO tai pabrėžia per išskirtus kibernetinio saugumo aspektus: techninį, socialinį ir ekonominį, nacionalinį ir tarptautinį saugumą bei teisėsaugą (kibernetiniai nusikaltimai) (EBSCO, 2022). Siekiant atitikti šį platesnį saugumo kontekstą, reikalingi papildomi saugumo sprendimai nei tik organizacijos informacinio saugumo lygmenyje. Saugumo problematika pirmiausia kyla už organizacijos konteksto ribų, o tai turi įtakos asmenims, kurie naudojasi žiniatinkliu privačiame ar socialiniame kontekste. Taigi kibernetinis saugumas yra sprendimas sutelkiantis dėmesį į šį visa apimantį platesnį kontekstą.

Kibernetinės erdvės koncepcija yra laikoma kibernetinio saugumo analizės pagrindu (ISO, 2012; ENISA, 2017). Vienareikšmės kibernetinės erdvės definicijos trūkumas įtakoja ir kibernetinio saugumo

sampratos vystymą (Lahsen ir kt., 2020; ENISA, 2016). Tai pripažįstama tiek tarp profesionalų (Barzilay, 2013; Stubley, 2013; Walls, Perkins ir Weiss, 2013), tiek vyriausybiniu (EU, 2020), tiek akademiniu lygiu (Cainsetal, 2021; Lahsen ir kt., 2020). Cainsetalo (2021) atlikto tyrimo rezultatai rodo: kibernetinio saugumo ir kibernetinio saugumo rizikos apibrėžimai skiriasi tarp JAV Armijos Tyrimų Laboratorijos ir akademinių sektorių ir kibernetinio saugumo ir kibernetinio saugumo rizikos apibrėžimai skiriasi tarp kibernetinių ekspertų ir ontologijos vystytojų. Be to, kai kurie ekspertai turėjo tarpusavyje priklausomus kibernetinio saugumo ir kibernetinio saugumo rizikos apibrėžimus, naudojant vieną terminą kitam apibrėžti. Taip pat, kibernetinio ir informacinio saugumo sąvokų persipynimas formuoja kibernetinio saugumo kaip atskiros saugumo disciplinos suvokimą. Autorių Özkan ir Choudhury (2019) nuomone sąvokos informacijos ir kibernetinio saugumo srityse yra glaudžiai susijusios, todėl nekvalifikuotiems suinteresuotiesiems subjektams viskas tampa komplikuota. Reidas ir Van Niekerk (2014), Perkinsas, Wallsas ir Weissas (2013) medijų retorikoje įžvelgė kibernetinio saugumo sąvokos asimiliaciją su informaciniu saugumu ir teigė, kad yra daroma klaidinga prielaida. Siekdama padėti organizacijoms ir asmenims praplėsti suvokimą apie kibernetinio saugumo standartizavimą, sertifikavimą ir ženklinimą, Europos kibernetinio saugumo organizacija (ECSO) paskelbė esamų kibernetinio saugumo standartų ir sertifikavimo schemų apžvalgą (ECS, 2017). Šiame dokumente pateikiami ir ISO standartai, kurie nubrėžia aiškią ribą tarp informacinio ir kibernetinio saugumo. ISO/IEC 27000:2018 standartas informacinį saugumą apibrėžia kaip: „informacijos konfidencialumo, vientisumo ir prieinamumo (angl. CIA) išsaugojimą plačiąja prasme“ (ISO, 2018). Tuo tarpu ISO/IEC 27032:2012 standartas apibrėžia kibernetinį saugumą kaip: „informacijos konfidencialumo, vientisumo ir prieinamumo (angl. CIA) kibernetinėje erdvėje išsaugojimą“ (ISO, 2012). Taip pat šis standartas apibrėžia ryšį tarp kibernetinio saugumo ir kitų sričių: „Kibernetinis saugumas remiasi informacijos saugumu, programų saugumu, tinklo saugumu ir interneto saugumu kaip pagrindiniais elementais. Jis turi unikalią taikymo sritį, todėl suinteresuotosios šalys turi aktyviai veikti siekiant išlaikyti, jei ne pagerinti, kibernetinės erdvės naudingumą ir patikimumą“ (ISO, 2012). Autoriai (Lahsen ir kt., 2020; Antunes, Maximiano, Gomes ir Pinto, 2021) kibernetinio saugumo tyrimuose taip pat remiasi ISO standarto pateikiama CIA triada kaip esminiais kriterijais vertinančiais kibernetinį saugumą. CIA triados indikacija kibernetinio saugumo definicijoje, kibernetinį saugumą priskiria prie vieno iš informacinio saugumo komponentų, funkcionuojantį kibernetinės erdvės ribose. Taigi dėl apibrėžto ryšio tarp informacinio saugumo ir kibernetinio saugumo yra pagrįsta daryti prielaidą, kad tai, kas taikoma informacijos saugumui užtirinti turėtų būti taikoma ir kibernetiniam saugumui (Özkan, 2019; Gcaza, von Solms, ir van Vuuren, 2015; Uchendu, Nurse, Bada ir Furnell, 2021).

Mokslininkai Solmsas ir van Niekerkas (2013) siekė išskirti kibernetinį saugumą iš informacinio saugumo konteksto, pabrėždami tik kibernetinei erdvei būdingas ypatybes. Atliktame tyrime jie išskiria du kibernetinio saugumo aspektus, kurie nėra įtraukiami į informacinio saugumo apibrėžtį ir priskiriami

tik kibernetinio saugumo sričiai. Tai yra ne informacinio turto (individo veikiančio kibernetinėje erdvėje) ir pačios kibernetinės erdvės saugumas (žr.3 pav.).



Šaltinis: adaptuota pagal Solms ir Johan van Niekerk, 2013

3 pav. Informacinio, IRT ir kibernetinio saugumo sąsajos

Šiuos mokslininkų išskirtus aspektus taip pat pabrėžia ir ENISA. Agentūros teigimu kibernetinis saugumas turi remtis CIA paradigma, kuri turi būti išplėsta sprendžiant individualių/juridinių asmenų (žmonių ir organizacijų) privatumo apsaugos ir atsparumo (atsistatymo po atakos) klausimus (ENISA, 2016). ITU šią kibernetinio saugumo sampratą dar labiau išplėtoja, kibernetinį saugumą traktuodama kaip „įrankių, politikos krypčių, saugumo koncepcijų, saugumo priemonių, gairių, rizikos valdymo metodų, veiksmų, mokymų, geriausios praktikos, užtikrinimo ir technologijų, kurios gali būti naudojamos kibernetinei aplinkai ir organizacijai bei vartotojo turtui apsaugoti, rinkinį“. Šių kibernetinio saugumo objektų išskyrimas išplečia saugumo koncepciją reikalaudamas papildomų saugumo priemonių, kurios būtų nukreiptos į asmenį. Be to, tai, ar žmonės saugiai naudoja technologijas ir visiškai bei teisingai seka saugių procesų gaires įtakoja šių komponentų saugumo mastą, nes žmonės gali sąmoningai ir nesąmoningai tapti grėsme bet kokiam informacijos saugumo sprendimui. Kibernetinio saugumo kultūros kūrimas yra viena iš efektyviausių priemonių, kuri skatina priimtiną žmonių elgesį kibernetinėje erdvėje (Alfawaz, Nelson ir Mohannak, 2010; Da Veiga ir Eloff , 2010).

1.3 Kibernetinio saugumo kultūros samprata

Kultūra yra sudėtingas reiškinys, apimantis įvairias sritis ir turintis daugybę apibrėžimų literatūroje (Leidner ir Kayworth, 2006; Straub, Loch, Evaristo, Karahanna ir Srite, 2002). Šie kultūros apibrėžimai pateikia skirtingas sąvokas, kurios apima vertybes, simbolius, žinias, elgesį, nuostatas, įsitikinimus, suvokimą ir pagrindines prielaidas (Hofstede, Hofstede ir Minkov, 2005; Schein, 2010). Kultūra skirstoma į kategorijas pagal atskiras bendrų vertybių dimensijas nacionaliniu lygiu (Hofstede, 2005), organizacijos lygmeniu (Cameron ir Quinn, 2011; Schein, 2010) ir individualiu lygiu. Daugumoje informacinių saugumo studijų kultūra buvo konceptualizuota remiantis nacionaliniais ir organizaciniais lygmenimis. Plačiausiai priimtas mokslinės bendruomenės analizuojančios organizacinius procesus (Kreps, 1990; Van de Steen, 2010, Gzaca ir von Solms, 2017; Huang ir Pearlson, 2019) organizacinės kultūros modelis yra Schein modelis. Scheinas (1990) organizacijos kultūrą apibrėžia kaip: „pagrindinių prielaidų modelis – sugalvotas, atrastas arba sukurtas tam tikros grupės, kai ji mokosi susidoroti su išorinio prisitaikymo ir vidinės integracijos problemomis – kuris pasiteisina pakankamai, kad būtų laikomas galiojančiu, ir todėl yra pateikiamas naujiems nariams kaip teisingas metodas suvokti, vertinti ir jausti šias problemas“. Taip pat, Schein pristatė tris kultūros lygius, pateikdamas analizės ir diferencijavimo priemones, susijusias su vertybėmis, kurios apibrėžia organizacinę kultūrą. Šie trys lygiai vienas kitą papildo ir gali būti apibūdinti kaip (Schein, 2010):

- Artefaktai: yra tai, kas gali būti stebima, matoma, išgirsta ir jaučiama organizacijoje, t. y. tai, kas vyksta organizacijoje ir gali būti stebima be papildomų įgūdžių.
- Vertybės: yra oficialus organizacijos požiūris, kuris apima vertybes, principus ir viziją. Šios vertybės komunikuojamos su misijos teiginiais, strategijos dokumentais, elgesio kodeksu ir kitais dokumentais apibūdinančiais organizacijos vertybes.
- Prielaidos: susideda iš darbuotojų įsitikinimų ir vertybių, perimtų iš organizacijos sėkmės laikui bėgant.

Šis modelis buvo vystomas kitų mokslininkų siekiant organizacinę kultūrą susieti su informaciniu saugumu. Redi ir van Niekerkas (2014) patvirtino, kad Scheino organizacijos kultūros modelis kartu su kai kuriais pakeitimais gali sudaryti palankią aplinką saugumo kultūrai. Autoriai šio modelio pagrindu sukūrė informacinės saugumo kultūros modelį, įtraukdami dar vieną - žinių lygį. Šis papildomas lygis - informacinio saugumo žinios - buvo pridėtas siekiant paremti kitus tris lygius, nes žinios laikomos pagrindine saugumo kultūros dalimi. Edgellas ir Granteris (2019, p. 131) Schein modelyje taip pat pristatė papildomą - anstatinį lygmenį, kuris atkreipia dėmesį į išorinius veiksnius. Jų nuomone, organizacijos neveikia izoliuotoje aplinkoje ir sąveikauja su nacionaliniais, visuomeniniais ir ekonominiais veiksniais, kurie turi įtakos kultūrai ir į tai reikėtų atsižvelgti. Taigi Schein (2010)

organizacinės kultūros modelis gali būti laikomas pagrindu informacinio saugumo kultūros sampratos plėtojimui, dėl plačios informacinio saugumo mokslinės analizės organizaciniame kontekste.

Informacinio apdorojimo ir apsaugos sąvokų perėjimo iš techninių ir matematinių aspektų į socialiai reikšmingų apraiškų plotmę parodo poreikį įtraukti visus socialinės sąveikos aspektus, ypač elgesio kultūros formavimą (Vilkova, Litvishkov Shvyrev, 2020). Būtent kultūros apibrėžties kompleksiškumas įtakojo teorinį informacinio saugumo kultūros apibrėžtį ir konceptualizavimą literatūroje. Priklausomai nuo naudojamos kultūros teorijos, informacinio saugumo kultūros tyrinėtojai savo supratimą apie informacinio saugumo kultūrą sutelkia į veiksmus (elgesį) (Masrek, Harun ir Zaini, 2018; Ruhwanya ir Ophoff, 2019) ir bendras organizacijos vertybes (Batteau, 2011; Olivos, 2012; Shahibi ir kt., 2012). Kiti tyrinėtojai informacijos saugumo kultūrą priskiria organizacinės kultūros daliai arba subkultūrai (Mokwetli ir Zuva, 2018). Taip pat, tyrimai rodo, kad kontekstiniai skirtumai yra esminis veiksnys, į kurį reikia atsižvelgti kuriant informacinio saugumo priemones, kad būtų pasiektas atitiktį tenkinantis elgesys (Aurigemma ir Mattson, 2019). Autorių Hengstlerio ir Pryazhnykovos (2021) atlikta mokslinės literatūros analizė rodo, kad dabartiniai informacinio saugumo kultūros tyrimai sutelkti į keturias pagrindines tematikas:

1. kultūros įtaką elgesiui laikantis informacinės saugumo politikos;
2. informacinę saugumo kultūrą organizacijose;
3. kultūros įtaką informacinio saugumo sąmoningumo kėlimo programoms;
4. kultūros poveikį informacinio saugumo valdymui.

Esamuose tyrimuose analizuojami įvairūs mechanizmai, darantys įtaką darbuotojų atitikties elgesiui, pvz. asmens socialinė aplinka, neoficialių ir formalių sankcijų taikymas siekiant užtikrinti atitiktį. Informacinio saugumo kultūros ugdymas socialiniame kontekste daro įtaką asmens elgesiui, o tai stipriai įtakoja informacinį saugumą (Marotta ir Pearlson, 2019; D'Arcy ir Greene, 2014). Schliengeris ir Teufelis (2003) teigia, kad saugumo kultūra, „turėtų remti visą veiklą taip, kad informacijos saugumas taptų natūraliu aspektu kiekvieno darbuotojo kasdienėje veikloje". Remiantis šiais atliktais moksliniais tyrimais galima teigti, kad informacinio saugumo kultūra šiuo metu yra koncentruota į organizacinį lygį ir darbuotojų elgesio atitikties saugumo standartams užtikrinimą. Tai patvirtina ir autoriai Gangire, Veiga ir Herselman (2019), kurių teigimu: „informacijos saugumo kultūra gali būti kolektyvinis visų įmonės darbuotojų supratimas ir pagarba informacijos saugumui". Tačiau informacinio saugumo kultūros puoselėjimas tik organizaciniame kontekste nebėra pakankamas apsaugoti daugumą žmonių, kurie veikia kibernetinėje erdvėje. Taip pat, saugumo poreikis nebėra laikomas vien tik organizaciniu klausimu. Saugumo kultūros vystyme dėmesys nebėra koncentruojamas vien į techninius informacinio saugumo aspektus, o procesų ir technologijų pusiausvyrą įtraukiant asmenis, grupes ir organizacijas (Tang, Li ir Zhang, 2016). Taigi galima daryti prielaidą, kad būtent šie ribotumai aktualizuoja kibernetinio saugumo kultūrą ir jos poreikį žmogui kasdienėse operacijose.

Kibernetinio saugumo kultūra ir informacinio saugumo kultūra yra glaudžiai susijusios. Autoriai Uchendu, Nurse, Bada ir Furne (2021) 2010 - 2020 metais moksliniuose straipsniuose analizavo trijų pagrindinių definicijų - saugumo kultūros, informacinės saugumo kultūros ir kibernetinio saugumo kultūros - pasiskirstymą. Jie nustatė, kad kibernetinio saugumo kultūros definicija pradėta plačiai naudoti tik 2019 metais, tuo tarpu informacinės saugos kultūros samprata buvo plačiai polemizuojama ir vystoma nuo tyrimo pradžios intervalo, 2010 metų. Taip pat, mokslininkai patvirtina prielaidą, kad nors ir buvo žymių informacinio saugumo kultūros ir kibernetinio saugumo kultūros sąvokų naudojimo diferenciacijų, esminiai veiksniai abiem terminams yra tapatūs. Nors kultūros skatinimas siekiant kibernetinio saugumo yra plačiai diskutuojamas ir nurodomas kaip strateginis tikslas tiek organizaciniame, tiek tarptautiniame lygmenyje, tyrimai, kuriuose daug dėmesio skiriama kibernetinio saugumo kultūros apibrėžimui ir vertinimui, yra tik pradinėje vystymo stadijoje (Da Veiga, 2016). Reido ir van Niekerko (2014) atlikti tyrimai atskleidė, kad kibernetinio saugumo kultūros sąvoka neturi esminių ją išskiriančių elementų. Tai patvirtino ir autoriai Gzaca ir von Solms (2017), atlikę kibernetinės saugumo kultūros sampratos literatūrinę analizę ir konstatavę, kad ji neturi koncepcijos ir aiškiai nubrėžtų kibernetinio saugumo kultūros sąvoką apimančių ribų. Galima daryti prielaidą, kad kibernetinio saugumo kultūros samprata ir koncepcija yra apibrėžiama ir priklauso nuo tyrimo objekto. Taigi nėra vienareikšmės apibrėžties, kuri galėtų būti laikoma pagrindu kibernetinio saugumo kultūros teoriniuose ir empiriniuose tyrimuose.

Moksliniuose empiriniuose ir teoriniuose straipsniuose autoriai pateikia nevienareikšmius kibernetinės erdvės apibrėžimus. Tziarras (2014) savo straipsnyje siekia argumentuoti globalaus ir daugiapakopio kibernetinio saugumo valdymo plėtros poreikį. Kibernetinio saugumo kultūra jo darbe apibrėžiama kaip: „visuma priemonių – tai yra nevalstybinių, subnacionalinių ir nacionalinių nuostatų, elgesio modelių, įsitikinimų, taip pat (kibernetinio) saugumo sampratų, pagrįstų poreikiu apsaugoti referencinius objektus nuo įvairių kibernetinių grėsmių, kurios turėtų įtakos kibernetinio saugumo strategijoms“. Roerio (2015) kibernetinio saugumo kultūrą apibūdina kaip „konkrečių žmonių ar grupės idėjas, papročius ir socialinį elgesį, padedantį jiems išsivaduoti nuo grėsmės ir pavojų“. Ioannou, Stavrou ir Bada (2019) savo empiriniame tyrime analizuoja veiksnius, susijusius su kibernetinio saugumo kultūros kūrimu organizaciniame kontekste. Jie apibrėžia kibernetinio saugumo kultūrą kaip „procesus, kuriuos organizacija nustato visiems savo darbuotojams, pateikdama veiksmų seką visose su duomenų vientisumu susijusiose situacijose“. Tuo tarpu Wiley, McCormaco ir Calico (2020) savo tyrime analizavo sąryšį tarp organizacinės kultūros, saugos kultūros ir kibernetinio saugumo sąmoningumo. Šiame tyrime kibernetinio saugumo kultūra apibrėžiama kaip „organizacijos kultūros subkultūra, apimanti požiūrius, įsitikinimus, vertybes ir žinias, kurių pagrindu asmenys kasdien sąveikauja su organizacijų sistemomis ir atlieka atitinkamas procedūras, užduotis ir veiklas“. Huangas ir Pearlsonas (2019) savo teoriniame moksliniame straipsnyje taip pat analizavo organizacinį kibernetinį

saugumą. Autoriai kibernetinio saugumo kultūrą apibrėžė kaip „įsitikinimus, vertybes ir nuostatas, įtakojančias darbuotojų elgesį, siekiant apsaugoti ir ginti organizaciją nuo kibernetinių atakų“. ENISA nutolsta nuo organizacinio lygmens atsižvelgdama į individualų, vartotojo lygį ir kibernetinio saugumo kultūrą apibrėžia kaip: „žmonių žinias, įsitikinimus, suvokimą, požiūrį, prielaidas, normas ir vertybes, susijusias su kibernetiniu saugumu ir kaip jos pasireiškia žmonių elgesyje naudojant informacines technologijas“ (ENISA, 2018). Da Veiga (2016) savo teoriniame tyrime siekė apibrėžti kibernetinio saugumo kultūrą teigdamas, kad „kibernetinio saugumo kultūra turi būti skatinama tarptautiniu, nacionaliniu, organizaciniu ir asmeniniu lygmeniu, siekiant sumažinti riziką žmogaus atžvilgiu kibernetinėje erdvėje“ (žr. 4 pav.).



Šaltinis: adaptuota pagal Da Veiga, 2016

4 pav. Kibernetinio saugumo kultūros lygiai

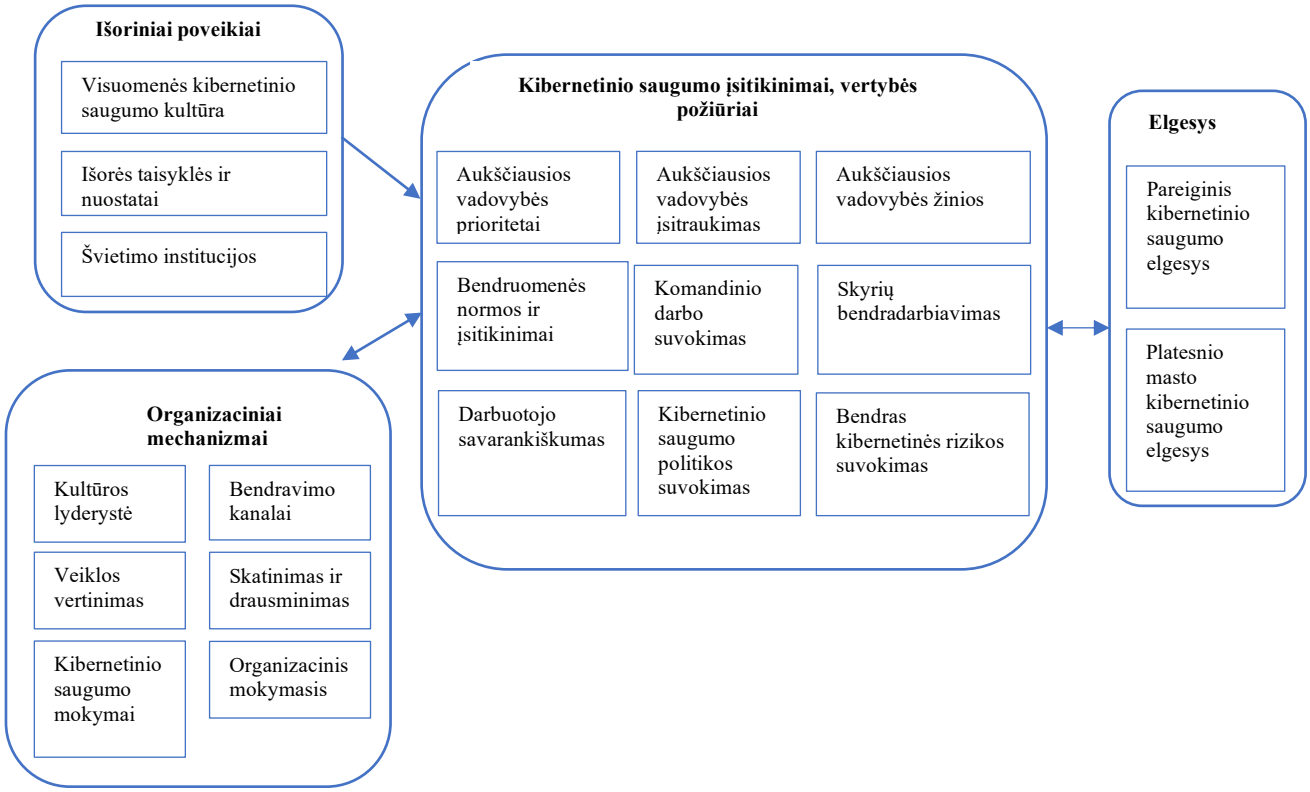
Išvadose jis pateikia šį kibernetinės saugumo kultūros apibrėžimą: „nesąmoninga ar sąmoninga elgsena, kuriuo kibernetinė erdvė naudojama keturiais lygiais tarptautiniu, nacionaliniu, organizaciniu arba asmeniniu, kuri skatina arba varžo asmenų, organizacijų ar vyriausybių saugumą, privatumą ir pilietines laisves“.

Kibernetinio saugumo kultūros samprata, kaip ir informacinio saugumo plačiausiai analizuojama organizaciniame lygyje. Tai įtakoja ir sąvokų “informacinė saugumo kultūra” ir “kibernetinio saugumo kultūra” persipynimą ir jų naudojimo konteksto neaiškumą. Svarbu pabrėžti, kad kibernetinis saugumas išskiriamas iš informacinio saugumo konteksto dėl pačio žmogaus saugumo veikiančio kibernetinėje erdvėje. Da Veiga (2016) pateiktas apibrėžimas neįtraukia techninio aspekto, tačiau apima plačiausią spektrą kibernetinio saugumo apibrėžties objektų ir nurodo esminį veiksnį - žmogaus sąmoningą ar nesąmoningą elgseną. Šis apibrėžimas atskleidžia kibernetinės saugumo kultūros kompleksiškumą, daugiamatiškumą ir tarpdisciplininės analizės kryptį tolimesniems moksliniams tyrimams.

1.4 Kibernetinio saugumo kultūros modeliai

Mokslinėje literatūroje plačiai vystomi informacinio saugumo kultūros modeliai, tarp kurių Da Veigos (2010) informacinio saugumo kultūros modelis, AlHogail (2015) informacijos saugumo kultūros sistema, Tolah, Furnell, ir Papadaki (2017) išsami informacijos saugos kultūros sistema, Nel ir Drevin (2019) pagrindinių informacinės saugumo kultūros elementų nustatymas. Da Veigos (2010) atlikta informacinio saugumo kultūros analizė ir pristatytas modelis yra laikomas kibernetinio saugumo kultūros tyrimų pagrindu. Tačiau šiuo metu stingant vienareikšmės kibernetinio saugumo koncepcijos, tyrimai kultūros vystymo klausimais yra labai riboti.

Mokslininkai Huangas ir Pearlsonas (2019) pristatė vadybinius kibernetinio saugumo kultūros valdymo aspektus (žr. 5 pav.).

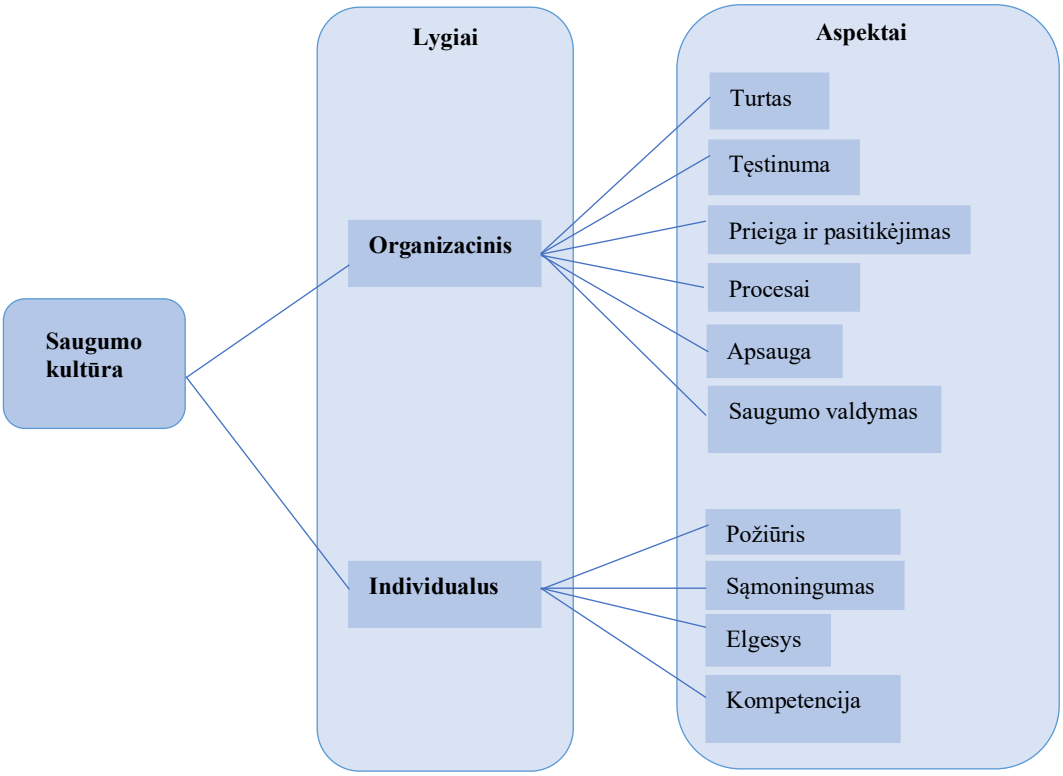


Šaltinis: adaptuota pagal Huang ir Pearlson, 2019

5 pav. Huang ir Pearlson organizacinio kibernetinio saugumo modelis

Šis modelis yra orientuotas į organizacijos vadovą ir jo įtaką kibernetinio saugumo kultūros kūrimui. Kibernetinio saugumo įsitikinimams, vertybėms ir požiūriams įtakos turi išorės veiksniai, kurių negali kontroliuoti vadovas ir vidiniai organizaciniai mechanizmai, kuriuos tiesiogiai įtakoja organizacijos vadovai. Kibernetinio saugumo įsitikinimai, vertybės ir požiūriai skirstomi į tris lygius: individualų, grupinį ir vadovybės. Jie tiesiogiai įtakoja elgesį, kuris skirstomas į pareiginį kibernetinio saugumo elgesį ir papildomą, kuris išreiškiamas bendradarbiavimu ir įsitraukimu. Autorių teigimu vadovai gali naudoti šią sistemą kibernetinio saugumo vystymui ir investicijų planavimui organizacijoje.

Autoriai Georgiadou, Mouzakitis, Bounas ir Askounis (2020) derindami į žmogų orientuotus elementus ir aspektus su organizaciniais, tiek išoriniais, tiek vidiniais, parametrais, sukūrė globalizuotą kibernetinio saugumo kultūros modelį (žr. 6 pav.).



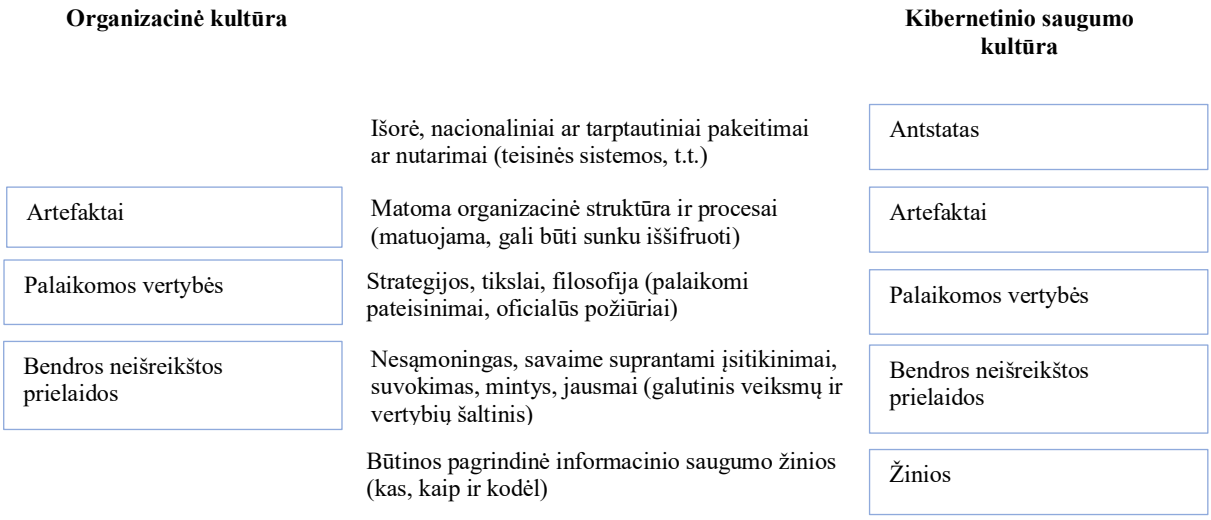
Šaltinis: adaptuota pagal Georgiadou ir kt., 2020

6 pav. Georgiadou ir kt. (2020) saugumo kultūros modelis

Šis modelis aiškiai apibrėžia du lygius: organizacinį lygį, apimantį visus veiksnius, susijusius su organizacijos saugumo technologine infrastruktūra, operacijomis, politika ir procedūromis ir individualųjį lygį, kuris yra orientuotas į darbuotojo savybes, turinčias tiesioginės įtakos elgesiui ir jų požiūriui į saugumą. Taigi, modelis aprėpia abu - išorinius žmogiškuosius veiksnius, taip pat vidinius, skatinamus individualių sampratų. Tada kiekvienas lygis suskirstomas į skirtingus matmenis. Georgiadou ir kt. (2020) modelis taip pat apima kiekvieno elemento suskirstymą į konkrečias disciplinas, kuriose įvedami rodikliai, siekiant pateikti tikslų kiekybinį įvertinimą. Gauti rezultatai tiksliai parodo esamas saugumo silpnybes ir spragas, kurios leidžia personalizuoti saugumo mokymo programas ir jas pritaikyti prie konkrečių vartotojų poreikių. Pasiūlymai ir rekomendacijos teikiamos tiek asmenims, tiek direktoriams, o sprendimus priimanti taryba turi tikslų jų saugumo kultūros statusą ir silpnąsias vietas. Tačiau šis modelis neįtraukia išorinių veiksnių, kurie taip pat tiesiogiai įtakoja tiek saugumo kultūrą, tiek organizacinį ir individualų lygius.

Moksliniame darbe autorius Michalos (2021, p. 34) sujungia autorių Redi ir Va Niekerko (2014) bei Edgello ir Granterio (2019, p. 131) tyrimus Schein organizacinės kultūros modelio srityje. Modelis

įtraukia žinių lygį, kuris yra esminis IT srityje, taip pat Edgello ir Granterio (2019, p. 131) anstatinį lygį, kuris atspindi išorinius veiksnius (žr. 7 pav.).



Šaltinis: adaptuota pagal Michalos, 2021, p. 34

7 pav. Michalos (2020) kibernetinio saugumo kultūros modelis

Autoriaus teigimu, šiame modelyje aptariama daug aspektų, turinčių tiesioginės įtakos kibernetinio saugumo kultūrai ir jie turėtų būti išplėtoti kuriant kompetentingą kibernetinio saugumo kultūrą.

Literatūros analizė atskleidė ribotą tyrimų kiekį kibernetinės kultūros vystymo srityje. Mokslininkų vystomi kibernetinio saugumo kultūros vertinimo kriterijai yra pradinėje stadijoje ir koncentruojasi į organizacinį kultūros lygį. Kibernetinio saugumo kultūros apibrėžimo priklausomybė nuo autorių perspektyvos ir taikymo konteksto patvirtina, kad kibernetinio saugumo kultūros samprata šiuo metu yra nepakankamai apibrėžta. Kultūros vystymo ir plėtojimo galimybės šiuo metu nėra pakankamai plačiai diskutuojamos ir sprendžiamos mokslinėje bendruomenėje. Tačiau, visuose atliktuose tyrimuose pateikiami kibernetinio saugumo kultūrą įtakojantys išoriniai ir vidiniai faktoriai yra orientuoti į žmogaus elgesį, kuris turi tenkinti pagrindinius kibernetinio saugumo reikalavimus. Taigi galima daryti prielaidą, kad kibernetinio saugumo kultūra turi būti plėtojama žmogaus sąmoningumo ugdymo, mokymo ir švietimo programomis.

1.5 Kibernetinio saugumo kultūros plėtros aspektai

ENISA pasitelkia Maslow poreikių piramidės metodą siekiant atspindėti kibernetinio saugumo poreikių hierarchiją, pradedant nuo pagrindinių ES vertybių, demokratijos ir žmogaus teisių aukščiausiame lygmenyje ir baigiant pagrindu - kibernetine higiena, žmonių naudojančių internetą sauga ir saugumu (ENISA, 2017). Siponenas (2001) išskiria penkias sąmoningo saugumo dimensijas ir

pagrindines jų problemas, kurias reikia išspręsti, kad būtų patenkinti visi žmogaus saugumo poreikiai. Šie aspektai apima :

- organizacinius;
- plačiosios visuomenės;
- socialinius ir politinius;
- kompiuterinio etinio;
- institucinio švietimo aspektus.

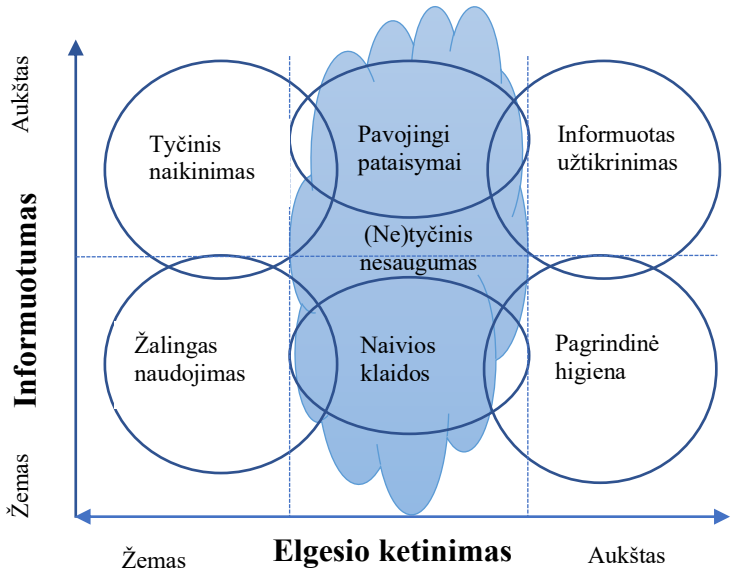
Visų šių dimensijų informuotumo didinimas gali lemti kibernetinio saugumo suvokimo kultūrą visoje visuomenėje. Tačiau atlikti moksliniai tyrimai šiuo metu koncentruojasi organizaciniame lygyje ir formuoja saugumo informuotumo didinimo vystymąsi.

1.5.1 Žmogiškasis faktorius

Moksliniai tyrimai IRT pažeidžiamumų srityje atlikti autorių Huango ir Pearlsono (2019), Ghernouti (2016), Lacey (2009), O'Brien, Islam, Bao, Weng, Xiong ir Ma (2013), Parsons, McCormac, Butavicius and Ferguson (2010), Wiley, McCormac ir Calic (2020), Luthra (2020) konstatuoja, kad žmogiškasis faktorius įtakoja visas informacijos ir ryšių saugumo priemones. Tai lemia kibernetinės atakos išnaudojančios žmogaus psichologijos aspektus, klaidas ar darbuotojų aplaidumą. Hallas (2016) darbuotojus įvardija kaip „didžiausią kibernetinio saugumo pastangų (arba) plano silpnybės šaltinį". Autorius pabrėžia, kad rengdamos bet kokį kibernetinio saugumo planą organizacijos turėtų atsižvelgti į pažeidžiamumus, kuriuos sukelia darbuotojai. Sisanecis, Akinas, Karamanas ir Saglamas (2013) pasitelkė piramidės metodą analizuojant institucinį kibernetinį saugumą, kuriame darbuotojai taip pat laikomi kibernetinio saugumo pagrindu tuo pačiu ir silpniausia grandimi. Organizacijos pasitelkia technologinius sprendimus ir politiką sprendžiant kibernetinio saugumo problemas, tačiau darbuotojų mokymai ir kibernetinio saugumo sąmoningumo ugdymas nėra prioretizuojami (Rauf, 2019). Siekiant kovoti su kibernetinio saugumo grėsmėmis žmonės, technologijos ir politika turi būti integruoti kartu. Taigi atliktų tyrimų rezultatai atskleidžia, kad informacinio saugumo programos sėkmė priklauso nuo žmogaus elgesio ir sąmoningumo, susijusio su informaciniu saugumu. Taip pat galima daryti prielaidą, kad geresnis žmogaus elgesio ypatybių supratimas gali padėti įvertinti ir tobulinti su informaciniu saugumu susijusį elgesį ypač dinamiškoje kibernetinėje aplinkoje.

Žmogiškųjų veiksnių (pvz. individualus pasirinkimas ir elgesys) ir kaip šie veiksniai susiję su požiūriu į informacinį saugumą (Afawaz, 2010) ir jo valdymą yra laikomi saugumo kultūros plėtojimo pagrindu. Washo (2010) teigimu detalūs žmogaus ir visuomenės psichologiniai kibernetinio saugumo elgesio modeliai gali padėti kibernetinio saugumo specialistams kurti geresnes ir intuityvesnes saugumo technologijas. Informacinio saugumo kultūros kontekste Furnell ir Thomson (2009) nustatė daugybę

veiksnių, kurie, gali būti teorizuoti kaip darantys įtaką žmogaus norui laikytis nustatytų saugumo kultūros normų. Jų teigimu veiksniai, į kuriuos reikėtų atsižvelgti vystant kibernetinio saugumo kultūrą, yra šie: funkcijos, kurias turi atlikti žmogus; užduoties pobūdis; žmogaus elgsena ir psichologija. Remiantis šiais trimis aspektais, galima konstatuoti, kad žmogaus elgsena ir psichologija yra laikoma prioritetine sritimi. Alfawaz (2010) organizaciniame lygmenyje sukūrė informacinio saugumo praktikos sistemą grįstą darbuotojų elgesiu. Šioje sistemoje, darant prielaidą, kad asmuo susipažinęs su saugumo taisyklėmis ir turi pagrindinius įgūdžius, individualus saugumo elgesys skirstomas į keturis rėžimus: nežinau - neatlieku; nežinau - atlieku; žinau - neatlieku; žinau - atlieku. Svarbu šiuose rėžimuose išskirti nežinau - atlieku rėžimą, kurio metu išreiškiama darbuotojo iniciatyva dalyvauti kuriant organizacijos saugumo kultūrą, net ir neturint įgūdžių. Taip pat, žinau - neatlieku, kai darbuotojas net ir turėdamas visus įgūdžius ir žinias nesiima veiksmų organizacijos saugumo užtikrinimui. Autorių teigimu tai gali būti pagrįsta asmens įsitikinimų rinkiniu arba asmenine kultūra. Būtent šie veiksniai formuoja žmogaus asmeninį požiūrį ir elgesį informacinio saugumo srityje. Šie veiksniai taip pat gali turėti įtakos tam, ar žmogus būtų pasirengęs priimti ir taikyti kibernetinio saugumo kultūrą (Furnell, 2009). Autorių Ngoqo ir Flowerday (2015) atliktame tyrime atskleidžiamas galimas ryšys tarp informacinio saugumo suvokimo ir informacinio saugumo elgesio ketinimų sudarant žmonių saugumo elgesio profilius. Šiems profiliams priskiriami: žalingas naudojimas, tyčinis naikinimas, naivios klaidos, pavojingi pataisymai, pagrindinė higiena ir sąmoningas užtikrinimas (žr. 8 pav.).



Šaltinis: adaptuota pagal Ngoqo ir Flowerday, 2015

8 pav. Informacijos saugumo elgesio profiliavimo modelis

Tyrimo rezultatai konstatuoja, kad dėl žemo ar vidutinio informacijos saugumo suvokimo lygio, žmonės priima sprendimus dėl saugumo priemonių, remdamiesi vidutiniu informuotumo lygiu ir prastais elgesio

ketinimais. Taigi remiantis šia sistema galima daryti prielaidą, kad nuolatinės pastangos gerinti žmonių supratimą, informuotumą ir sąmoningumą kibernetinio saugumo srityje įtakoja žmogaus elgesį kibernetinėje erdvėje. Jis pereina į „Informuoto užtikrinimo“ kategoriją, kuriai būdingi aukšti sąmoningumo ir saugaus elgesio ketinimų lygiai.

1.5.2 Informuotumo didinimo programos organizacijose

Kibernetinio saugumo informuotumo didinimo pastangos yra skirtos žmogaus elgsenai pakeisti arba sustiprinti gerąją saugumo praktiką (NIST, 2003; Vilkova, Litvishkov ir Shvyrev 2020). Informuotumo didinimo programos gali būti skirtos tam, kad pagerintų konkrečią su saugumu susijusią elgseną apibrėžtoms auditorijoms. Jos taip pat gali būti naudojamos strateginėse pastangose pagerinti saugumo kultūrą. Literatūroje greta sąmoningumo ugdymo vartojami mokymo ir švietimo terminai, kurie nėra tapatūs ir jiems taikomi skirtingi reikalavimai, bei metodai. NIST teigimu informacinio saugumo mokymasis yra tęstinis, jis prasideda sąmoningumo ugdymu, tęsiamas mokymo programomis ir perauga į švietimą. Tsohou, Karyda, Kokolakis ir Kiountouzis (2012) apibrėždami informacinio saugumo sąmoningumą teigia, kad tai yra nuolatinės pastangos, kurių metu auditorijos dėmesys kreipiamas į informacijos saugumą ir jo svarbą, siekiant skatinti į saugumą orientuotą elgesį. Abawajy (2014) informuotumą apie saugumą apibrėžė kaip „vartotojo žinias apie geriausią internetinę praktiką“. Abawajy (2014) teigė, kad saugumo sąmoningumo ugdymo kampanijos daugiausia orientuotos į internetinių galutinių vartotojų informuotumo apie kibernetinį saugumą lygį, o šių informavimo kampanijų sėkmė iš esmės priklauso nuo informacijos pateikimo metodų. NIST specialiame leidinyje 800-16 sąmoningumą apibrėžia kaip: „Sąmoningumo ugdymo pristatymų tikslas yra tiesiog sutelkti dėmesį į saugumą. Sąmoningumo ugdymo pristatymai skirti padėti asmenims atpažinti IT saugumo problemas ir atitinkamai reaguoti“. Tuo tarpu mokymai yra skirti žmonėms įtrauktiems į procesus susijusius su IT sistemomis, kurių metu suteikiami informacinio saugumo pagrindai ir raštingumas (NIST, 2003). Šį mokymų poreikio aspektą pabrėžė ir mokslininkai Vilkova (2020) bei Siponen (2001), jų teigimu, visi žmonės susiję su bet kokiomis IRT, ypač interneto aplinkoje, turi turėti bent tam tikrą informacinio ar kibernetinio saugumo supratimą. Tuo tarpu švietimas, NIST požiūriu, yra skirtas specialistų ir profesionalų rengimui. Furman, Theofanos, Choong ir Stanton (2011) šias tris praktikas apibendrina savo darbe pateikdami išvadą, kad žmonių elgesį susijusį su saugumu galima įtakoti keliant jų sąmoningumą (patraukiant žmonių dėmesį ir sukeliant susidomėjimą), švietimo programomis ir mokymais (suteikiant reikiamą įgūdžių rinkinį).

Informacinio saugumo techninės kontrolės pažeidžiamumų galima išvengti arba sušvelninti naudojant stiprias informacinio saugumo švietimo, mokymo ir sąmoningumo ugdymo (angl. SETA) programas. ENISA teigimu, suvokimas apie riziką ir turimas apsaugos priemones yra pirmoji

informacinių sistemų ir tinklų saugumo gynybos linija (ENISA, 2010). SETA programos padeda ne tik informuoti žmones apie rizikas ir grėsmes, bet ir yra nukreiptos į klaidingus įsitikinimus, įtakojančius žmogaus veiksmus (Kirlappos ir Sasse, 2012). Autoriai Menard ir Shropshire (2016) pateikia SETA programų raidą mokslinėje literatūroje 2 lentelėje.

2 lentelė. SETA programų raida

Programa	Aprašymas	Tikslas	Autorius
Tradicinė SETA	Kursų derinys, seminarai, video, dalomoji medžiaga, nurodymai, priminimai, naujienlaiškiai	Pateikite pradinę informaciją, saugumo problemų suvokimui	Murray, 1991
Pakartotinis SETA įtraukimas	Rekomenduoja vaidmenų atlikimo metodus, atvejų tyrimo analizę arba saugumo vaizdo įrašų peržiūras	Tęstinis SETA siekiant įtakoti darbuotojų elgesį	Mitnick ir Simon, 2002
Internetinis mokymas	Internetinis mokymas. Visiems dalyviams pristatoma tekstinių modulių serija. Po kiekvieno modulio pateikiamas klausimynas.	Kad būtų laikomasi nustatytų saugumo mokymo reikalavimų rangovams.	Jones ir Pardehava, 200
"Hipermedija"	Mokymosi tekstu ir daugialypės terpės derinys, skirtas darbuotojų švietimui apie saugumo praktiką	Pagerinkite darbuotojų mokymąsi apie saugumą pateikdami informaciją turtingesniu formatu	Shaw ir kt., 2009
Motyvacinė SETA	Tradicinė tekstu ir vaizdo įrašu pagrįsta SETA programa su įterptomis motyvacinėmis manipuliacijomis	Nustatyti, ar darbuotojai gali būti iš esmės motyvuoti dalyvauti informavimo programoje	Menard, 2015

Šaltinis: adaptuota pagal Menard ir Shropshire, 2016

Remiantis lentelėje pateikta informacija galima įžvelgti dvi SETA programos vystymo kryptis: pateikimo formato dalyviams patrauklumas ir dalyvio įsitraukimo didinimas. Bada, Sasse ir Nurse (2019) išanalizavo didelę dalį kibernetinio saugumo sąmoningumo ugdymo kampanijų siekiant identifikuoti kampanijos sėkmės ar nesėkmės priežastis. Tyrėjai pateikė šiuos veiksnius lemiančius kibernetinio saugumo informavimo kampanijų sėkmę: saugumo ugdymo programa turi būti gerai parengta bei veiksminga ir tikslinga, taip pat ji turėtų būti lanksti, kad ją priimtų įvairios kultūros. Šia

tematika taip pat dirbo ir Reid ir van Niekerk (2014). Autoriai atliktame tyrime siekė sukurti standartinį metodą struktūrizuojant saugumo kultūrą skatinančią švietimo programą. Pateikiamos tyrimo išvados konstatuoja, kad mokomosios medžiagos platinimo būdas turi įtakos tam, kaip/ar informacija pasiekė tikslinę grupę; mokytojų įtraukimas į kibernetinio saugumo kampaniją yra esminis; kampanija turi būti kuriama atsižvelgiant į tikslinės auditorijos amžių, veiklos sritį, pateikimo formatą. Galiausiai kampanijos turinys turi būti tinkamas ir nuolat tobulinamas. Dan Blum (2020) teigimu kampaniją organizuojantys specialistai turi pritaikyti turinį ir taktiką tikslinei auditorijai remiantis šiomis darbuotojų elgesio grupėmis: motyvuoti ir galintys atlikti darbą, motyvuoti, bet negalintys, galintys, bet nemotyvuoti, ir tie, kurie neturi nei motyvacijos, nei gebėjimų. Taigi efektyvi sąmoningumo ugdymo programa turi remtis elgesio mokslu, daugialypės terpės turinio kūrimu ir dėmesio valdymu. Tačiau Menard ir Shropshire (2016) teigia, kad dauguma SETA programų kuriamos taip, kad būtų pristatytos kuo platesnei auditorijai ir naudojamos kuo ilgiau. Tai apriboja SETA programos pritaikymą darbuotojų kasdienėje veikloje ir motyvaciją aktyviai įsitraukti į saugumo kultūros vystymą.

Informacinio saugumo švietimo, mokymo ir sąmoningumo ugdymo programos ne tik turi suteikti informaciją tikslinei auditorijai, bet ir apimti tam tikrus vertinimo kriterijus (Da Veiga, 2015). Tsohou (2012) pateikia trijų dimensijų saugumo sąmoningumo ir mokymo programą, kurią sudaro: saugesnio elgesio skatinimas, tikslinės informavimo kampanijos ir saugumo kultūros gerinimas. Autorių teigimu esminis šios programos aspektas yra nuolatinis vertinimas ir tobulinamas. Kruger ir Kearney (2006) taip pat pabrėžia sąmoningumo didinimo kampanijos poveikio įvertinimo svarbą. Siekdami nustatyti visuotinį organizacijos informuotumo lygį, jie identifikavo vertinimo aspektų rinkinį, susijusį su tuo, ką vartotojai žino (žinios), galvoja (požiūris) ir daro (elgesys).Tačiau A. Da Veiga (2015) teigimu nė vienas iš mokslinėje literatūroje pateikiamų saugumo sąmoningumo ir mokymo metodų yra holistinis, apimantis formalius etapus, įtraukiančius sąmoningumo ir mokymo efektyvumo įvertinimą informacijos saugumo kultūros kontekste, naudojant patvirtintą vertinimo priemonę. To pasekoje autorius sukūrė ir pateikė informacinio saugumo mokymo ir sąmoningumo metodą (ISTAAP), kuris gali būti naudojamas informacinio saugumo kutūros žmogaus faktoriaus riziką. Šiame modelyje yra išskiriami keturi etapai. Pirmajame etape atliekamas efektyvumo vertinimas. Informacinės saugumo kultūros lygis vertinamas naudojant ISCA metodą (ISCA) (Da Veiga ir Martins, 2015), kuris pateikia pradinį poreikių įvertinimą ir tampa pagrindu lyginamajai analizei ateityje. ISCA klausimyną sudaro devyni konstruktai: informacinio turto valdymas, informacinio saugumo valdymas, pokyčių valdymas, sistemos naudotojų valdymas, informacinio saugumo politikos, informacinio saugumo programos, pasitikėjimo ir informacinio saugumo lyderystė. Klausimai šiais aspektais atsakomi Likerto skalėje. Sekančiame etape, planavimas ir tikslai, informacinio saugumo mokymo ir informavimo tikslai yra sudaromi remiantis organizacijos ir informacinio saugumo strategijomis, taip pat informacinio saugumo politika ir reguliavimo reikalavimais. Trečiajame, sąmoningumo ir mokymų vystymo etape pasitelkiamos įvairios

technikos ir metodai pateikti informaciją. ISCA apklausos rezultatai naudojami apibrėžiant, kokią mokymo ir informavimo medžiagą bei turinį kurti. Paskutiniame etape, atliekamas tikslinis programos įgyvendinimas. ISCA rezultatai pateikia empirinius duomenis su labiausiai pageidaujamais ir veiksmingiausias mokymo ir informavimo metodais kiekvienai suinteresuotųjų šalių grupei organizacijoje. Taigi bet kuriame saugumo sąmoningumo ugdymo ir mokymo plane svarbiausiu žingsniu galima laikyti žmonių rizikos suvokimo vertinimą, kuris tampa pagrindu individualizuotai mokymo programai. Taip pat galima išskirti šiuos pagrindinius programų elementus orientuotus į žmogaus požiūrio ir elgesio keitimą:

- Programos turi būti kruopščiai suplanuotos naudojant formalizuotą metodiką, kurioje atsižvelgiama į aspektus, susijusius tiek su besimokančiaisiais, tiek su aplinka, kurioje jie dirba.
- Programos turėtų būti sukurtos atsižvelgiant į aiškiai apibrėžtą rezultatą arba tikslą.
- Įvertinimas arba vertinimas yra labai svarbus mokymosi programos sėkmei. Besimokantieji turi gauti grįžtamąjį ryšį.
- Besimokantieji turi būti ne tik mokomi, kaip elgtis konkrečioje situacijoje, bet ir kodėl jie turėtų taip elgtis.
- Mokymosi medžiaga turėtų būti pritaikyta individualiai.

1.5.3 Informuotumo didinimo programos švietimo įstaigose

Informacinio saugumo informuotumo didinimo, mokymo ir švietimo programų integravimas į darželių, mokyklų, kolegijų ir universitetų mokymo planus sumažintų su kibernetiniu saugumu susijusias rizikas (Tonye, 2019) ilgalaikėje perspektyvoje. Švietimo sistema turi būti laikoma pamatine kibernetinio saugumo kultūros formavimo priemone. Ši tematika analizuota Tirumala, Sarrafzadeh ir Pang (2016), Zwilling, Lesjak, Natek, Phusavat, ir Anussornnitisarn (2019), Rahman, Sairi, Zizi ir Khalid (2020) darbuose. Al Shamsi (2019) išskiria pagrindines temas ir jų aspektus kibernetinio sąmoningumo programoje skirtoje mokykloms (žr. 3 lent.).

3 lentelė. Kibernetinio informuotumo didinimo mokyklų programose temos ir aspektai

Pagrindinės temos	Pagrindiniai aspektai
Interneto pavojai su kuriais gali susidurti mokiniai	O1: elektroninės patyčios O2: slaptažodžio vagystė O3: tapatybės vagystė O4: sukčiavimas internetu O5: privatumo pažeidimas

Pagrindinės temos	Pagrindiniai aspektai
Sąmoningumo programos turinys	C1: Interneto sauga C2: Kibernetinės patyčios C3: Tapatybės vagystė C4: Sukčiavimas internete C5: Privatumas C6: Slaptažodis C7: Saugios svetainės C8: Internetiniai nepažįstamieji C9: Saugumas
Kibernetinio saugumo sąmoningumo programos efektyvumas	E1: Labai efektyvus E2: Teigiamai veikia elgesį internete
Poveikis mokiniams	EF1: Apsaugo savo asmeninę informaciją EF2: Naudoja stiprius slaptažodžius EF3: Tinkamai reaguoja į įvairius incidentus internete EF4: Būna atsargesni žaisdami internetinius žaidimus EF5: Informuoja savo tėvus, jei internete jie jaučiasi nepatogiai EF6: Žino apie sukčiavimo el. laiškus ir pranešimus EF7: Neatsako nepažįstamiesiems internete

Šaltinis: adaptuota pagal Al Shamsi, 2019

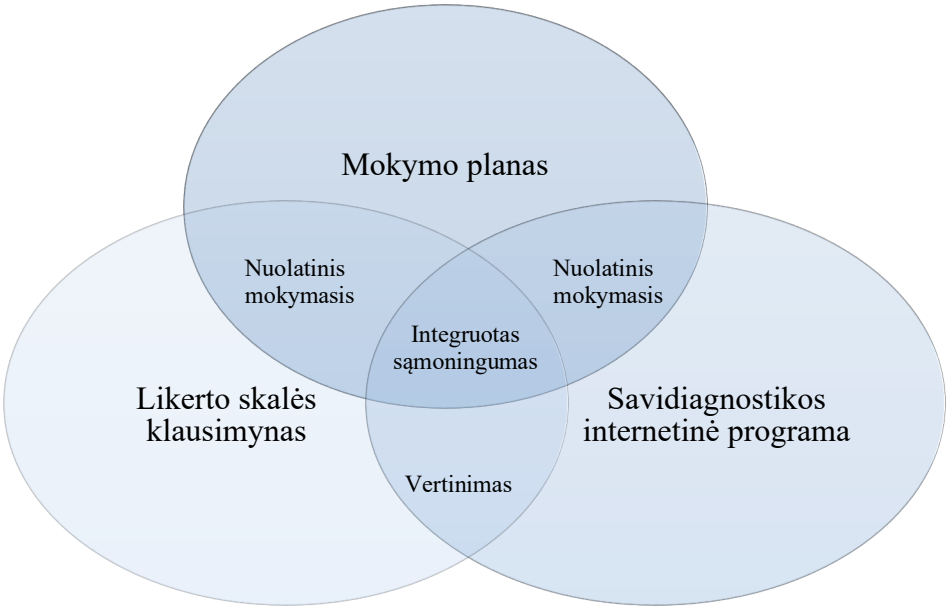
Šiuos aspektus ir grėsmes savo darbuose taip pat pabrėžia autoriai Valcke, De Wever, Van Keer, Schellens (2011), Livingstone, Mascheroni ir Staksrud, (2015), Cabello-Hutt, Cabello and Magdalena Claro (2017), Bőthe, Tóth-Király, Zsila, Demetrovics, Griffiths ir Orosz (2017), Manap, Abdul Rahim, Taji, (2015). Jungtinės Karalystės Interneto saugos tarnyba šias grėsmes išplečia personalizuodami ir struktūruodami informuotumo didinimo aspektus atsižvelgiant į vaikų amžių. Tarnybos išleistame informaciniame leidinyje „Švietimas susietam pasauliui – 2020 m. leidimas“ išskiriami šie kibernetinio saugumo aspektai:

- Internetinis Aš įvaizdis ir tapatybė
- Internetiniai santykiai
- Internetinė reputacija
- Internetinės patyčios
- Informacijos valdymas internete
- Sveikata, gerovė ir gyvenimo būdas

- Privatumas ir saugumas
- Intelektinė nuosavybė
- Kibernetinės grėsmės

Visos šios temos yra integruojamos į Jungtinės Karalystės nacionalinę ugdymo programą atsižvelgiant į kibernetinio saugumo daugiadisciplinišKumą.

Antunes ir kt. (2021) savo darbe pristato integruotą kibernetinio saugumo ir kibernetinio sąmoningumo strategiją mokyklose, kuri koreliuoja su Al Shamsi (2019) programos aspektais, tačiau papildo Al Shamsi tyrimo ribotumą - nuolatinį saugumo sąmoningumo vertinimą. Strategiją sudaro trys pagrindiniai komponentai: 1) požiūrio į kibernetinį saugumą ir elgesio įvertinimo, 2) savidiagnostikos ir 3) mokymo/si veiklos. (žr. 9 pav.)



Šaltinis: adaptuota pagal Atunes ir kt., 2021

9 pav. Kibernetinio saugumo informuotumo didinimo metodologija mokykloms

Požiūrio į kibernetinį saugumą ir elgesio vertinimui buvo sukurti du nauji klausimynai, skirti įvertinti mokinių rizikingą požiūrį (CsA-S) (žr. 1 priedą) ir elgesį (CsB-S) (žr. 2 priedą), kai jie yra prisijungę prie interneto tiek laisvalaikio metu, tiek mokyklos aplinkoje. Atsakymai pateikiami naudojantis Likerto skale. Antroji dalis apima savidiagnostikos internetinę programą. Bendra metodika, priimta kuriant savidiagnostikos žiniatinklio programą:

1. Pagrindinės sritys: globali CSIRT taksonomija (10 sričių).
2. Duomenų bazės paruošimas: kelių pasirinkimų klausimai.
3. Grįžtamojo ryšio tekstas: pateikiama papildoma informacija pasirinkus neteisingą atsakymą.
4. Klausimyno paruošimas: klausimų skaičiaus, pasirinkimo kriterijų ir grįžtamojo ryšio pateikimo maketavimas.

5. Internetinė versija: galutinė versija prieinama internetiniame puslapyje.

Autorių teigimu savidiagnostikos programos žaidybinimas turi būti laikomas kitu etapu vystant šią metodiką. Sukūrus žaidybinę mobiliąją versiją su „atlygio“ mechanizmais, būtų pateikiamas nuolatinis ir platus kibernetinio saugumo savidiagnostikos programos naudojimas. Trečiasis elementas, pamokos planas, buvo sudarytas įtraukiant tarptautines gaires, specifiškai ENISA informacinių incidentų klasifikacijos taksonomijos ataskaitą ir ENISA informacijos saugumo informuotumo didinimo medžiagą. Pamoka pradedama instruktažu apie dalyką, po to pateikiamas temų sąrašas, suskirstytas į tris pagrindines grupes:

1. Bendrosios problemos apimančios žalingą turinį, kenkėjišką kodą, socialinę inžineriją, dalijimąsi informacija, kibernetines patyčias, stebėjimą;
2. Techniniai sprendimai - antivirusinės, programos kovai su kenkėjiškomis programomis, ugniasienės, programų atnaujinimas;
3. Kitos temos - blokavimo prietaisai, slaptažodžiai, socialiniai tinklai, keičiamos laikmenos, melagienos, incidentų valdymas.

Po pamokos vyksta diskusijos išmoktoms temoms aptarti. Pateikta strategija ir metodika autorių teigimu, taip pat pritaikoma skirtinguose kontekstuose. Analizuojamos metodikos ir strategijos gali būti integruotos į švietimo sistemą siekiant paruošti visuomenę naujausioms informacijos saugumo grėsmėms ir keliant jos informuotumą saugumo tematika nuolat besivystančioje kibernetinėje erdvėje.

Plėtojant kibernetinio saugumo mokymo programas siekiama paspartinti kibernetinio saugumo įgūdžių ugdymą ir informuotumą visoje švietimo sistemoje. Mokymo programos turėtų būti integruotos, daugiadisciplininės ir apimti ne tik techninius, bet ir netechninius kibernetinio saugumo įgūdžius ir temas, tokias kaip skaitmeninis raštingumas, viešoji politika, teisė, valdymas, ekonomika, rizikos valdymas, etika, socialiniai mokslai ir tarptautiniai santykiai. Pradinėse ir vidurinėse mokyklose turėtų būti parengtos specialios kibernetinio saugumo programos. Taip pat, ugdymo programose turėtų būti skatinamas informuotumas apie karjeros galimybes kibernetinio saugumo srityje ir skatinamas domėjimasis jomis.

2. KIBERNETINIO SAUGUMO KULTŪROS PLĖTROS IKIMOKYKLINIO IR BENDROJO UGDYMO ĮSTAIGŲ PROGRAMŲ PAGRINDU TYRIMAS

2.1 Empirinio tyrimo metodologija

Tyrimo metodika ir organizavimas. Siekiant atskleisti kibernetinio saugumo kultūros vystymą ikimokyklinio ir bendrojo ugdymo programų pagrindu pasirinktas kombinuotas tyrimas.

Tyrimo tikslas. Išanalizuoti kibernetinio saugumo kultūros plėtrą švietimo srityje ikimokyklinio ir bendrojo ugdymo programų pagrindu ir pateikti programų plėtojimo kryptis.

Tyrimo hipotezės:

- Lietuvos ikimokyklinio ir bendrojo ugdymo programų koncepcija įtakoja saugumo kultūros plėtojimo problematiką švietimo sistemoje.
- Lietuvos kibernetinio saugumo teisinė bazė lemia kibernetinio saugumo kultūros plėtojimo problematiką švietimo sistemoje.

Tyrimo uždaviniai:

1. Atlikti kokybinį ekspertų nuomonės tyrimą, kurio pagrindu galima vertinti kibernetinio saugumo kultūros aspektą ikimokyklinio ir bendrojo ugdymo programose ir nustatyti kibernetinio saugumo kultūros plėtojimo kryptis.
2. Išanalizuoti Jungtinės Karalystės nacionalinę informatikos ugdymo programą.
3. Atlikti Lietuvos Kibernetinio saugumo įstatymo ir Kibernetinio saugumo strategijos poveikio vertinimą kibernetinio saugumo kultūros plėtojimui.
4. Atlikti vertinimą ir lyginimą parengiant kibernetinės kultūros plėtojimo kryptis ikimokyklinio ir bendrojo ugdymo programų pagrindu.

Tyrimo metodai. Tyrimui atlikti bus naudojami tokie metodai:

1. Mokslinės literatūros analizė.
2. Dokumentų kokybinio turinio (angl. Content) analizė.
3. Pusiau struktūrizuotas interviu. Kokybiniam tyrimui pasirinktas pusiau struktūrizuotas ekspertinis interviu.
4. Lyginamoji gautų duomenų analizė. Siekiant palyginti gautus duomenis iš mokslinės literatūros ir dokumentų turinio (angl. Content) analizių ir kokybinio pusiau struktūrizuoto ekspertinio interviu naudojama lyginamoji analizė.

Tyrimo reprezentatyvumas. Tyrimo imties nustatymui naudojama netikimybinė tikslinė atranka. Šalis, kuri nagrinėjama kibernetinio saugumo kultūros vystyma pagal šiuos kriterijus:

a. Valstybės švietimo sistema yra įtraukta į šalies nacionalinę kibernetinę saugumo strategiją.

b. Valstybės švietimo strategija įtraukia ir eskaluoja kibernetinio saugumo kultūros plėtros klausimus.

c. Valstybė yra pirmoji Europoje pagal ITU GCI.

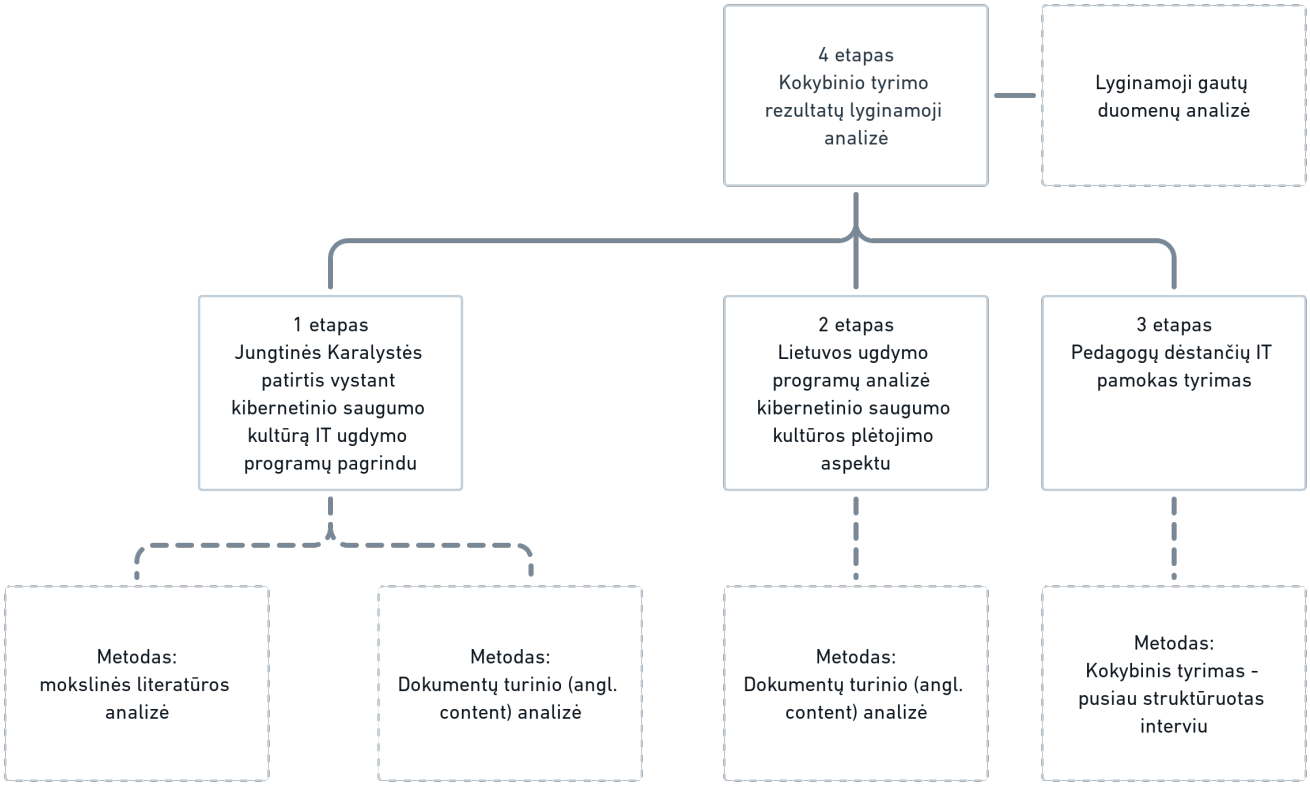
Kokybinio pusiau struktūrizuoto ekspertinio interviu respondentai atrenkami pagal šiuos kriterijus:

a. IT specializacijos pedagogai.

b. Pedagogai turi turėti ne mažiau nei trijų metų darbo patirtį.

Kibernetinės kultūros plėtojimo kryptims ugdymo programose nustatyti buvo vertinama, lyginama ir analizuojama IT ugdymo programa. Ši programa buvo pasirinkta remiantis literatūros analize, kuri pateikė IT pamokas kaip pagrindinį kibernetinio saugumo informuotumo didinimo komunikacijos kanalą.

Tyrimo loginis planas. Planas pateikiamas dešimtame paveiksle.



10 pav. Tyrimo loginis planas

1 etapas. Jungtinės Karalystės patirtis vystant kibernetinio saugumo kultūrą. Šiame etape išsamiai atliekama literatūros ir dokumentų turinio (angl. Content) analizė, kuri yra susijusi su Jungtinės Karalystės praktika rengiant nacionalinę kompiuterijos ugdymo programą. Moksliniai straipsniai plačiau nagrinėjami teorinėje dalyje.

2 etapas. Lietuvos ugdymo programų analizė kibernetinio saugumo kultūros plėtojimo aspektu. Šiame etape analizuojamos ikimokyklinio ugdymo ir bendrojo IT ugdymo programos, švietimo sistemos teisinė bazė siekiant įvertinti kibernetinio saugumo kultūros plėtojimą.

3 etapas. Pedagogų atsakingų už kibernetinio saugumo švietimą ugdymo įstaigose tyrimas. Šiame etape atliekamas kokybinis tyrimas pusiau struktūrizuotas ekspertinis interviu. Šiuo tyrimu bus siekiama išsiaiškinti kokie veiksniai įtakoja kibernetinio saugumo kultūros plėtrą ugdymo programose, su kokiomis problemomis yra susiduriama.

4 etapas. Kokybinio tyrimo rezultatų lyginamoji analizė. Šiame etape bus siekiama palyginti Jungtinės Karalystės ir Lietuvos ikimokyklinio ir bendrojo ugdymo IT programų konceptus. Iš gautų rezultatų formuojamos rekomendacijos, kurios bus tinkamos ir pritaikomos Lietuvos ikimokyklinio ir bendrojo ugdymo programose.

2.2 Kokybinio tyrimo duomenų analizė

Kokybinio tyrimo organizavimas. Kibernetinio saugumo kultūros vystymo aspektai ir priemonės analizuojami ir vertinami ekspertiniame lygyje. Šios tematikos specifiškumas ir visuomenės informuotumo trūkumas lėmė kokybinio tyrimo pasirinkimą. Siekiant kuo detaliau reflektuoti ugdymo programų turinį šiame kontekste, tyrimui buvo pakviesti IT specializacijos pedagogai turintys daugiau nei 3 metų darbo patirtį šioje srityje. Sudarant eksperimentinio tyrimo imtį vadovautasi Baležentis, A. ir Žalimaitė, M. (2011) atlikto tyrimo išvadomis, kurios konstatavo, kad pakankamas ekspertų skaičius vertinime yra 7 asmenys. Tyrimas atliktas 2022 m. sausio 26 – vasario 12 dienomis. Kokybinio tyrimo etapai pateikiami 4 lentelėje.

4 lentelė. Kokybinio tyrimo eiga

Etapas	**Etapo veikla**	**Etapo tikslas**
Tyrimo eigos sudarymas	Parenkamas tyrimo metodas, paruošiami su tyrimo veikla susiję dokumentai, nustatomi vertinimo kriterijai bei tyrimo apribojimai.	Sudaryta tyrimo koncepcija, tyrimo pristatymas respondentams ir interviu klausimai.
Ekspertų atranka	Paruoštas tyrimo pristatymas ir kvietimas išsiunčiamas 7 IT pedagogams elektroniniu paštu.	Gautas IT pedagogo sutikimas dalyvauti tyrime.
Duomenų rinkimas	Su pedagogais susisiekiama jų prašomu būdu ir pateikiami sudaryti interviu klausimai.	Surinkta IT pedagogų nuomonė interviu klausimų gairėmis.
Duomenų analizė	Gauta informacija analizuojama, pašalinamos galimos klaidos.	Surinkta informacija vertinanti kibernetinio saugumo kultūros plėtojimo aspektus ikimokyklinio ir bendrojo IT ugdymo programų pagrindu.

Etapas	Etapo veikla	Etapo tikslas
Rezultatų interpretavimas	Informacija yra apibendrinama.	Suformuota bendra ekspertų nuomonė interviu pateiktų klausimų pagrindu.
Rezultatų ir išvadų pateikimas	Ruošiamos tyrimo išvados ir rezultatai.	Gautos tyrimo išvados yra įtraukiamos į lyginamąją analizę.

Tyrimo etika. Tyrimas buvo atliktas remiantis šiais principais (Židžiūnaitė, 2011) :

- Geranoriškumo – užtikrintas laisvanoriškas respondentų dalyvavimas jų pasirinktu bendravimo būdu.
- Pagarbos asmens orumui – informacija pateikiama interviu metu yra neutrali, objektyvi ir orientuota į atliekamo tyrimo specifiką.
- Teisingumo – tyrimo respondentai parenkami pagal konkrečius kriterijus susijusius su magistrinio darbo tyrimo objektu ir neįtraukia asmeninės informacijos, kuri leistų atpažinti konkretų asmenį.
- Teisės gauti informaciją – respondentams išsiųstas tyrimo pristatymas.

Tyrimo dalyvių interviu struktūra. Respondentams pateikiami šie 10 klausimų:

1. Kaip Jūs suprantate kibernetinio saugumo kultūrą?
2. Jūsų nuomone, ar pagrindinio ugdymo informacinių technologijų bendroji programa kelia mokinių sąmoningumą kibernetinio saugumo srityje?
3. Jūsų nuomone, ar pagrindinio ugdymo informacinių technologijų ugdymo programa atitinka mokinių gebėjimus?
4. Jūsų nuomone, ar pagrindinio ugdymo informacinių technologijų programa ugdo bendrąsias ir esmines dalykines kompetencijas?
5. Jūsų nuomone, kas turėtų būti įtraukta ar išbraukta iš pagrindinio ugdymo informacinių technologijų ugdymo programos veiklos sričių?
6. Jūsų nuomone, ar informacinių technologijų mokytojo kompetencijos yra keliamos sistemingai?
7. Jūsų nuomone, ar ikimokyklinis ugdymas turėtų įtraukti saugaus interneto pagrindus?
8. Jūsų nuomone, ar pradinio ugdymo bendroji programa turėtų įtraukti saugaus naudojimo internete pagrindus?
9. Jūsų nuomone, kokios pagrindinio ugdymo programos turėtų integruoti kibernetinio saugumo pagrindus?
10. Ar turėtumėte papildomų pastabų ir pasiūlymų?

Tyrimo dalyvių apklausos analizė. Respondentų atsakymai į pateiktus interviu klausimus:

1. Kaip Jūs suprantate kibernetinio saugumo kultūrą?

Visų respondentų atsakymai buvo lakoniški. Jie atskleidė, kad kibernetinio saugumo žinios apsiriboja pagrindais, kurie įtraukia saugių slaptažodžių naudojimą, atsargų gautų nuorodų vertinimą ir neapibrėžtą saugų naršymą internete:

< Gebėti susikurti stiprius, saugius slaptažodžius; žinoti, kaip saugiai naršyti internete; nespausti įtartinų nuorodų ir kt.>

<...Saugiai ir atsakingai elgtis virtualioje erdvėje, naudoti saugius slaptažodžius.>

Tai rodo kompetencijų kėlimo poreikį siekiant juos įgalinti plėtoti saugumo kultūrą tiek mokyklos, tiek klasės lygmeniu.

2. Jūsų nuomone, ar pagrindinio ugdymo informacinių technologijų bendroji programa kelia mokinių sąmoningumą kibernetinio saugumo srityje?

Atsakymai šiuo klausimu išsiskyrė. Trys respondentai teigė, kad programa kelia sąmoningumą, tačiau nepakankamai. Likę pedagogai tvirtino, kad programa nėra pakankamai išplėtota šiuo aspektu. Tačiau visi vienareikšmiškai išskyrė šias problemines sritis: per mažas skiriamų pamokų kiekis ir informacijos trūkumas:

<... Yra keliamas sąmoningumas kibernetinio saugomu srityje, tačiau informacijos suteikiama nepakankamai...>

<... Nelabai, nes tai temai skiriama labai mažai pamokų...>

3. Jūsų nuomone, ar pagrindinio ugdymo informacinių technologijų ugdymo programa atitinka mokinių gebėjimus?

Visi respondentai sutiko, kad programa iš dalies atitinka mokinių gebėjimus, tačiau pabrėžė, kad daugeliu atveju mokinių informacinių technologijų įgūdžiai yra pažengę ir lenkia ugdymo programos turinį tam tikrai amžiaus grupei:

<... Iš dalies atitinka, nes nemažai mokinių domisi informacinėmis technologijomis ir yra pažengę į priekį...>

4. Jūsų nuomone, ar pagrindinio ugdymo informacinių technologijų programa ugdo bendrąsias ir esmines dalykines kompetencijas?

Šiuo klausimu 6 respondentai teigė, kad programa vysto esmines dalykines kompetencijas. Vienas iš jų pabrėžė reikalingas plėtojimo sritis:

<...Mano nuomone stengiamasi, bet į ugdymo programą būtų galima įtraukti dar daugiau praktinių darbų ir informacijos...>

Du respondentai atsakė, kad kompetencijos nėra vystomos ir programa turi būti iš esmės atnaujinta.

5. Jūsų nuomone, kas turėtų būti įtraukta ar išbraukta iš pagrindinio ugdymo informacinių technologijų ugdymo programos veiklos sričių?

Visi pedagogai vienareikšmiškai sutiko, kad programa turi būti pildoma išskiriant šias sritis:

- ugdymo priemonės turėtų atliepti naujausias technologijas ir būti taikomos praktiniuose užsiėmimuose;
- tiek informacinių technologijų, tiek kitos ugdymo programos turėtų nuosekliai integruoti saugumo kultūrą naudojantis IT;
- įtraukti daugiau praktinių užduočių, kurios leistų mokiniams vystyti įvairiapusišką suvokimą.

6. Jūsų nuomone, ar informacinių technologijų mokytojo kompetencijos yra keliamos sistemingai?

Keturi respondentai atsakė teigiamai, o likę keturi pabrėžė informacijos trūkumą dėl pačios sistemos, kuria grindžiamas kompetencijų kėlimas:

<...Keliamos nesistemingai, kai kurie metodai ir mokymo programos dėstomos pagal senas metodikas...>

7. Jūsų nuomone, ar ikimokyklinis ugdymas turėtų įtraukti saugaus interneto pagrindus?

Visi 7 respondentai interviu metu vienareikšmiškai sutiko, kad ikimokyklinis ugdymas turi įtraukti vaiko raidą atitinkančius informacinių technologijų pagrindus:

<...Taip turėtų supažindinti bent su minimaliais pagrindais, nes dauguma vaikų yra susipažinę ir naudojasi technologijomis...>

8. Jūsų nuomone, ar pradinio ugdymo bendroji programa turėtų įtraukti saugaus naudojimo internete pagrindus?

Interviu metu informacinių technologijų mokytojai taip pat pabrėžė IT ugdymo svarbą pradinėse klasėse ir vienareikšmiškai sutiko su IT srities įtraukimu į pradinį ugdymą:

< Būtinai, nes pradinių klasių mokiniai nemažai internete naršo, ieško informacijos, žaidžia, siunčia programas. Būtina mokyti šių temų.>

<Turėtų įtraukti, technologijomis naudojamasi kiekvieną dieną ypatingai šiais laikais, tai aktualu net ir pradinių klasių moksleiviams, saugaus naudojimo internete pagrindai turėtų būti dėstomi, siekiant išvengti kibernetinių grėsmių.>

9. Jūsų nuomone, kokios pagrindinio ugdymo programos turėtų integruoti kibernetinio saugumo pagrindus?

Pedagogai nurodė šias programas, kurios gali integruoti kibernetinio saugumo problematiką: informacinės technologijos, bendrųjų kompetencijų ir gyvenimo įgūdžių ugdymas, technologijos.

10. Ar turėtumėte papildomų pastabų ir pasiūlymų?

Papildomų pastabų ar pasiūlymų nebuvo pateikta.

Interviu metu gauti duomenys atkleidė šiuos kibernetinio saugumo kultūros plėtojimo kryptis:

- Saugaus interneto naudojimo pagrindai turi būti įtraukti į ikimokyklinio ir pradinio ugdymo programas.
- IT pedagogų kompetencijos turi būti keliamos nuosekliai, taikant konsoliduotą sistemą Lietuvos lygiu atsižvelgiant į sparčius technologinius pokyčius pasaulyje.

- Ugdymo programos turi apibrėžti bendrąsias ugdomas mokinių kompetencijas IT srityje atsižvelgiant ir įvertinant IT įtaką vaikų kasdieniame gyvenime.
- IT ugdymo programos turi būti nuolatos keičiamos ir atnaujinamos siekiant užtikrinti mokinių gaunamų kompetencijų konkurencingumą pasaulinėje darbo rinkoje ir visuomenėje.
- IT pamokos turi labiau plėtoti praktinį informacijos taikymą.

3. KIBERNETINIO SAUGUMO KULTŪROS PLĖTOJIMO VERTINIMAS UGDYMO PROGRAMOSE LYGINAMUOJU PAGRINDU

Nacionalinėje kibernetinio saugumo ataskaitoje (2020) teigiama, kad „pagrindiniai kibernetinio saugumo iššūkiai yra susiję su žinomų pažeidžiamumų išnaudojimu, paviršutiniškai ar nepakankamai tiksliai vertinamomis informacijos saugumo rizikomis, per lėtai gerėjančia interneto svetainių būkle, stringančiu kibernetinio saugumo reikalavimų įgyvendinimu, kibernetinio saugumo higienos trūkumu, nekritiškai vertinama informacija socialiniuose tinkluose“. Krašto Apsaugos Ministerijos pateiktos kibernetinių incidentų priežastys didžiąja dalimi gali būti apibendrintos žmogiškojo faktoriaus problematika. Taigi visuomenės kibernetinio saugumo informuotumo kėlimas yra pagrindinė kibernetinių incidentų užkardymo priemonė. Nacionalinio kibernetinio saugumo reglamentavimas ir politikos nuostatos turi formuoti informuotumo didinimo, mokymų ir švietimo programas. Švietimo ugdymo programos turi būti laikomos prioritetine sritimi, kuri turi užtikrinti kibernetinį atsparumą ilgalaikėje perspektyvoje.

3.1 Informuotumo didinimo aspektas Kibernetinio saugumo įstatyme

Lietuvos Respublikos kibernetinio saugumo įstatymo pirmasis straipsnis nustato kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijas, šių institucijų įgaliojimus kibernetinio saugumo srityje, kibernetinio saugumo subjektų pareigas, tarpinstitucinį bendradarbiavimą, ryšių ir informacinių sistemų spragų paieškos ir pranešimo apie jas ir kibernetinius incidentus pagrindus, taip pat nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas ir įgaliojimus (Lietuvos Respublikos Kibernetinio saugumo įstatymas, 2018). Šiame straipsnyje svarbu pabrėžti tarpinstitucinį bendradarbiavimą, kurio pagrindu kibernetinis saugumas ir jo kultūros vystymas turi būti traktuojami kaip kompleksinė problema. Kompleksinės problemos suvokiamos kaip sudėtingi socialiniai ir ekonominiai iššūkiai, kurių sprendimui reikalingos novatoriškos priemonės ir daugiau nei kelių ministerijų susitelkimas (Jurkonienė, 2017). Siekiant aiškiai apibrėžti kibernetinio saugumo problematiką ir bendradarbiavimo poreikį, vienareikšmė terminologija yra laikoma to pagrindu. Įstatymo 2 straipsnis pateikia pagrindines sąvokas. Kibernetinės erdvė apibrėžiama kaip „aplinka, kurią sudaro kompiuteriai ir kita IRT įranga ir juose sukuriama ir (arba) jais perduodama elektroninė informacija“ (Kibernetinio saugumo įstatymas, 2018). Remiantis atlikta literatūrine analize galima teigti, kad šis kibernetinės erdvės apibrėžimas remiasi fiziniu ir loginiu aspektais, neįtraukiant kibernetinės erdvės socialinio aspekto. Tai gali apriboti kibernetinio saugumo vystymo kryptis, ypač kultūros plėtojimo tematika. Kibernetinio saugumo sąvoka, neišskiria kibernetinio saugumo iš

informacinio saugumo konteksto ir remiasi IRT saugumo užtikrinimu. Rizika taip pat vertinama tik poveikiu ryšių ir informacinių sistemų saugumui. Tuo tarpu kibernetinio saugumo sąvoka yra labiau išplėtota. Ji įtraukia ne tik technines, bet ir „visumą teisinių, informacijos sklaidos, organizacinių priemonių, kuriomis siekiama užtikrinti kibernetinį atsparumą“ (Kibernetinio saugumo įstatymas, 2018). Taip pat, šiame apibrėžime įtraukiamas ir ekonominis aspektas – paslaugų teikimas. Tačiau socialinė sąveika, pačios kibernetinės erdvės ir joje veikiančių interneto vartotojų saugumas lieka už šio apibrėžimo ribų. Dezinformacija, kibernetinės patyčios, tapatybės vagystės ir kitos su kibernetine erdve susijusios grėsmės nėra įtraukiamos. Taigi galima daryti išvadą, kad įstatyme pateikiamos sąvokos neatspindi kibernetinio saugumo daugiadisciplinišKumo ir formuoja izoliuotą tik į IRT orientuotą kibernetinio saugumo sampratą. To pasekoje, tarpinstitucinis bendradarbiavimas ir kompleksinis kibernetinio saugumo problemos sprendimas stipriai apribojamas nacionaliniu lygiu.

Kibernetinio saugumo įstatyme (2018) pateikiamos kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos ir subjektai, kurie atlikdami jiems priskirtas funkcijas ir pareigas užtikrina kibernetinio atsparumo didinimą šalyje. 5 lentelėje pateikiamos institucijos ir subjektai bei jiems įstatymo nuostatomis priskiriamos funkcijos ir pareigos visuomenės informuotumo didinimo srityje.

5 lentelė. Institucijos ir jų funkcijos informuotumo didinimo aspektu Kibernetinio saugumo įstatyme (2018)

Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos ir subjektai	**Informuotumo didinimo visuomenėje aspektas**
Vyriausybė	4 straipsnis. 1. Kibernetinio saugumo politikos strateginius tikslus, pažangos uždavinius ir jiems pasiekti būtinas priemones nustato Lietuvos Respublikos Vyriausybė.
Krašto apsaugos ministerija	6 straipsnis. 1. rengia kibernetinio saugumo politikos pažangos uždavinius įgyvendinančias nacionalines plėtros programas, organizuoja, koordinuoja ir kontroliuoja jų įgyvendinimą.
Kibernetinio saugumo taryba	7 straipsnis. 4. 1) teikia kibernetinio saugumo dalyviams pasiūlymus dėl kibernetinio saugumo prioritetų, plėtros krypčių, siektinų rezultatų ir jų įgyvendinimo būdų;
	7 straipsnis. 4. 2) Teikia kibernetinio saugumo dalyviams pasiūlymus dėl viešojo sektoriaus, verslo ir mokslo bendradarbiavimo galimybių kibernetinio saugumo užtikrinimo srityje;

Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos ir subjektai	**Informuotumo didinimo visuomenėje aspektas**
	7 straipsnis. 4. 3) Analizuoja kibernetinio saugumo užtikrinimo tobulinimo tendencijas, teikia kibernetinio saugumo dalyviams išvadas ir pasiūlymus dėl kibernetinių incidentų valdymo;
	7 straipsnis. 4. 4) Teikia kibernetinio saugumo dalyviams rekomendacijas dėl kibernetinio saugumo stiprinimo.
Nacionalinis kibernetinio saugumo centras	8 straipsnis. 13) Kai būtina informuoti visuomenę siekiant išvengti kibernetinio incidento arba valdyti vykstantį kibernetinį incidentą, pasikonsultavęs su kibernetinio saugumo subjektu, pranešusiu apie kibernetinį incidentą, informuoja visuomenę apie pavienius kibernetinius incidentus arba reikalauja, kad tai padarytų kibernetinio saugumo subjektas
	8 straipsnis. 16) Kartu su verslo subjektais, mokslo ir studijų institucijomis ir kibernetinio saugumo subjektais plėtoja nacionalinį kibernetinį saugumą stiprinančius projektus.
Valstybinės duomenų apsaugos inspekcijos	9 straipsnis. Valstybinė duomenų apsaugos inspekcija įgyvendina kibernetinio saugumo politiką asmens duomenų apsaugos srityje ir atlieka 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) nustatytas priežiūros institucijos užduotis.
Viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai	12 straipsnis. 3. [...] viešai skelbia savo interneto svetainėse ar kitomis visuomenės informavimo priemonėmis paslaugų gavėjams rekomendacijas dėl priemonių kibernetiniam saugumui užtikrinti naudojantis viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų teikiamomis paslaugomis.
Elektroninės informacijos prieglobos paslaugų teikėjai	12 straipsnis. 4. [...]viešai skelbia savo interneto svetainėse ar kitomis visuomenės informavimo priemonėmis elektroninės informacijos prieglobos paslaugų gavėjams rekomendacijas dėl priemonių kibernetiniam saugumui užtikrinti naudojantis elektroninės informacijos prieglobos paslaugomis.
Skaitmeninių paslaugų teikėjai	12 straipsnis. 5. 1) [...]viešai skelbia savo interneto svetainėse ar kitomis visuomenės informavimo priemonėmis paslaugų gavėjams rekomendacijas dėl priemonių kibernetiniam saugumui užtikrinti naudojantis skaitmeninių paslaugų teikėjų teikiamomis paslaugomis.

Šaltinis: parengta pagal Kibernetinio saugumo įstatymą, 2018.

Remiantis lentelėje pateiktais duomenimis tik viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai, viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai ir elektroninės informacijos prieglobos paslaugų teikėjai įstatymiškai yra įpareigoti tiesiogiai teikti kibernetinį saugumą užtikrinančių priemonių rekomendacijas visuomenei. Tačiau šiuo metu tai gali būti priskiriama tik formaliajai atitikčiai, nes praktikoje ši informacijos sklaidos priemonė visuomenėje nėra vystoma. Remiantis Eurobarometer 2019 m. spalio tyrimo duomenimis „Europiečių požiūris į kibernetinį saugumą“, 80% procentų apklaustųjų Lietuvoje teigė, kad jie neturi informacijos apie interneto puslapį, elektroninio pašto adresą, internetinę formą ar kontaktinį numerį, kuriuo būtų galima pranešti apie bet kokį kibernetinį incidentą. Taigi šių trijų kibernetinio saugumo subjektų pareigų vykdymas sutelkia dėmesį į Ryšių reguliavimo tarnybos vaidmens svarbą kibernetinio saugumo kontekste, kuriai įstatyme nėra priskiriamos kibernetinio saugumo politikos formavimo ir įgyvendinimo funkcijos. Taip pat, Kibernetinio saugumo įstatyme (2018) apibrėžtos kibernetinių saugumo subjektų pareigos nėra taikomos „skaitmenines paslaugas teikiančioms mažoms ir labai mažoms įmonėms, kurios yra apibrėžtos Smulkiojo ir vidutinio verslo plėtros įstatyme“, nepateikiant reikalingų prevencinių priemonių jų veiklos kibernetinio saugumo užtikrinimui.

Taigi remiantis atlikta Kibernetinio saugumo įstatymo (2018) analize informuotumo didinimo visuomenėje pagrindu galima daryti išvadą, kad įstatyme jis yra fragmentiškas ir apima ne visas su kibernetine erdve siejamas grėsmes. Kibernetinis atsparumas ir higiena nėra įtraukiami į sąvokas. Taip pat nėra pabrėžiama takoskyra tarp „kibernetinis“ ir „skaitmeninis“ sąvokų, kurios apriboja tam tikros informacijos sklaidą visuomenėje. Institucijos informacijos sklaidos ir informuotumo didinimo klausimais veikia izoliuotai, nėra koordinuojančios institucijos šiame kontekste. Švietimo, mokslo ir sporto ministerija neatlieka jokių funkcijų Kibernetinio saugumo įstatymo pagrindu. Saugumo taryboje nėra įtraukiama Švietimo, mokslo ir sporto ministerija, specifiškai Valstybinio mokslinių tyrimų institutas. Tai gali lemti kompetencijų poreikio atotrūkį tarp švietimo ir saugumo institucijų

3.2 Kibernetinio saugumo kultūros plėtojimas Kibernetinio saugumo strategijoje

Krašto apsaugos ministro Raimondo Karoblio (2018) teigimu, „strategija parengta laikantis holistinio požiūrio – kibernetinis saugumas suprantamas ne kaip savarankiškas valstybės tikslas ar tik kaip atsakas į šiuolaikinės skaitmeninės Lietuvos valstybės keliamus iššūkius, bet į kibernetinį saugumą žvelgiama kaip į vieną iš integruotos skaitmeninės ekosistemos dalių“. Šiame įžanginiame tekste galima išskirti šias esmines sąvokas: kibernetinis saugumas, skaitmeninė valstybė ir skaitmeninė ekosistema. Jų pagrindu, kuriama Lietuvos kibernetinio saugumo koncepcija. Dokumente pabrėžiama, kad

pagrindinis Nacionalinės kibernetinio saugumo strategijos (2018) numatytas tikslas „užtikrinti galimybę Lietuvos visuomenei saugiai naudotis informacinių ir ryšių technologijų teikiamomis galimybėmis“. Siekiant įgyvendinti tai pateikiami penki strateginiai tikslai, jų keliami uždaviniai ir vertinimo kriterijai. 6 lentelėje pateikiama jų analizė informuotumo didinimo visuomenėje pagrindu.

6 lentelė. Kibernetinio saugumo strategijos (2018) uždaviniai informuotumo didinimo aspektu

Uždavinys	**Informuotumo didinimo visuomenėje aspektas**	**Vertinimo kriterijus**
Pirmasis strategijos tikslas - stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą		
Kurti sisteminį požiūrį į kibernetinį saugumą ir prevencinę veiklą.	[...] tobulinant kibernetinio saugumo rizikos nustatymo, vertinimo ir prognozavimo būdus, [...] užtikrinant visuomenės informavimą apie kibernetinio saugumo būklę, vykdant kitas kibernetinį saugumą ir prevencinę veiklą stiprinančias priemones ir veiksmus.	-
Antrasis strategijos tikslas - užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą		
Stiprinti nusikalstamų veikų kibernetinėje erdvėje prevenciją ir kontrolę.	Uždavinys bus įgyvendinamas propaguojant visuomenės savisaugos kultūrą ir atsakingą elgesį kibernetinėje erdvėje [...].	Projektų, skirtų nusikalstamų veikų kibernetinėje erdvėje prevencijai ir kontrolei stiprinti, skaičius vienetais.
Trečiasis strategijos tikslas - skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą		
Ugdyti kūrybiškumą, pažangius gebėjimus ir rinkos poreikius atitinkančius kibernetinio saugumo įgūdžius ir kvalifikaciją.	-	Investicijų į kibernetinio raštingumo kultūros skatinimą, saugumo žinių, mokslinių tyrimų plėtrą, suma tūkstančiais eurų.
		Per Valstybės tarnautojų registro ir valstybės tarnybos valdymo informacinės sistemos modulį mokytų institucijų ir įstaigų valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis, dalis procentais.

Uždavinys	Informuotumo didinimo visuomenėje aspektas	Vertinimo kriterijus
Ketvirtasis strategijos tikslas – stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą		
Kurti atsakingą viešojo ir privataus sektorių IRT saugumo spragų atskleidimo praktiką.	Uždavinys bus įgyvendinamas propaguojant visuomenės savisaugos kultūrą ir atsakingą elgesį kibernetinėje erdvėje, tobulinant teisėsaugos institucijų kovos su nusikalstamomis veikomis kibernetinėje erdvėje funkcijų vykdymą ir užtikrinant operatyvų tarptautinį bendradarbiavimą tiriant šias nusikalstamas veikas, [...].	Priemonių, skirtų viešojo bei mažų ir vidutinių privataus sektorių atstovų kibernetinio saugumo būklei gerinti, skaičius vienetais.
		Priemonių, skirtų atsakingai viešojo ir privataus sektorių IRT saugumo spragų atskleidimo praktikai formuoti, skaičius vienetais.
Penktasis strategijos tikslas – stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą		
-	-	-

Šaltinis: parengta pagal Kibernetinio saugumo strategiją, 2018.

Pirmojo strategijos tikslo uždavinys nedetalizuoja kibernetinį saugumą ir prevencinę veiklą stiprinančių priemonių bei veiksmų visuomenėje (Kibernetinio saugumo strategija, 2018). Taip pat, nėra pateikiamas ir vertinimo kriterijus. Antrasis tikslas priskiriamas policijos kompetencijai. Šio tikslo viena iš priemonių yra „stiprinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, propaguojant visuomenės savisaugos kultūrą ir atsakingą elgesį kibernetinėje erdvėje“. Vertinimo kriterijus yra įgyvendinti/vykdomi prevenciniai projektai, kurių minimali reikšmė (2) visame laikotarpyje (2018-2023) nesikeičia. Trečiasis tikslas tiesiogiai skirtas kibernetinio saugumo kultūros vystymui. Šio tikslo apraše aptariama problematika įtraukia visuomenės informuotumo trūkumą, kibernetinio saugumo integravimą į ikimokyklinio ir bendrojo ugdymo programas ir mokytojų kompetencijų kėlimą. Suformuluotas uždavinys yra labai platus, tuo tarpu vertinimo kriterijus apsiriboja minimalia investicine suma į žinių ir mokslinių tyrimų plėtrą nedetalizuojant konkrečių priemonių. Galima teigti, kad ketvirtasis tikslas, jo uždaviniai ir vertinimo kriterijai yra glaudžiai susieti ir konkrečiai suformuluoti. Informacijos sklaidos aspektas taip pat detalizuojamas. Penktasis tikslas yra kompetencijų kėlimo pagrindas visais kibernetinio saugumo aspektais, įtraukiant ir kibernetinio saugumo kultūros plėtrą bei informuotumo visuomenėje didinimą. Visi kibernetinėje strategijoje iškelti tikslai yra plačiai aktualizuojami ir jų įgyvendinimas turėtų reikšmingą pokytį šalies kibernetinio saugumo srityje ir jos kultūros plėtojime. Tačiau iškeltos užduotys pirmojo ir trečiojo tikslams pasiekti, kurios laikomos kertinėmis kibernetinio saugumo kultūros vystymui, yra labai plačios ir pateikiami vertinimo kriterijai neatspindi viso uždavinių turinio. Antrojo ir ketvirtojo tikslų užduočių aprašuose įvedama nauja terminologija - savisaugos kultūra kibernetinėje

erdvėje, kuri nėra detalizuojama. Taip pat, nėra pateikiama ir kibernetinio saugumo kultūros samprata. Visa tai lemia nuoseklumo trūkumą strategijos įgyvendinime. Ugdymo programų ir kibernetinio saugumo informacijos sklaidos aspektai kaip ilgalaikės kibernetinių incidentų prevencinės priemonės nėra priskiriamos strateginėms užduotims ar jų vykdymo vertinimo kriterijams.

3.3 Kibernetinio saugumo kultūros plėtojimo vertinimas ikimokyklinio ir bendrojo ugdymo programų pagrindu

Šiandiena vaikai auga vis sudėtingesniame pasaulyje, kuris gali būti dalomas į „*online*“ ir „*offline*“ rėžimus. Švietimo sistema jiems turi suteikti žinių reikalingų saugiai, sąmoningai ir pagarbiai naudotis interneto ir technologijų teikiamais privalumais. Švietimas turi būti grindžiamas integracija į visuomenės ir valstybės gyvenimą.

Lietuvos Respublikos Švietimo įstatymas (1991) yra pagrindinis dokumentas, reglamentuojantis švietimo sistemos veiklą. Šiame įstatyme (1991) pateikiami švietimo tikslai atspindi informacinių technologijų ir skaitmeninio raštingumo svarbą valstybiniu lygiu:

1) […] išlavinti dabartiniam gyvenimui svarbius jo komunikacinius gebėjimus, padėti įsisavinti žinių visuomenei būdingą informacinę kultūrą, [..], informacinį raštingumą, […];

2) nustatyti asmens kūrybinius gebėjimus ir pagal tai padėti jam įsigyti kompetencijų ir (ar) kvalifikaciją, atitinkančią šiuolaikinį kultūros bei technologijų lygį ir padedančią jam įsitvirtinti ir sėkmingai konkuruoti tolydžiai kintančioje darbo rinkoje, perteikti technologijų, ekonomikos ir verslo kultūros pagrindus, būtinus šalies ūkio pažangai, konkurencingumui bei darniai raidai laiduoti, sudaryti sąlygas nuolat tenkinti pažinimo poreikius ir tobulėti mokantis visą gyvenimą;

3) stiprinti visuomenės galias užtikrinant krašto ūkio, aplinkos ir žmogiškųjų išteklių darnų vystymąsi, vidinį ir tarptautinį ūkio konkurencingumą, nacionalinį saugumą ir demokratinės valstybės raidą.

Taip pat, įstatyme pateikiamas kontekstualumo principas užtikrina nuolatinį švietimo sistemos atsinaujimą ir atitikimą nuolat kintančioms visuomenės reikmėms. Lietuvos švietimo sistema apima (Lietuvos Švietimo įstatymas, 1991):

1) formalųjį švietimą (pradinį, pagrindinį, vidurinį ugdymą, formalųjį profesinį mokymą ir aukštojo mokslo studijas);

2) neformalųjį švietimą (ikimokyklinį, priešmokyklinį, kitą neformalųjį vaikų (taip pat formalųjį švietimą papildantį ugdymą) ir suaugusiųjų švietimą);

3) savišvietą;

4) švietimo pagalbą (profesinį orientavimą, švietimo informacinę, psichologinę, socialinę pedagoginę, specialiąją pedagoginę ir specialiąją pagalbą, sveikatos priežiūrą mokykloje, konsultacinę, mokytojų kvalifikacijos tobulinimo ir kitą pagalbą).

Šio įstatymo pagrindu yra rengiamos ikimokyklinių, priešmokyklinių ir bendrojo ugdymo programos. Konkretus ugdymo turinys kuriamas ir sistemingai atnaujinamas atsižvelgiant į atitinkamos grupės ar tipo mokyklai keliamus ugdymo, mokymo ir studijų tikslus, besikeičiančios socialinės ir kultūrinės aplinkos lemiamus Lietuvos visuomenės poreikius, vietos ir mokyklos bendruomenės reikmes, taip pat mokinių ir studentų turimą patirtį, ugdymosi poreikius ir interesus (Lietuvos Respublikos Švietimo įstatymas, 1991). Didžiausiu iššūkiu ruošiant ugdymo programas tampa technologijų vystymosi sparta.

3.3.1 Ikimokyklinio ugdymo programa

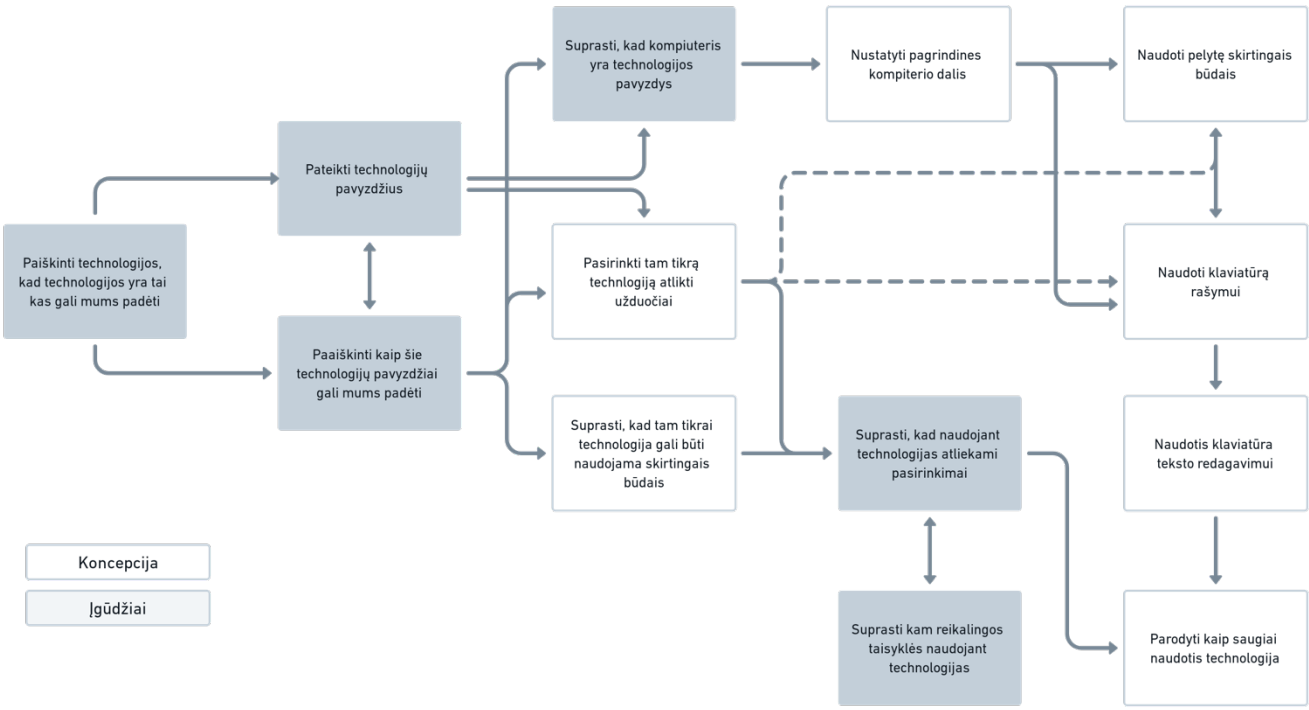
Švietimo įstatymas (1991) apibrėžia ikimokyklinio ugdymo paskirtį: „padėti vaikui tenkinti prigimtinius, kultūros, taip pat ir etninės, socialinius, pažintinius poreikius“. Švietimo ir mokslo ministro įsakymas dėl ikimokyklinio ugdymo programų kriterijų aprašo (2005) nurodo, kad „ikimokyklinio amžiaus vaikai ugdomi šeimoje, o tėvams (globėjams) pageidaujant ar švietimo ir mokslo ministro ir socialinės apsaugos ir darbo ministro nustatyta tvarka ir atvejais – pagal ikimokyklinio ugdymo programą“. Ikimokyklinio amžiaus vaikų pasiekimų aprašas (2014) pateikia šešerių metų vaiko ugdymosi pasiekimų sąvadą, kurį sudaro 18 ugdymo sričių. Skaitmeninio raštingumo aspektas nėra įtraukiamas nė į vieną iš pasiekimų sričių. Tačiau žemiau pateikiamos 5-6 metų amžiaus vaikų ugdymo pasiekimų sritys, kurios referuoja į skaitmeninius įgūdžius:

- Rašytinė kalba rašymas, rašytinės kalbos srities pasiekimai, 6 - asis žingsnis: „Spausdintomis raidėmis rašo savo vardą, kopijuoja aplinkoje matomus žodžius. Piešiniuose užrašo atskirų objektų pavadinimus. Įvairiais simboliais bando perteikti informaciją. Planšetiniu kompiuteriu rašo raides, žodžius. Supranta rašymo tikslus“.
- Meninė raiška, meninės raiškos srities pasiekimai, 7- asis žingsnis: „Kūrybiškai panaudoja tradicines ir netradicines medžiagas, priemones, technikas sumanymui įgyvendinti. Bando kurti naudodamasis skaitmeninio piešimo ar kitomis kompiuterinėmis programomis, skaitmeninėmis priemonėmis“.
- Tyrinėjimas, tyrinėjimo srities pasiekimai, 7-asis žingsnis: „Tyrinėjimams naudoja skaitmenines technologijas (kompiuterį, mobilųjį telefoną, fotoaparatą ir kt.).

Taigi programoje daroma prielaida, kad šios amžiaus grupės vaikų ugdymas šeimoje įtraukė pažintį su technologijomis ir tinkamu jų naudojimu. Ši prielaida pateikiama ir „Ikimokyklinio ugdymo metodinėse rekomendacijose“ (2015), kuriose vaikai apibūdinami kaip: „[...] „interneto amžiaus“, Z kartos, skaitmeninių technologijų vaikais ir kt. Jie auga su kompiuteriais, internetu, interaktyviomis lentomis, mobiliaisiais telefonais, fotoaparatais, skaitmeninėmis knygomis bei žaislais.“. Tačiau tai apriboja vaikų, kurie dėl socialinių priežasčių šeimose neturėjo galimybės ugdyti šių įgūdžių, pažintį su IT ir su jomis siejama sauga bei saugumu. Taip pat, šeimoje formuojamos vaiko elgesio normos informacinių

technologijų srityje priklauso nuo tėvų skaitmeninio raštingumo, saugumo kultūros ir neužtikrina vaiko raidą atitinkančio ugdymo šioje srityje. EUROSTAT 2021 metų duomenimis Lietuvoje 49% asmenų turėjo pagrindinius arba aukštesnius nei bazinius bendruosius skaitmeninius įgūdžius. Remiantis šiais duomenimis ir atsižvelgiant į sparčią technologinę raidą galima daryti išvadą, kad tiek tėvams, tiek ikimokyklinio amžiaus vaikams yra reikalinga sisteminga švietimo programa, kuri didintų jų informuotumą, formuotų bei vystytų reikiamus įgūdžius IT srityje.

Atsižvelgiant į ikimokyklinio ugdymo programoje įtrauktus IT metodus ir specialistų išsakytą nuomonę, buvo analizuojama 5-6 metų amžiaus vaikams taikoma kompiuterijos ugdymo programos metodologija Jungtine Karalystėje. Šioje šalyje privalomas ugdymas prasideda nuo penkerių metų. Kompiuterija yra įtraukta į privalomąją ugdymo programą. Penkerių metų vaiko kompiuterijos ugdymo programos skyrius „Technologijos aplink mus“ atspindi pagrindinius aspektus apie technologijas ir tinkamą jų naudojamą. 11 pav. pateikiama kompiuterijos ugdymo metodologija.



Šaltinis: sudaryta pagal Jungtinės Karalystės nacionalinę ugdymo programą, 2014

11 pav. Kompiuterijos ugdymo metodologija ankstyvame amžiuje.

Atsižvelgiant į Lietuvos ikimokyklinio ugdymo koncepciją ir reglamentavimą (ikimokyklinis ugdymas nėra privalomas) ši metodologija turėtų būti integruota į sudarytos ugdymo programos veiklos sritis. Siūlomos šios sritys:

- Kasdienio gyvenimo įgūdžiai.
- Aplinkos pažinimas.
- Problemų sprendimas.
- Tyrinėjimas.

- Mokėjimas mokytis.
- Meninė raiška.
- Rašytinė kalba.

Technologijų ir tinkamo jų naudojimo pagrindai 5 - 6 metų vaikams suteiks naujų, papildomų žinių šioje srityje, kurios leis saugiai naudotis technologijomis ir už ugdymo įstaigos ribų. Tai taip pat įtakos ir šeimoje suformuotą elgesio modelį, taps saugumo kultūros pagrindu.

3.3.2 Priešmokyklinio ugdymo programa

Priešmokyklinio ugdymo bendrojoje programoje (2014) ugdomos šios kompetencijos: socialinė, sveikatos, pažinimo, komunikavimo ir meninė. Programos ugdymo gairėse IT pasitelkiamos tam tikros kompetencijos pasiekimui. Ugdymo programoje daroma prielaida, kad vaikas jau turi skaitmeninio raštingumo pradmenis ir gebėjimas naudotis IT priskiriamas bendriesiems gebėjimams. Priešmokyklinio ugdymo pedagogui pateikiami rekomendaciniai leidiniai, kurie nurodo įvairius IT integravimo būdus ugdymo procese: „Informatinis mąstymas priešmokykliniame amžiuje“ (2021) „„Projektų metodas priešmokyklinėje grupėje“ (2021), „STEAM priešmokykliniame amžiuje“ (2021). Išanalizavus ugdymo programos žinių ir supratimo sritį IT informuotumo pagrindu, nustatytos dvi programos sritys įtraukiančios saugaus elgesio poreikį naudojantis IT ir internetu. Pirmasis nukreipimas yra socialinės sveikatos ugdymo sritis, kurioje aptariama seksualinio išnaudojimo ir prievartos grėsmė: „Aptariami galimi pavojai internete (pvz., siūlymai susidraugauti, susitikti, pasidalyti nuotraukomis, adresais ir kt.) ir elgesio tokiose situacijose būdai. Vaikai drąsinami kreiptis pagalbos, kai jaučiasi nesaugūs“. Antrasis kalbos suvokimo ir kalbėjimo srityje tiesiogiai įtraukia IT ir su jomis siejamas rizikas (žr. 7 lent.).

7 lentelė. Priešmokyklinio ugdymo programos (2014) informuotumo didinimo aspektas

Pasiekimai			**Ugdymo gairės**
Nuostatos	**Gebėjimai**	**Žinios ir supratimas**	
Bendravimui naudotis informacinėmis ir komunikacinėmis technologijomis	Naudojasi mobiliuoju ir (ar) kompiuteriu pokalbiams su artimaisiais, draugais, kitoms kultūroms, šalims pažinti	Paaiškina esmines naudojimosi kompiuteriu, mobiliuoju telefonu taisykles, pasako galimus naudojimosi jais pavojus, nusako informacinių ir komunikacinių	Vaikai dalijasi patirtimi apie informacinių ir komunikacinių technologijų svarbą jų gyvenime, pvz., galimybę susisiekti su draugais, užsienyje gyvenančiais giminaičiais. Suderinus su vaiko šeima, bandoma paskambinti, pabendrauti „Skype“ programa su draugais, užsienyje gyvenančiais giminaičiais.

		technologijų svarbą kasdieniame gyvenime.	Vaikai skatinami kartu su suaugusiaisiais naršyti internete ir ieškoti informacijos projektams vykdyti, pažinti kitų šalių kultūras (pvz., klausytis kitų šalių kalbos, dainų, stebėti šokius ir pan.).

Šaltinis: parengta pagal Priešmokyklinio ugdymo programą, 2014.

7 lentelėje skiltis „Žinios ir supratimas“ pateikia šiai vaikų amžiaus grupei reikalingas žinias saugiai naudotis technologijomis bei įvardina susijusias rizikas. Tačiau pateikiamos pasiekimų nuostatos ir gebėjimai susiaurina ugdomąją veiklą IT srityje apsiribojant tik bendravimui skirtomis informacinėmis ir komunikacinėmis priemonėmis. Taigi IT naudojimo ir saugumo tematika turėtų būti plėtojama šioje ugdymo programoje, tik kitoje srityje. Siekiant nustatyti galimas vystymo kryptis išanalizuota Jungtinės Karalystės kompiuterijos 6 - 7 metų ugdymo programa. Modulio „Technologijos aplink mus“ metodinė medžiaga kryptingai analizuoja IT, ji pateikiama 8 lentelėje:

8 lentelė. Jungtinės Karalystės kompiuterijos 6 - 7 metų ugdymo programa

Amžius	Mokymosi tikslai	Sėkmės kriterijus
6 - 7	Atpažinti informacinių technologijų naudojimo būdus ir ypatybes	- Galiu apibūdinti kai kuriuos kompiuterių panaudojimo būdus - Galiu nustatyti kompiuterių pavyzdžius - Galiu atpažinti, kad kompiuteris yra informacinių technologijų dalis
6 - 7	Paaiškinti, kaip saugiai naudotis informacinėmis technologijomis	- Galiu išvardinti informacinių technologijų panaudojimo būdu - Galiu pasakyti, kaip taisyklės gali padėti mane apsaugoti - Galiu kalbėti apie informacinių technologijų naudojimo taisykles - Galiu išvardinti informacinių technologijų panaudojimo būdus - Galiu pasakyti, kaip taisyklės gali padėti mane apsaugoti - Galiu kalbėti apie visas informacinių technologijų naudojimo taisykles

Amžius	Mokymosi tikslai	Sėkmės kriterijus
6 - 7	Nustatyti informacinių technologijų panaudojimo galimybes mokykloje	- Galiu išskirti informacinių technologijų pavyzdžių - Galiu nustatyti, kad kai kurios informacinės technologijos gali būti naudojamos ne vienu būdu - Galiu rūšiuoti mokyklos informacines technologijas pagal tai, kam jos naudojamos
6 - 7	Atpažinti, kad naudojantis informacinėmis technologijomis daromi pasirinkimai	- Informacinių technologijų naudojimo poreikį galiu paaiškinti įvairiai - Galiu atpažinti pasirinkimus, kuriuos darau naudodamasis informacinių technologijų - Galiu naudoti informacines technologijas įvairioms veikloms
6 - 7	Atpažinti informacines technologijas už mokyklos ribų	- Galiu rasti informacinių technologijų pavyzdžių - Galiu rūšiuoti informacines technologijas pagal tai, kur ji randama - Galiu kalbėti apie informacinių technologijų panaudojimą
6 - 7	Paaiškinti, kaip informacinės technologijos mums padeda	- Galiu pademonstruoti, kaip informacinių technologijų įrenginiai veikia kartu - Galiu atpažinti įprastas technologijų rūšis - Galiu pasakyti, kodėl naudojame informacines technologijas
6 - 7	Paaiškinti, kad informaciją galime pateikti naudodami kompiuterį	- Galiu pateikti paprastus pavyzdžius, kodėl informacija neturėtų būti dalijama - Galiu pasidalinti tuo, ką sužinojau naudodamasis kompiuteriu - Galiu naudoti kompiuterinę programą įvairiai pateikti informaciją

Šaltinis: sudaryta pagal Jungtinės Karalystės nacionalinę kompiuterijos ugdymo programą.

Šis modulis ne tik įtraukia įvairius IT pažinimo aspektus, bet ir atkreipia vaiko dėmesį į jo atliekamus pasirinkimus naudojantis IT. Kadangi ikimokyklinio ugdymo programoje pateikti integralumo ir kontekstualumo principai pagrindžia platesnį informuotumo poreikį IT srityje, šis pilnas modulis galėtų būti įtrauktas į pažinimo kompetencijos sritį. Programoje „Mokykla 2030“ priešmokyklinio ugdymo programa įtraukia naują – skaitmeninę kompetenciją. Ji integruotai vystoma gamtamokslio, kalbinio, matematinio, meninio, sveikatos ir fizinio ir visuomeninio ugdymo pagrindu. Projekto šiai amžiaus grupei pateikiamame kompetencijų apraše, skaitmeninė kompetencija, kurioje įtrauktas ir saugumo

aspektas, plačiai išplėtota. Tačiau ugdymo programa to neatspindi ir palieka kokybišką šių įgūdžių vystymą mokytojo kompetencijai.

3.3.3 Pradinio ugdymo programa

Vienas iš uždavinių keliamų pradiniam ugdymui yra „padėti vaikui įgyti prasmingų, aktualių žinių apie save, pasaulį ir kitus žmones“ (Pradinio ugdymo programa, 2016). Pradinėje mokykloje IT gebėjimų ugdymas integruojamas į kitas ugdymo sritis ir priskiriamas pagalbinei ugdymo priemonei (Pradinio ugdymo programa, 2016). Mokyklos gali savo nuožiūra pasiūlyti mokiniams pasirenkamuosius IT būrelius ar panašias ugdymo formas. Mokytojai integruojantys IT į ugdymo procesą, jas panaudoja ugdymo procesui modernizuoti ir tobulinti. Pradinio ugdymo bendrojoje programoje nurodoma: „Jei pamokose mokiniai naudojasi komunikacijos priemonėmis, būtina formuoti saugaus naršymo internete bei saugaus bendravimo nuostatas, svarbu, kad internetas mokiniams būtų saugus. Todėl mokytojas privalo pasikalbėti su mokiniais apie pavojus, kurie gali tykoti internete, paaiškinti asmeninės informacijos atskleidimo pavojingumą, aptarti, kaip vengti tokių situacijų.“ Šio reikalavimo įgyvendamas priklauso nuo mokytojo turimų kompetencijų, papildoma metodologija šiuo aspektu ugdymo programoje neteikiama. Taigi galima daryti išvadą, kad IT traktavime nėra koncentro su pagrindinio ugdymo programa.

Jungtinėje Karalystėje 7 – 11 metų vaikams kompiuterijos ugdymo programoje (2021) vystomi šie gebėjimai:

- kurti, rašyti ir derinti programas, kurios pasiekia konkrečius tikslus, įskaitant fizinių sistemų valdymą arba modeliavimą; išspręsti problemas, skaidant jas į mažesnes dalis;
- programose naudoti seką, pasirinkimą ir kartojimą; dirbti su kintamaisiais ir įvairiomis įvesties ir išvesties formomis;
- naudoti loginius samprotavimus, siekiant paaiškinti, kaip veikia kai kurie paprasti algoritmai, ir aptikti bei ištaisyti algoritmų ir programų klaidas;
- suprasti kompiuterių tinklus, įskaitant internetą; kaip jie gali teikti kelias paslaugas, pvz., World Wide Web ir jų teikiamas bendravimo bei bendradarbiavimo galimybes;
- efektyviai naudoti paieškos technologijas, įvertinti, kaip rezultatai atrenkami ir reitinguojami, būti įžvalgiems vertinant skaitmeninį turinį;
- pasirinkti, naudoti ir derinti įvairią programinę įrangą (įtraukiant interneto paslaugas) įvairiuose skaitmeniniuose įrenginiuose, kuriant dizainą ir programas, sistemas ir turinį, kurie įgyvendina nurodytus tikslus, įskaitant duomenų ir informacijos rinkimą, analizę, vertinimą ir pateikimą;
- saugiai, pagarbiai ir atsakingai naudotis technologijomis; atpažinti priimtiną/nepriimtiną elgesį; nurodyti įvairius būdus, kaip pranešti apie susirūpinimą dėl turinio.

Šioje amžiaus grupėje išryškėja labai didelis Jungtinės Karalystės ir Lietuvos vaikų ugdomų IT gebėjimų atotrūkis. Projekto „Mokykla 2030“ derinamoje „Pradinio ugdymo programoje“ (2021) keliami šie informatikos uždaviniai:

1. spręsdami įvairias realaus gyvenimo problemas geranoriškai bendradarbiauja, sumaniai naudojasi skaitmeninėmis technologijomis, pasitiki savo jėgomis;
2. ugdosi informatinio mąstymo pradmenis, praktiškai taiko įgytas žinias spręsdami aplinkos problemas;
3. tinkamai vartoja informatikos sąvokas, etiškai bendrauja ir saugiai naudoja įvairias skaitmenines komunikavimo priemones;
4. tobulina savo skaitmeninius gebėjimus, vertina informatiką kaip svarbią, įdomią ir naudingą mokymosi sritį.

Taip pat išskiriamos 6 pasiekimų grupės:

1. Skaitmeninio turinio kūrimas.
2. Algoritmai ir programavimas.
3. Duomenų tyryba ir informacija.
4. Technologinių problemų sprendimas.
5. Virtualioji komunikacija ir bendradarbiavimas.
6. Saugus elgesys.

Saugaus elgesio sričiai priskiriami pasiekimai nurodomi 9 lentelėje:

9 lentelė. Saugaus elgesio pasiekimai informatikos Bendrojo ugdymo projekto programoje (2021).

Pasiekimas	**1-2 klasės**	**3-4 klasės**
F1. Saugo sveikatą.	F1.3. Pateikia sveikatą tausojančio darbo skaitmeninėmis technologijomis pavyzdžių.	F1.3. Aptaria ir laikosi sveikatą tausojančio darbo skaitmeninėmis technologijomis taisyklių.
F2. Saugo aplinką.	F2.3. Kalba apie skaitmeninių įrenginių poveikį aplinkai.	F2.3. Pateikia skaitmeninių technologijų poveikio visuomenei ir aplinkai pavyzdžių.
F3. Saugiai elgiasi virtualiojoje erdvėje.	F3.3. Saugo asmens duomenis ir skaitmeninę tapatybę, pateikia ir aptaria pavyzdžius.	F3.3. Aptaria ir laikosi saugaus darbo virtualiojoje erdvėje taisyklų, gerbia asmens privatumą.

Šaltinis: sudaryta pagal Informatikos ugdymo programos projektą, 2021.

Šios ugdymo programos įgyvendinimas iš esmės pakeistų 7 – 11 metų amžiaus grupės vaikų kompetencijas IT srityje išlaikant vaikų įgūdžius konkurencingais tarptautiniame kontekste ir diegtų bei vystytų kibernetinio saugumo kultūrą. Šios programos įgyvendinimo sėkmė priklausys nuo mokytojų kompetencijos. Pedagogų kompetencijų kėlimas ir su juo susijusi problematika turėtų būti prioretizuojama.

3.3.4 Pagrindinio ir vidurinio ugdymo programos

Pagrindinio ir vidurinio ugdymo programos apibrėžiamos aprašant numatomus mokinių mokymosi pasiekimus, pateikiant rekomenduojamas ugdymo proceso gaires, nurodant dalykų turinio apimtį ir aprašant mokinių pasiekimų lygių požymius (Lietuvos Respublikos Švietimo ir mokslo ministro įsakymas, 2008). Informacinių technologijų paskirtis bendrojo lavinimo programose – ugdyti informacinę ir technologinę mokinių kompetencijas (Lietuvos Respublikos švietimo ir mokslo ministro įsakymas, 2005).

Siekiant įvertinti ugdymo programos turinį kibernetinio saugumo kultūros vystymo pagrindu buvo išanalizuota pagrindinio ugdymo IT programa (2005) 5-10 klasėms (žr. 10 lent.)

10 lentelė. Informacinių technologijų ugdymo bendrosios programos (2005) turinys informuotumo didinimo aspektu

Veiklos sritys	5-6 klasės	7-8 klasės	9-10 klasės
1. Informacijos tvarkymas kompiuteriu	Taisyklingai vartoti kompiuterijos informacinių technologijų terminus, sąvokas. Saugoti informaciją kompiuterinėse laikmenose. Teisėtai naudoti kompiuterio programas. Apibūdinti kompiuterių svarbą kasdienei žmogaus veiklai.	Taisyklingai vartoti kompiuterijos ir informacinių technologijų terminus, apibūdinti pagrindines sąvokas. Informacijos ir duomenų apsaugai naudoti antivirusinę programą, taikyti hierarchinę informacijos laikymo kompiuteryje struktūrą. Teisėtai naudoti kompiuterio programas ir kitų autorių darbus. Paaiškinti viešųjų elektroninių paslaugų svarbą.	Saugiai, atsakingai dirbti kompiuteriu, rūpintis sveika gyvensena. Tinkamai naudotis programine ir aparatine kompiuterio įranga, išorinėmis informacijos laikmenomis. Taisyklingai vartoti kompiuterijos ir informacinių technologijų

			terminus, apibūdinti sąvokas. Teisėtai naudoti kompiuterio programas bei autorių darbus, rūpintis duomenų saugumu.
4. Internetas ir jo paslaugos	Saugiai naudotis interneto pokalbių paslaugas	-	-

Šaltinis: sudaryta pagal informatikos bendrojo ugdymo programą, 2005.

Analizės rezultatai atskleidžia, IT ugdymo programos veiklos sričių fragmentiškumą, veiklos sritys nėra plėtojamos nuosekliai. Saugumo ir kibernetinio saugumo kultūros ugdymo pirminiai aspektai (saugi komunikacija internete, intelektinė nuosavybė) įtraukiami tam tikrose ugdymo programos veiklose. Internetas ir jo paslaugos, kaip pagrindas kibernetinio saugumo kultūros plėtojimui, dėstomas tik 5-6 klasėje su ribotu saugumo turiniu. 7-8 klasių mokiniai neturi veiklos srities interneto tema, ji yra integruojama kitose ugdymo programose. Tuo tarpu 9 -10 klasių mokiniai šia tematika nediskutuoja saugumo klausimais. Vidurinio ugdymo programos 11 – 12 klasių išplėstiniam kursui pateikiamos elektroninės leidybos, duomenų bazių kūrimas ir valdymas bei programavimo moduliai. Šių modulių apraše, tik elektroninės leidybos modulis įtraukia autorinių teisių apsaugos aspektą: „Naudotis autorių teisių ir gretutinių teisių apsaugą reglamentuojančiais teisės aktais)“. Taigi galima daryti išvadą, kad pagrindinio ir vidurinio ugdymo programų turinys neįtraukia kibernetinio saugumo ir saugumo tematika nėra nuosekliai vystoma ir plėtojama šiose vaikų amžiaus grupėse.

Jungtinė Karalystė savo kompiuterijos programoje 11 – 15 metų amžiaus vaikams įtraukia specialiuosius modulius skirtus kibernetinio saugumo kultūros vystymui – pagarbus bendradarbiavimas internete, kibernetinis saugumas ir saugumas internete. Moduliai ir jiems keliami tikslai pateikti 11 lentelėje.

11 lentelė. Jungtinės Karalystės 11 -15 metų kompiuterijos ugdymo programos (2021) kibernetinio saugumo moduliai

Amžius	Modulis	Sėkmės kriterijus
11 - 12	Pagarbus bendradarbiavimas internete	- Sukurkite įsimintiną ir saugų paskyros slaptažodį mokyklos tinkle - Raskite asmeninius dokumentus ir įprastas programas - Atpažinkite pagarbų el. laišką - Sukurkite veiksmingą el. laišką ir išsiųskite jį tinkamiems gavėjams - Apibūdinkite, kaip bendrauti su bendraamžiais internete - Suplanuokite efektyvius pristatymus konkrečiai auditorijai

Amžius	Modulis	Sėkmės kriterijus
		- Apibūdinkite elektronines patyčias - Paaiškinkite patyčių internete pasekmes - Suplanuokite efektyvius pristatymus konkrečiai auditorijai - Apibūdinkite elektronines patyčias - Paaiškinkite patyčių internete pasekmes - Patikrinkite, su kuo kalbate internete.
13 - 14	Kibernetinis saugumas	- Paaiškinkite skirtumą tarp duomenų ir informacijos - Kritikuoti internetines paslaugas, susijusias su duomenų privatumu - Nustatykite, kas atsitiks su duomenimis, įvestais internete - Paaiškinkite Duomenų apsaugos įstatymo poreikį - Nustatyti, kaip žmogaus klaidos kelia pavojų duomenų saugumui - Įgyvendinti strategijas mažinant rizikas duomenų pažeidžiamumui dėl žmogaus klaidų - Apibrėžkite įsilaužimą kibernetinio saugumo kontekste - Paaiškinkite, kaip DDoS ataka gali paveikti internetinių paslaugų vartotojus - Nustatykite strategijas, kaip sumažinti „brute force“ sėkmingos atakos tikimybę - Paaiškinkite „Piktnaudžiavimo kompiuteriu“ įstatymo poreikį - Išvardykite įprastas kenkėjiškų programų grėsmes - Ištirkite, kaip įvairių tipų kenkėjiškos programos sukelia kompiuterių sistemų problemas - Diskutuoti galimą botų įtaką visuomenės problemoms - Palyginkite saugumo grėsmes su tikimybe ir galimu poveikiu organizacijoms - Paaiškinkite, kaip tinklus galima apsaugoti nuo įprastų saugumo grėsmių - Nustatyti efektyviausius kibernetinių atakų prevencijos būdus
14 - 15	Saugumas internete	- Aptarkite pagrindinius saugumo klausimus, susijusius su prisijungimu - Apmąstykite veiklą internete saugumo požiūriu - Apibrėžkite internetinę reputaciją ir aptarkite, iš ko ji susideda - Aptarkite būdus, kaip susikurti teigiamą reputaciją internete - Aptarkite, kaip gali kilti grėsmė jūsų internetinei reputacijai ir kaip ją apginti - Apibrėžkite terminus „didieji duomenys“ ir „duomenų analizė“ - Aptarkite didelių duomenų naudojimo etiką - Ištirkite suinteresuotąsias šalis, kurios naudoja didelius duomenis ir kodėl - Paaiškinkite, kaip renkami duomenys ir kaip jie naudojami

Amžius	Modulis	Sėkmės kriterijus
		- Ištirkite įstatymines teises į privatumą JK - Aptarkite, kurios teisės, kaip manoma, yra saugomos - Diskutuoti, ar teisė į privatumą yra svarbi, kodėl taip gali būti ir ar teisė į privatumą yra nesuderinama su kitomis teisėmis - Įvertinkite, kokie internete sukurti duomenys yra vertingi ir kam - Aptarkite būdus, kuriais duomenys gali būti pavogti - Apibrėžkite terminus „sukčiavimas“ ir „kenkėjiška programa“ - Raskite būdus, kaip apsaugoti savo duomenis internete - Aptarkite dezinformacijos plitimo internete pavyzdžius - Apibrėžkite terminą „netikros naujienos“ ir aptarkite internete pasiekiamų netikrų naujienų kiekį - Nustatykite, kodėl egzistuoja netikros naujienos ir kas jas kuria - Aptarkite melagienų ir kitų dezinformacijos formų atpažinimo būdus - Paaiškinkite, kodėl tam tikras internetinis turinys gali būti žalingas - Apibūdinkite JK įstatymus, reglamentuojančius internetinį turinį - Aptarkite, kodėl internetinių erdvių priežiūra gali būti sudėtinga - Parodykite, kaip pranešti apie neteisėtą internetinį turinį - Aptarkite, kaip nusprendžiame, koks turinys turi būti neteisėtas - Diskutuoti apie teisę gauti informaciją, susijusią su saugos problemomis internete, jau aptarta šiame skyriuje - Palyginkite JK įstatymus su kitų šalių įstatymais - Atraskite įvairias technologijas, naudojamas norint pasiekti ir dalytis informacija internete - Apsvarstykite, kaip dideli duomenys ir kiti įrankiai padeda nukreipti informaciją konkretiems vartotojams - Aptarkite, kokį poveikį tai gali turėti skirtingų žmonių patirčiai internete ir galimus gyvenimo interneto burbule trūkumus. - Pagalvokite apie galimą buvimo internete žalą - Nustatykite praktinius veiksmus, kurių galima imtis norint apsisaugoti internete - Apibendrinkite pagrindinius saugos internete aspektus

Šaltinis: parengta pagal Jungtinės Karalystės nacionalinę kompiuterijos ugdymo programą, 2021.

Remiantis šia medžiaga galima teigti, kad Jungtinės Karalystės kompiuterijos programa stipriai susieta su šių dienų kibernetinio saugumo aktualijomis. Mokinių kursas įtraukia DDoS atakas, didžiuosius duomenis, kenkėjiškų programų analizę ir informacinio saugumo reglamentavimą šalyje. Šių modelių ugdymo gairės gali papildyti Lietuvos informacinių technologijų ugdymo turinį. Projekto „Mokykla

2030“ parengta „Informatikos ugdymo programa“ (2021) labai praplečia ir struktūruoja vaikų gaunamas žinias IT srityje, nagrinėjamas kibernetinės saugos ir duomenų saugos ryšys. Programoje (2021) pateikiami šie saugaus darbo virtualioje aplinkoje principai, pavojai ir problemos: „Mokomasi saugiai naudotis pasirinkta virtualiąja erdve, prisimenami saugaus darbo principai: naudoti tinkamas mokymo(si) ir bendradarbiavimo platformas ir legalią ir atnaujintą programinę įrangą; bendravimui pasirinkti uždaras grupes; laikytis drausmės (susitarimų) ir mandagaus elgesio taisyklių, netoleruoti kitų netinkamą elgesį, patyčias, pastebėję, atitinkamai reaguoti; saugoti prisijungimo duomenis; susidūrę su neteisėtu ar žalingu turiniu internete, pranešti apie tai interneto karštajai linijai ar suaugusiems; daryti svarbiausių duomenų atsargines kopijas saugyklose internete („debesyse“) arba išorinėse laikmenose. Aptariami pavojai, kurie gali kilti bendraujant ir bendradarbiaujant internete: tapatybės vagystės, socialinės inžinerijos atakos, patyčios, priekabiavimas, užgauliojimas, paslapčių išdavimas, apkalbos, gąsdinimas. Aptariama šių reiškinių žala.[..]“. Taigi programoje ypatingas dėmesys skiriamas būtent kibernetinio saugumo informuotumo ir kultūros plėtrai – įtraukiamas saugaus elgesio mokymosi turinys. Tačiau svarbu pabrėžti šios programos terminologiją, kuri neįtraukia žodžio „kibernetinė erdvė“ sąvokos. Programoje vartojama „virtuali erdvė“, tuo tarpu žodis „kibernetinis“ siejamas ir vartojamas aprašant įvairias grėsmes internete. Ugdymo programoje nepateikiamas virtualios erdvės apibrėžimas, taip pat virtualios erdvės sąvoka nėra reglamentuojama kibernetinio saugumo ir duomenų apsaugos srityse. Tai vysto informacijos sklaidos ir paieškos problematiką.

Atsižvelgiant į sparčiai besivystančią kibernetinę erdvę ir su ja siejamas rizikas, ugdymo programos turėtų integruoti nuolatinę mokinių elgesio kibernetinėje erdvėje vertinimo sistemą, kuri leistų gilinti tam tikras programoje numatytas tematikas. Taip pat, mokiniai turi būti motyvuojami gilinti savo žinias kibernetinio saugumo srityje. Šiuo aspektu Antunes ir kt. (2021) pasiūlė savidiagnostikos programėlių kūrimą, kurios gali būti prieinamos internete. Sužaidybintos, vaikų raidą atitinkančios programėlės gali tapti kibernetinio saugumo kultūros plėtojimo pagrindu. Mokyklos gali išplėtoti įvairias programas, turnyrus ir kitas veiklas siekiant įtraukti visą mokyklos bendruomenę.

3.4 Kibernetinio saugumo kultūros vystymo kryptys ikimokyklinio ir bendrojo ugdymo programų pagrindu

Ikimokyklinio ir priešmokyklinio ugdymo amžiaus vaikų kibernetinio saugumo kultūra formuojama šeimoje. Remiantis literatūrine analize kibernetinio saugumo kultūros pagrindu laikomos žinios. Tad tėvų informuotumo didinimas yra prioritetinė sritis ankstyvojo amžiaus vaikų saugumo kultūros formavime. Ikimokyklinio ir priešmokyklinio ugdymo informaciniai leidiniai publikuojami LR Švietimo, mokslo ir sporto ministerijos puslapyje apsiriboja ikimokyklinėmis didaktinėmis publikacijomis. Tarp jų ministerija pateikia ir rekomendacijų leidinį skirtą ikimokyklinio ir

priešmokyklinio amžiaus vaikų tėvams (globėjams) ir mokytojams – „Išmaniosios technologijos ir informatinis mąstymas“(2020). Šiame leidinyje tėvams pateikiami šie saugumo reikalavimai: „Visuose išmaniuosiuose įrenginiuose būtina įdiegti vaikams netinkamo turinio filtravimo programas. Ikimokyklinuką ar priešmokyklinuką, besinaudojantį įrenginiais, prijungtais prie interneto, taip pat visuomet turi prižiūrėti suaugusysis, palikti vaiko su įrenginiu vieno – negalima.“ Šis trumpas aprašas tėvams nesuteikia detalesnės informacijos apie metodus turinio vertinimui internete, taip pat neinformuoja apie nemokamas turinio filtravimo programas ar edukacines internetines erdves skirtas saugiai vaiko veiklai internete. Tiek šis leidinys, tiek Švietimo, mokslo ir sporto ministerijos informacinis leidinių puslapis neįtraukia kitų institucijų vykdomų projektų ir iniciatyvų vaikų saugumo internete klausimais, kurie galėtų praplėsti tėvų ir mokytojų žinias. RRT vysto šiuos informuotumo didinimo projektus: esaugumas.lt, svarusinternetas.lt , nebūkberyšio.lt, taip pat teikia informacinius leidinius ir atsako į iškilusius klausimus susijusius su saugumu naudojantis interneto paslaugomis. Taip pat, svarbu didintų tėvų informuotumą ir duomenų apsaugos srityje. Valstybinė duomenų inspekcija vykdo edukacinį projektą „Uždėk filtrą“, taip pat pateikia „EBPO rekomendacijos dėl vaikų skaitmeninėje aplinkoje“ leidinį, svetainės skiltis „Vaikams ir jaunimui“ publikuoja daugiau aktualios informacijos vaiko duomenų apsaugos srityje. Taigi galima daryti išvadą, kad institucijos veikia izoliuotai savo kompetencijų srityse ir ši informacija nėra prieinama centralizuotai. 12 paveikslėlyje pateikiamas kibernetinio saugumo informacijos sklaidos modelis švietimo pagrindu.



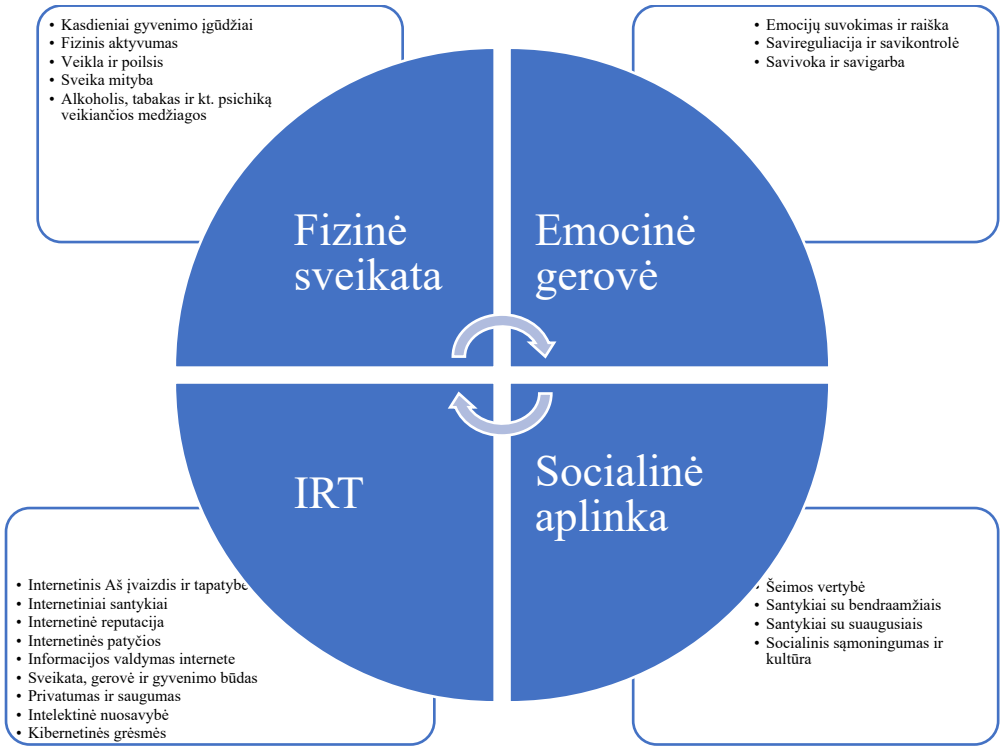
12 pav. Kibernetinio saugumo informacijos sklaida švietimo pagrindu

Šis modelis pabrėžia tarpinstitucinio bendradarbiavimo svarbą kibernetinio saugumo informuotumo didinimo tėvų ir pedagogų, taip pat ir vyresnio amžiaus vaikų tarpe. Centralizuotas ir koordinuotas

savalaikės informacijos teikimas plėtoja kibernetinio saugumo kultūrą ir kompetencijas individualiame lygyje. Taip pat, programos turi atitikti šiuos reikalavimus išskirtus literatūros analizės metu:

- Programos turi būti kruopščiai suplanuotos naudojant formalizuotą metodiką, kurioje atsižvelgiama į aspektus, susijusius tiek su tiek su tiksline auditorija, tiek su aplinka, kurioje jie veikia.
- Programos turėtų būti sukurtos atsižvelgiant į aiškiai apibrėžtą rezultatą arba tikslą.
- Besimokantieji turi būti ne tik mokomi, kaip elgtis konkrečioje situacijoje, bet ir kodėl jie turėtų taip elgtis.
- Mokymosi medžiaga turėtų būti pritaikyta individualiai.

Ugdymo programos rengiamos koncentruojantis į individualius vaiko poreikius taip pat visapusišką vaiko asmenybės vystymą ir reikiamų kompetencijų ir įgūdžių lavinimą. Siekiant užtikrinti nuoseklų ugdymo programų vystymą esminiu rodikliu turi būti laikomas šiuolaikinio vaiko pasaulis. Remiantis ugdymo programų turiniu ir kibernetinio saugumo kultūros pagrindu, 13 paveikslėlyje pateikiama šiuolaikinio vaiko pasaulėvoka.



13 pav. Šiuolaikinio vaiko pasaulėvoka

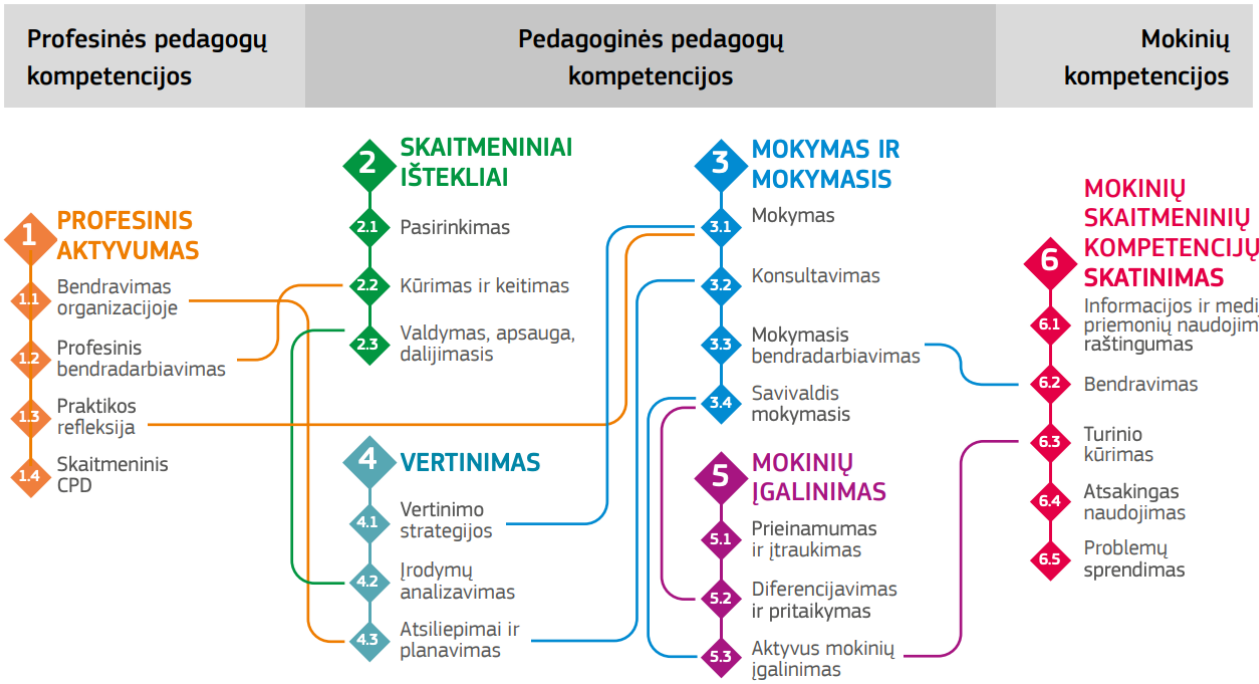
Ši pasaulėvoka įtraukia ir skaitmenį pasaulį, kuriame jis kuria savo identitetą, tad visi išorinio pasaulio veiksniai aktualizuojami IT dalyje tame tarpe ir kibernetinės grėsmės. Svarbu pabrėžti ir vizualizuojamą skaitmeninio pasaulio ir kibernetinio saugumo daugiadisciplinišKumą. Ugdymo programos turi ne tik

integruoti IRT kaip priemonę kitų disciplinų ugdymui, bet ir didelį dėmesį skirti individualiai IRT ugdymo programai, neapsiribojant vien technine didaktika.

Pedagogų kompetencijos tiek komunikacijoje su tėvais (globėjais), tiek ugdymo programų įgyvendinime yra esminis kriterijus. Lietuvos Švietimo strategijoje teigiama: „Jų kompetencija, asmeninės savybės, motyvacija, kūrybiškumas ir noras nuolat tobulėti, gebėjimas perimti gerąją praktiką yra pagrindinis Lietuvos švietimo sėkmės matas.“ Pedagogo profesija susiduria su greitai besikeičiančiais poreikiais, kuriems reikalingas platus ir sudėtingesnis nei anksčiau kompetencijų rinkinys.

Lietuvos švietimo įstatyme 23 straipsnio antroje dalyje numatoma: „[...] mokyklai ir mokytojui padedama tobulinti veiklą, siekti geresnės švietimo kokybės konsultuojant, atliekant mokyklos veiklos kokybės įsivertinimą ir išorinį vertinimą bei sudarant sąlygas mokytojams tobulinti kvalifikaciją“. Lietuvos Respublikos Švietimo ir mokslo ministro įsakymas „Dėl reikalavimų mokytojų kompiuterinio raštingumo programoms patvirtinimo“ (2018), pateikia mokytojų kompetencijų kėlimo programų reikalavimus ir vertinimo būdų rekomendacijas. Įsakymas parengtas DigComp 2.1 ir DigCompEdu programų rekomendacijomis. Taip pat, ES Tarybos rezoliucija dėl Europos bendradarbiavimo švietimo ir mokymo srityje strateginės programos siekiant sukurti Europos švietimo erdvę ir imtis veiksmų vėlesniu laikotarpiu (2021–2030 m.) pabrėžia mokymo meistriškumo skatinimą visais švietimo ir mokymo lygiais, efektyviai organizuojant mokymąsi ir struktūrines paskatas, skatinant tinkamus paramos mechanizmus, infrastruktūrą ir mokymo medžiagą bei moksliniais tyrimais pagrįstą mokytojų rengimą.

Kibernetinis saugumas ir su juo siejama tematika reikalauja nuolatinio tarptautinio bendradarbiavimo informuotumo ir kompetencijų lygio palaikymui. Tai aktualu ne tik kibernetinio saugumo profesionalams, bet ir pedagogams. Siekiant užtikrinti pedagogų tarptautinį kompetencijų lygį turi būti integruota tarptautinė IRT kompetencijų vertinimo kėlimo sistema. Redecker Christine (2017) pristatė Europos pedagogų skaitmeninių kompetencijų sistemą („DigCompEdu“) (žr. 14 pav.).



Šaltins: Europos pedagogų skaitmeninių kompetencijų sistema „DigCompEdu“, 2017.

14 pav. Europos pedagogų skaitmeninių kompetencijų sistema.

Europos pedagogų skaitmeninių kompetencijų sistemos (2017) nustatomas šis tikslas: „[...] identifikuoti ir aprašyti skaitmenines pedagogų kompetencijas. Pateikiamos į 6 sritis suskirstytos 22 pagrindinės kompetencijos. 1 sritis skirta platesnei profesinei aplinkai, t. y. pedagogų kompetencija naudoti skaitmenines technologijas profesiniuose santykiuose su kolegomis, mokiniais, tėvais ir kitomis suinteresuotomis šalimis, siekiant savo pačių profesinio tobulėjimo bei dėl bendrų organizacijos interesų. 2 sritis apima kompetencijas, kurių reikia efektyviai ir atsakingai naudoti skaitmeninius išteklius siekiant kurti ir dalytis mokymosi tikslais. 3 sritis apima mokymo ir mokymosi srities skaitmeninėms technologijoms tvarkyti bei organizuoti skirtas kompetencijas. 4 srities kompetencijos skirtos naudoti skaitmenines strategijas atliekant vertinimą. 5 sritis skirta į mokinį orientuotam mokymui ir mokymosi strategijoms skirtų skaitmeninių technologijų potencialui. 6 srityje nurodomos skaitmeniniam mokinių raštingumui gerinti reikalingos specialios pedagoginės kompetencijos. Kiekvienai kompetencijai suteikiamas pavadinimas ir trumpas aprašas“. Šios sistemos tarptautinė adaptacija suteikia motyvacijos pedagogams vystant kompetencijas tarptautiniu lygiu ir garantuoja savalaikę informaciją.

Apibendrinant analizės rezultatus galima išskirti šias esmines kibernetinio saugumo kultūros plėtojimo kryptis:

- centralizuota informacijos sklaida ir projektai švietimo sektoriui. Pateikiamas turinys turi būti personalizuotas ir pritaikytas tam tikrai grupei: tėvai (globėjai), pedagogai ir vaikai.

- Šiuo metu bendrojo ugdymo programų turinys nevysto kibernetinio saugumo kultūros mokinių tarpe. Tačiau pedagogai įtraukia IRT saugumo pagrindus į dėstomas temas savo kompetencijų ribose. Projekto „Mokykla 2030“ ruošiamos ugdymo programos yra stipriai pažengusius IRT srities kompetencijų plėtojime, tame tarpe ir kibernetinio saugumo. Siekiant nuosekliai plėtoti ugdymo programų turinį sukurta vaiko pasaulėvoka įtraukiant ir IRT, kuria turėtų būti grindžiamas ir ugdymo programų vystymas.
- Pedagogų kompetencijos yra esminis kriterijus kiekvienos ugdymo programos įgyvendinimui. Spartūs technologiniai pokyčiai kasdieniuose procesuose reikalauja nuolatinio pedagogų kompetencijų kėlimo IRT srityje. DigCompEdu sistema suteikia galimybę konsoliduoti ir standartizuoti pedagogų kompetencijas ne tik nacionaliniu, bet ir tarptautiniu lygiu. Tai yra labai aktualu šiuo metu sparčiai vykstančiame globalizacijos kontekste.

IŠVADOS IR REKOMENDACIJOS

1.1 Mokslinės literatūros analizės metu nustatyta, kad kibernetinė erdvė yra apibrėžiama kaip žmonių socialinė sąveika palaikoma IRT įtraukiant ir technines priemones. Šios apibrėžties socialinis aspektas yra plačiai polemizuojamas ir tai įtakoja kibernetinės erdvės sampratos vystymą. Analizuojant įvairių tarptautinių organizacijų žodynus pateikiančius kibernetinės erdvės apibrėžtis, galima konstatuoti, kad sąvoka grindžiama organizacijos veiklos sritimi ir taikoma politika. Tai formuoja kibernetinio saugumo kultūros plėtros problematiką tarptautiniu lygiu. Taip pat, analizuojant kibernetinio saugumo kultūros teorinius aspektus nustatyta kibernetinio saugumo ir informacinio saugumo sąryšio bei kiekvieno termino naudojimo ribų apibrėžties aktualumas siekiant pateikti informuotumo didinimo projektams, mokymams ir kitoms sritims skirtą informaciją. Tačiau takoskyra tarp šių dviejų terminų pilnai suvokiama tik profesionaliu, ekspertiniu lygiu. Šių sąvokų asimiliacija gali turėti neigiamą poveikį ateities kibernetinio saugumo kultūros vystymui.

1.2 Remiantis atlikta literatūros analize galima daryti išvadą, kad kibernetinio saugumo kultūros samprata ir koncepcija yra apibrėžiama ir priklauso nuo tyrimo objekto. Taigi nėra vienareikšmės kibernetinio saugumo kultūros apibrėžties, kuri galėtų būti laikoma pagrindu kibernetinio saugumo kultūros teoriniuose ir empiriniuose tyrimuose. Tačiau, visuose atliktuose tyrimuose pateikiami kibernetinio saugumo kultūrą įtakojantys išoriniai ir vidiniai faktoriai yra orientuoti į žmogaus elgesį. Tai suponuoja kibernetinio saugumo kultūros plėtojimą informuotumo didinimo, mokymo ir švietimo programomis. Moksliniai tyrimai šia tematika koncentruojasi organizaciniame lygyje, plačiai analizuojamos SETA programos. Išskirti du esminiai faktoriai į kuriuos turi būti atsižvelgta kuriant informavimo kampanijas: pateikimo formato dalyviams patrauklumas ir dalyvio įsitraukimo didinimas.

2. Remiantis kokybiniu ekspertų nuomonės vertinimu, nustatytos keturios pagrindinės kibernetinio saugumo kultūros plėtojimo kryptys: saugaus interneto naudojimo pagrindai turi būti pateikiami jau ankstyvojo amžiaus ugdymo programose, pedagogų kompetencijų kėlimo konsoliduota sistema, vaikų turimų kompetencijų vertinimo įtraukimas vystant IT ugdymo programas ir IT ugdymo programų adaptavimo sistema, kuri leidžia greitai įdiegti reikiamus pokyčius prisitaikant prie sparčios technologinės raidos.
3. Tyrimo metu iškelta pirmoji hipotezė buvo patvirtinta. IT bendrojo ugdymo programų turinys neįtraukia įvairiapusiško kibernetinio saugumo traktavimo ir su juo siejamų saugumo elgesio normų. Nustatytas stiprus Jungtinėje Karalystėje ugdomų vaikų IT kompetencijų atotrūkis lyginant su Lietuva. Antroji hipotezė taip pat buvo patvirtinta, Kibernetinio saugumo įstatymas neapibrėžia centralizuoto ir sistemingo informuotumo didinimo švietimo srityje. Lietuvos ikimokyklinio ir

bendrojo ugdymo programų analizės metu nustatytos trys kibernetinio saugumo kultūros plėtojimo kryptys. Pirmoji pabrėžia centralizuotos saugumo informacijos sklaidos švietimo sektoriui poreikį, kuri turi būti personalizuota ir pritaikyta tikslinei grupei: tėvai (globėjai), pedagogai ir vaikai (žr. 12 pav.). Antroji kryptis, koncentruojasi į dabartinį ugdomo vaiko portretą, kuris yra laikomas nuoseklios ugdymo programos vystymo pagrindu. To pasekoje, sukurtas vaiko pasaulėvokos modelis, kuris pabrėžia IRT svarbą kasdieniame vaiko gyvenime (žr. 13 pav.). Trečiasis plėtros elementas yra konsoliduotas pedagogų kompetencijų IT srityje kėlimas.

Rekomendacijos:

- Kibernetinio saugumo kultūros plėtojimas ikimokyklinių ir bendrojo ugdymo programų pagrindu sumažintų su kibernetiniu saugumu susijusias rizikas ilgalaikėje perspektyvoje. Šia tematika moksliniai tyrimai yra pradinėje vystymo stadijoje. Tačiau šiuo metu atliktų tyrimų pagrindu galima išskirti šiuos esminius informuotumo didinimo aspektus: bendrąsias problemos, kurios įtraukia kibernetines grėsmes, techninius sprendimus ir socialinę kibernetinės erdvės problematiką (internetiniai santykiai , internetinės patyčios ir kt.). Taip pat, vykdant informuotumo didinimo programas svarbu atkreipti dėmesį į turinio pateikimą, įsivertinimo galimybes ir sužaidybinimo elementus. Sužaidybintos, vaikų raidą atitinkančios programėlės gali tapti kibernetinio saugumo kultūros plėtojimo pagrindu. Mokyklos gali išplėtoti įvairias programas, rengti turnyrus ir kitas veiklas siekiant įtraukti visą mokyklos bendruomenę.
- Šiuo metu rengiamas Lietuvos informatikos ugdymo programos atnaujinimo projektas stipriai išplečia IT kompetencijas, taip pat įtraukia saugumo modulį. Tačiau ikimokyklinio ir pradinio ugdymo programose IT kompetencijų vystymas vis dar stipriai siejamas su pedagogo kompetencijomis šioje srityje. Atsižvelgiant į tai, kad pedagogas vysto visas vaikų kompetencijas šiose amžiaus grupėse reikia numatyti papildomus resursus (metodologinius, žmogiškuosius išteklius), kurie užtikrintų nuoseklų ir kokybišką vaikų skaitmeninių kompetencijų vystymą.
- IT ugdymo programos turi būti peržiūrimos kasmet, greitai adaptuojamos ir praktiškai taikomas siekiant užtikrinti savalaikią informaciją moksleiviams ir pedagogams.
- Pedagogų kompetencijų kėlimo planą rekomenduojama vystyti DigCompEdu sistemos pagrindu (žr. 14 pav.).

LITERATŪROS SĄRAŠAS

1. Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3), 237-248. doi: 10.1080/0144929X.2012.708787.
2. Al Shamsi, A. A. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. Int. J. *Inf. Technol. Lang. Stud,* 3(2), 8-29. doi: 10.13140/RG.2.2.28488.14083.
3. Alfawaz, S., Nelson, K., ir Mohannak, K. (2010). Information security culture: a behaviour compliance conceptual framework. *In Information Security 2010: AISC'10 Proceedings of the Eighth Australasian Conference on Information Security [Conferences in Research and Practice in Information Technology, Volume 105]* (p. 51-60). Australian Computer Society. Prieiga per internetą: https://www.researchgate.net/publication/40496478_Information_security_culture_A_behaviour_compliance_conceptual_framework.
4. AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 49, (p. 567–575). doi: 10.1016/j.chb.2015.03.054.
5. Antunes, M., Maximiano, M., Gomes, R., ir Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, 1(2), 219-238. doi: 10.3390/jcp1020012.
6. Antunes, M., Silva, C. ir Marques, F. (2021). An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context. *Applied Sciences, 11*(23), 11269. doi: 10.3390/app112311269.
7. Aurigemma, S. ir Mattson, T. (2019). Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research. *Journal of the Association for Information Systems*, 20(12). doi: 10.17705/1jais.00583
8. Bada, M., Sasse, A. M. ir Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. doi: 10.48550/arXiv.1901.02672.
9. Baležentis, A. ir Žalimaitė, M. (2011). Ekspertinių vertinimų taikymas inovacijų plėtros veiksnių analizėje: Lietuvos inovatyvių įmonių vertinimas. *Vadybos mokslas ir studijos-kaimo verslų ir jų infrastruktūros plėtrai, (3),* 23-31.
10. Batteau, A. W. (2011). Creating a culture of enterprise cybersecurity. *International Journal of Business Anthropology*, 2(2). Prieiga per internetą: https://www.researchgate.net/profile/Allen-Batteau/publication/266068991_Creating_a_Culture_of_Enterprise_Cybersecurity/links/56b2815308aed7ba3fede925/Creating-a-Culture-of-Enterprise-Cybersecurity.pdf.
11. Blum, D. (2020). Institute Resilience Through Detection, Response, and Recovery. In *Rational Cybersecurity for Business* (p. 259-295). Apress, Berkeley, CA. doi: 10.1007/978-1-4842-5952-8_9.

12. Bőthe, B., Tóth-Király, I., Zsila, Á., Griffiths, M. D., Demetrovics, Z. ir Orosz, G. (2018). The development of the problematic pornography consumption scale (PPCS*). The Journal of Sex Research, 55*(3), 395-406. doi: 10.1080/00224499.2017.1291798.
13. Cabello-Hutt, T., Cabello, P., ir Claro, M. (2018). Online opportunities and risks for children and adolescents: The role of digital skills, age, gender and parental mediation in Brazil. *new media & society*, 20(7), 2411-2431. doi: 10.1177/1461444817724168.
14. Cameron, K. S. ir Quinn, R. E. (2011). Diagnosing and changing organizational culture: Based on the competing values framework. John Wiley & Sons. Prieiga per internetą: http://ludmila-petrashko.com.ua/assets/files/kurs/Traning-CMP/Literatura/kameron_kuin_ok.pdf.
15. Clark, D. (2010). Characterizing cyberspace: past, present and future. *MIT CSAIL, Version, 1*, 2016-2028.
16. D'Arcy, J. ir Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. Information Management & Computer Security. doi: 10.1108/IMCS-08-2013-0057.
17. Da Veiga, A. (2015). An Information Security Training and Awareness Approach (ISTAAP) to Instil an Information Security-Positive Culture. In *HAISA* (p. 95-107). Prieiga per internetą: https://uir.unisa.ac.za/bitstream/handle/10500/19057/CSCAN-OA-261%20ISTAAP%20HAISA%202015.pdf?sequence=1.
18. Da Veiga, A. (2016, July). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In *2016 SAI computing conference (SAI)* (p. 1006-1015). IEEE. doi: 10.1109/SAI.2016.7556102
19. Da Veiga, A. ir Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 49*, 162-176. doi: 10.1016/j.cose.2014.12.006.
20. Da Veiga, A., ir Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & security*, 29(2), 196-207. doi: 10.1016/j.cose.2009.09.002
21. Dunn Cavelty, M. (2013). A resilient Europe for an open, safe and secure cyberspace. *UI Occassional Papers, 23*. doi: 10.2139/ssrn.2368223.
22. EBSCO (2022). *About - Organisation for Economic Co-operation and Development.* Prieiga per internetą: https://www.oecd.org/digital/global-forum-digital-security/about/
23. ECS (2017). *Overview of existing Cybersecurity standards and certification schemes*. Prieiga per internetą: http://www.ecs-org.eu/documents/uploads/state-of-the-art-syllabus-v1.pdf.
24. Edgell, S., ir Granter, E. (2019). *The sociology of work: Continuity and change in paid and unpaid work*. Sage.

25. ENISA (2016). *Definition of Cybersecurity - Gaps and overlaps in standardisation.* Prieiga per internetą: https://www.enisa.europa.eu/publications/definition-of-cybersecurity.
26. ENISA (2010). *The new user's guide: How to raise information security awareness.* Prieiga per internetą: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide/at_download/fullReport.
27. ENISA (2017). *ENISA overview of cybersecurity and related terminology.* Prieiga per internetą: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology.
28. ENISA, 2018. *Cyber Security Culture in organisations*. Prieiga per internetą: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations.
29. EU (2020). *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient.* Prieiga per internetą: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391.
30. EU (2020). *The EU's Cybersecurity Strategy for the Digital Decade.* Prieiga per internetą: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.
31. Furman, S., Theofanos, M. F., Choong, Y. Y. ir Stanton, B. (2011). Basing cybersecurity training on user perceptions. *IEEE Security & Privacy, 10*(2), 40-49. doi: 10.1109/MSP.2011.180.
32. Furnell, S., ir Thomson, K. L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. Computer fraud & security, 2009(2), 5-10. doi: 10.1016/S1361-3723(09)70019-3.
33. Gañán, C. H., Ciere, M., ir van Eeten, M. (2017, October). Beyond the pretty penny: The economic impact of cybercrime. *In Proceedings of the 2017 new security paradigms workshop* (p. 35-45). doi: 10.1145/3171533.3171535.
34. Gangire, Y., Da Veiga, A., ir Herselman, M. (2019, March). A conceptual model of information security compliant behaviour based on the self-determination theory. Pranešimas konferencijai *2019 Conference on Information Communications Technology and Society (ICTAS*) (p. 1-6). IEEE. doi: 10.1109/ICTAS.2019.8703629.
35. Gcaza, N., von Solms, R., ir van Vuuren, J. J. (2015). An Ontology for a National Cyber-Security Culture Environment. *HAISA* (p. 1-10). Prieiga per internetą: https://www.researchgate.net/publication/306292545_An_Ontology_for_a_National_Cyber-Security_Culture_Environment.
36. Georgiadou, A., Mouzakitis, S., Bounas, K. ir Askounis, D. (2020). A Cyber-Security Culture Framework for Assessing Organization Readiness. Journal of Computer Information Systems, 0(0), (p. 1–11). doi: 10.1080/08874417.2020.1845583.
37. Ghernaouti-Helie, S. (2013). *Cyber power: Crime, conflict and security in cyberspace.* Crc Press.

38. Google Trends (2022). *Palyginimas*. Prieiga per internetą: https://trends.google.com/trends/explore?date=2012-02-05%202022-03-05&q=information%20security,cyber%20security.
39. Gražienė, V., Jonynienė, V., Kondratavičienė, R., Markevičienė, N., Poškevičienė, E., Vaišvila, H., Vizbarienė, A. (2021). *Projektų metodas priešmokyklinėje grupėje.* Prieiga per internetą: https://sodas.ugdome.lt/metodiniai-dokumentai/atsisiusti/17151/e37ae86c-6da9-4986-ac7e-562f29932100
40. Gražienė, V., Jonynienė, V., Kondratavičienė, R., Markevičienė, N., Poškevičienė, E., Vaišvila, H., Vizbarienė, A. (2021). *Informatinis mąstymas priešmokykliniame amžiuje.* Prieiga per internetą: http://www.ukvm.lt/bylos/el_biblioteka/Ikimokyklinio_ugdymo_padejejas/Patirciu_erdves.Informatinis_mastymas.pdf
41. Gzaca, N. ir von Solms, R. (2017) A strategy for a cybersecurity culture: A South African perspective. *Electronic Journal of Information Systems in Developing Countries* 80(6): 1–17. doi: 10.1002/j.1681-4835.2017.tb00590.x.
42. Hall, M. (2016). Why people are key to cyber-security. Network Security, 2016(6), 9-10. doi: 10.1016/S1353-4858(16)30057-5
43. Hengstler, S. ir Pryazhnykova, N. (2021). Reviewing the Interrelation Between Information Security and Culture: Toward an Agenda for Future Research.
44. Hofstede, G., Hofstede, G. J., ir Minkov, M. (2005). *Cultures and organizations: Software of the mind* (Vol. 2). New York: Mcgraw-hill. Prieiga per internetą: http://homecont.ro/pitagora/Hofstede-4-dimensiuni.pdf.

https://kam.lt/download/70748/2020%20m.%20nacionalinio%20kibernetinio%20saugumo%20b%C5%ABkl%C4%97s%20ataskaita%20el.%20versija.pd

45. Huang, K., ir Pearlson, K. (2019, January 8). For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. Pranešimas konferencijoje 52nd Hawai International Conference on System Sciences. doi: 10.24251/HICSS.2019.769
46. IdentityForce (2020). *2020 Data Breaches.* Prieiga per internetą: https://www.identityforce.com/blog/2020-data-breaches
47. Ikimokyklinio ugdymo programa (2022). Prieiga per internetą: https://smsm.lrv.lt/web/lt/smm-svietimas/svietimo-sistema-ikimokyklinis-ugdymas/ikimokyklinio-ugdymo-programa
48. Informatikos ugdymo bendrosios programos projektas (2021). Prieiga per internetą: https://www.mokykla2030.lt/informatikos-ugdymas/.
49. Ioannou, Stavrou ir Bada (2019, June). Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination. Pranešimas

63. Lietuvos Respublikos švietimo ir ministerija (2015). *Ikimokyklinio ugdymo metodinės rekomendacijos.* Prieiga per internetą: https://www.ikimokyklinis.lt/uploads/files/dir1049/dir52/dir2/17_0.php.
64. *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://www.e-tar.lt/portal/lt/legalAct/TAR.F75FE2733AF1/asr.
65. *Lietuvos Respublikos Švietimo ir mokslo Ministro 2018 m. birželio 25 d. įsakymas Nr. V-598 ,, Dėl ikimokyklinio ugdymo programų kriterijų aprašo"*. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/599d489078af11e89188e16a6495e98c?jfwid=q8i88m58y.
66. *Lietuvos Respublikos Švietimo ir mokslo Ministro įsakymas 2008 m. rugpjūčio 26 d. Nr. ISAK-2433 ,,Dėl pradinio ir pagrindinio ugdymo bendrųjų programų patvirtinimo"*. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.326307/PdlziPcGuv.
67. *Lietuvos Respublikos Švietimo įstatymas, (1991).* Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.1480/asr.
68. *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.
69. Lietuvos švietimo ministerija (2013). *Valstybinė švietimo 2013-2022 metų strategija.* Prieiga per internetą: https://www.nsa.smm.lt/wp-content/uploads/2018/04/Valstybine-svietimo-strategija-2013-2020_svietstrat.pdf
70. Livingstone, S., Mascheroni, G., ir Staksrud, E. (2015). Developing a framework for researching children's online risks and opportunities in Europe. Prieiga per internetą: http://eprints.lse.ac.uk/64470/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_EU%20Kids%20Online_EU%20Kids%20Online_Developing%20framework%20for%20researching_2015.pdf.
71. Luthra, K. (2020). Can humans be patched? A short current state review. Prieiga per internetą: https://www.diva-portal.org/smash/get/diva2:1481074/FULLTEXT01.pdf.
72. Malik, J. K., ir Choudhury, S. (2019). A Brief review on Cyber Crime-Growth and Evolution. *Pramana Research Journal*, 9(3), 242. doi: 10.36349/easjehl.2019.v02i03.005
73. Manap, N. A., Rahim, A. A. ir Taji, H. (2015). Cyberspace identity theft: The conceptual framework. *Mediterranean Journal of Social Sciences, 6*(4), 595. doi: 10.5901/mjss.2015.v6n4s3p595.
74. Marotta, A. ir Pearlson, K. (2019). A culture of cybersecurity at Banca Popolare di Sondrio. Prieiga per internetą: https://cams.mit.edu/wp-content/uploads/BPS-Case-Study-03012019.pdf.

konferencijoje *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (p. 1-4). IEEE. doi: 10.1109/CyberSecPODS.2019.8885240.

50. ISO (2012). *Information technology — Security techniques — Guidelines for cybersecurity*. Prieiga per internetą: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en.
51. ISO (2018). *Information technology — Security techniques — Information security management systems — Overview and vocabulary.* Prieiga per internetą: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en.
52. ITU (2008). *Overwiew of cybersecurity*. Prieiga per internetą: https://www.itu.int/rec/T-REC-X.1205-200804-I
53. Jurkonienė, I. (2017). *Tarpinstitucinio bendradarbiavimo stiprinimo koncepcija.* Prieiga per internetą: http://kurklt.lt/wp-content/uploads/2016/10/tarpinstitucinio-bendradarbiavimo-stiprinimo-koncepcija-final.pdf.
54. KAM (2020). *Nacionalinė kibernetinio saugumo ataskaita (2020).* Prieiga per internetą*:*
55. Kirlappos, I., ir Sasse, M. A. (2011). Security education against phishing: A modest proposal for a major rethink. *IEEE Security & Privacy, 10*(2), 24-32. doi: 10.1109/MSP.2011.179.
56. Kramer, F. D., Starr S. H. ir Wentz L. K. 2009. *Cyber Power and National Security.* Prieiga per internetą*:* https://ndupress.ndu.edu/Publications/Article/1216674/cyberpower-and-national-security/.
57. Kreps, D. M. (1990). Corporate culture and economic theory. *Perspectives on positive political economy, 90*(109-110), 8.
58. Kruger, H. A., ir Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & security, 25*(4), 289-296. Prieiga per internetą: https://www.researchgate.net/profile/Hennie-Kruger/publication/222422461_A_prototype_for_assessing_information_security_awareness/links/5cd04374458515712e95ad03/A-prototype-for-assessing-information-security-awareness.pdf
59. Lacey, D. (2009). Managing the Human Factor in Information Security: How to win over staff and influence business managers. John Wiley & Sons.
60. Lahcen, R. A. M., Caulkins, B., Mohapatra, R., ir Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, 3(1), 1-18. doi: 10.1186/s42400-020-00050-w.
61. Leidner, D. E., ir Kayworth, T. (2006). A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS quarterly*, 357-399. doi: 10.2307/25148735.
62. *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.

75. Masrek, M. N., Harun, Q. N. ir Zaini, M. K. (2018). The Development of an Information Security Culture Scale for the Malaysian Public Organization. *International Journal of Mechanical Engineering and Technology (IJMET), 9(7)*, 1255–1267. Prieiga per internetą: https://www.researchgate.net/publication/326835969_THE_DEVELOPMENT_OF_AN_INFORMATION_SECURITY_CULTURE_SCALE_FOR_THE_MALAYSIAN_PUBLIC_ORGANIZATION.
76. Menard, P. ir Shropshire, J. (2016). Training Wheels: A New Approach to Teaching Mobile Device Security. Prieiga per interneta: https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1002&context=ccerp.
77. Michalo, M. (2021). *The contribution of fostering a cyber security culture in organizations' cyber resilience* (magistras). Prieiga per internetą: https://www.researchgate.net/publication/351710901_The_contribution_of_fostering_a_cyber_security_culture_in_organizations'_cyber_resilience.
78. Mokwetli, M. ir Zuva, T. (2018, August). Adoption of the ICT Security Culture in SMME's in the Gauteng Province, South Africa. Pranešimas konferencijooje *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)* (p. 1-7). IEEE.
79. NATO (2020). *Allied Joint Doctrine for Cyberspace Operations.* Prieiga per internatą: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.
80. Nel, F ir Drevin, L. (2019). Key elements of an information security culture in organisations. *Information & Computer Security, 27*(2), 146–164. doi: 10.1108/ICS-12-2016-0095.
81. Ngoqo, B., ir Flowerday, S. V. (2015). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *computers & security, 53*, 132-142. doi: 10.1016/j.cose.2015.05.011
82. NIST (2003). *Computer security.* Prieiga per internetą: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf.
83. O'Brien, J., Islam, S., Bao, S., Weng, F., Xiong, W., ir Ma, A. (2013). Information security culture: Literature review. Prieiga per internetą: https://minerva-access.unimelb.edu.au/items/75dde69e-853f-54c0-9bea-d72c9de53be0.
84. OECD (2019). *PISA 2021 ICT Framework.* Prieiga per internetą: https://www.oecd.org/pisa/sitedocument/PISA-2021-ICT-Framework.pdf
85. Olivos, O. (2012). Creating a Security Culture Development Plan and a case study. *HAISA* (p. 13-32).

86. Ottis R., Lorents P. (2010). *Cyberspace: Definition and Implications.* Pranešimas konferencijoje International Conference on Information Warfare and Security: Dayton, OH, US.
87. Özkan, B.Y.; Spruit, M. Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda. *In Research Anthology on Artificial Intelligence Applications in Security*; IGI Global: Hershey, PA, USA, 2021; p. 1252–1278. doi: 10.4018/IJSR.20190701.oa1
88. Pagrindinio ugdymo programa (2021). Prieiga per internetą: https://smsm.lrv.lt/web/lt/ugdymo_programos.
89. Parsons, K., McCormac, A., Butavicius, M., ir Ferguson, L. (2010). *Human factors and information security: individual, culture and security environment*. DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION EDINBURGH (AUSTRALIA) COMMAND CONTROL COMMUNICATIONS AND INTELLIGENCE DIV. Prieiga per internetą: https://apps.dtic.mil/sti/citations/ADA535944.
90. Perkins, E., Walls, A. ir Weiss, J. (2013). *Definition: Cybersecurity.* Prieiga per internetą: https://www.gartner.com/en/documents/2510116.
91. Pradinio ugdymo programa (2016). Prieiga per internetą: https://www.nsa.smm.lt/wp-content/uploads/2016/01/ugdpr_1priedas_pradinio-ugdymo-bendroji-programa.pdf.
92. Priešmokyklinio ugdymo programa (2022). Prieiga per internetą: https://smsm.lrv.lt/web/lt/smm-svietimas/svietimas-priesmokyklinis-ugdymas/priesmokyklinio-ugdymo-programa
93. Rahman, N., Sairi, I., Zizi, N., ir Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology, 10*(5), 378-382. Prieiga per internetą: http://www.ijiet.org/vol10/1393-JR419.pdf.
94. Rauf, A. (2019). *The Importance of Human Factor in Cybersecurity.* Prieiga per internetą: https://www.researchgate.net/publication/332539716_The_Importance_of_Human_Factor_in_Cybersecurity.
95. Redecker, C. (2017). *European framework for the digital competence of educators: DigCompEdu* (No. JRC107466). Joint Research Centre (Seville site).
96. Reid, R., ir Van Niekerk, J. (2014, August). From information security to cyber security cultures. In *2014 Information Security for South Africa* (p. 1-7). IEEE. doi: 10.1109/ISSA.2014.6950492
97. Roer, K. (2015). Build a security culture. IT Governance Ltd.
98. Ruhwanya, Z., ir Ophoff, J. (2019). Information security culture assessment of small and mediumsized enterprises in Tanzania. Pranešimas konferencijoje *International Conference on Social Implications of Computers in Developing Countries* (p. 776-788). Springer, Cham. doi: 10.1007/978-3-030-18400-1_63
99. Schein, E. H. (1990). Organizational culture. *American Psychologist, 45(2)*, 109–119. doi: 10.1037/0003-066X.45.2.109.

100. Schein, E. H. (2010). *Organizational culture and leadership* (Vol. 2). John Wiley & Sons.

101. Schlienger, T. ir Teufel, S. (2003). Information security culture-from analysis to change. *South African Computer Journal, 2003*(31), 46-52.Prieiga per internetą: https://hdl.handle.net/10520/EJC27949.

102. Shahibi, M. S., Rashid, R. M., Fakeh, S. K. W., Dollah, W. A. K. W. ir Ali, J. (2012). Determining factors influencing information security culture among ICT librarians. *Journal of Theoretical and Applied Information Technology, 37*(1). Prieiga per internetą: https://www.semanticscholar.org/paper/Determining-factors-influencing-information-culture-Shahibi-Rashid/f57955d768e3de62c0f899cd9c980f96e8c81e37#citing-papers.

103. Siponen, M. T. (2001). Five dimensions of information security awareness. *SIGCAS Comput. Soc., 31*(2), 24-29. doi: 10.1145/503345.503348.

104. Sisaneci, I., Akin, O., Karaman, M., ir Saglam, M. (2013, September). A Novel Concept For Cybersecurity: Institutional Cybersecurity. Pranešimas konferencijoje *6th International Conference on Information Security and Cryptology, Turkey, Ankara* (p. 89). Prieiga per internetą: https://www.researchgate.net/publication/299533127_Institutional_Cybersecurity_from_Military_Perspective.

105. Straub, D., Loch, K., Evaristo, R., Karahanna, E. ir Srite, M. (2002). Toward a theory-based measurement of culture. *Journal of Global Information Managemen*t (JGIM), 10(1), 13-23. doi: 10.4018/jgim.2002010102.

106. Sudeikienė, I (2020). *Išmaniosios technologijos ir informatinis mąstymas.* Prieiga per internetą: https://smsm.lrv.lt/uploads/smsm/documents/files/svietimas/pagrindinis/Ankstyvasis%20ugdymas%20ir%20IKT.pdf.

107. Tang, M., Li, M. G., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management, 17*(2), 179-186. doi: 10.1007/s10799-015-0252-2.

108. Tirumala, S. S., Sarrafzadeh, A., ir Pang, P. (2016, December). A survey on Internet usage and cybersecurity awareness in students. Pranešimas konferencijai *2016 14th Annual Conference on Privacy, Security and Trust (PST)* (p. 223-228). IEEE. doi: 10.1109/PST.2016.7906931.

109. Tolah, A., Furnell, S., ir Papadaki, M. (2017). *A Comprehensive Framework for Cultivating and Assessing Information Security Culture.* Pranešimas konferencijoje Eleventh International Symposium on Human Aspects of Information Security & Assurance. HAISA.

110. Tonye, W. S. (2019). The Human Side of Information Technology when Technical Controls Fails. *Global Journal of Computer Science and Technology*. Prieiga per internetą: https://computerresearch.org/index.php/computer/article/view/1861.

111. Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. *Information Technology & People*. doi: 10.1108/09593841211254358.

112. Tziarras, Z. (2014). The Security Culture of a Global and Multileveled Cybersecurity. In *Cyber-Development, Cyber-Democracy and Cyber-Defense* (p. 319-335). Springer, New York, NY. doi: 10.1007/978-1-4939-1028-1_13.

113. Uchendu, B., Nurse, J. R., Bada, M., ir Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109*, 102387. doi: 10.1016/j.cose.2021.102387.

114. UK National Curricullum (2014). Prieiga per ineternetą: https://www.gov.uk/government/collections/national-curriculum.

115. UNESCO (2003). *Recommendation Concerning the Promotion and Use of Multilingualism andUniversal Access to Cyberspace.* Prieiga per internetą: https://en.unesco.org/sites/default/files/en_recommendation_concerning_the_promotion_and_use_of_multilingualism_and_universal_access_to_cyberspace.pdf

116. UNICEF (2018). *Policy Guide on Children and Digital Connectivity*. Prieiga per internetą: https://www.unicef.org/esa/media/3141/file/PolicyLab-Guide-DigitalConnectivity-Nov.6.18-lowres.pdf.

117. United Nations (2021, March). *Final Substantive Report.* Pranešimas konferencijoje General Assembly.

118. US (2018). *U.S. Department of Homeland and Security Cyber Secuity Strategy.* Prieiga per internetą: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

119. Valcke, M., De Wever, B., Van Keer, H., ir Schellens, T. (2011). Long-term study of safe Internet use of young children. *Computers & Education, 57*(1), 1292-1305. doi: 10.1016/j.compedu.2011.01.010.

120. Vilkova, A., Litvishkov, V. M., ir Shvyrev, B. A. (2020). The Pedagogical Approach To The Development Of Information Security Culture. *In & S. Alexander Glebovich (Ed.), Pedagogical Education - History, Present Time, Perspectives, vol 87*. European Proceedings of Social and Behavioural Sciences (p. 777-783). European Publisher. doi: 10.15405/epsbs.2020.08.02.102

121. Von Solms, R., ir Van Niekerk, J. (2013). From information security to cyber security. *Computers & security*, 38, 97-102. doi: 10.1016/j.cose.2013.04.004.

122. Wash, R. (2010, July). Folk models of home computer security. *In Proceedings of the Sixth Symposium on Usable Privacy and Security* 1-16. Prieiga per internetą: https://www.rickwash.com/papers/rwash-homesec-soups10-final.pdf.

123. Wiley, A., McCormac, A. ir Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. Computers & Security, 88, 101640. doi: 10.1016/j.cose.2019.101640

124. World Economic Forum (2021). *The Global Risk Report 2021".* Prieiga per internetą: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf.

125. World Trade Organization (2017). *Electronic Commerce.* Prieiga per internetą: https://www.wto.org/english/thewto_e/minist_e/mc11_e/briefing_notes_e/bfecom_e.htm.

126. Zwilling, M., Lesjak, D., Natek, S., Phusavat, K. ir Anussornnitisarn, P. (2019, May). How to deal with the awareness of cyber hazards and security in (Higher) education. Pranešimas konferencijai *Thriving on future education, industry, business and society. Proceedings of the Makelearn and TIIM International Conference* (p. 433-439). Prieiga per internetą: http://www.toknowpress.net/ISBN/978-961-6914-25-3/papers/ML19-130.pdf.

127. Židžiūnienė, V (2011). Žydžiūnaitė, V. (2011). Baigiamojo darbo rengimo metodologija. *Mokomoji knyga. Klaipėda: Klaipėdos valstybinė kolegija.*

PRIEDAI

1. Kibernetinio saugumo požiūris mokyklose (CsA-S) klausimynas

Numeris	Klausimas
A1 *	Manau, kad yra saugu ignoruoti atnaujinimo įspėjimus iš kompiuterinės programinės įrangos.
A2	Aš žinau savo vaidmenį siekiant apsaugoti mokyklą nuo galimų kibernetinių nusikaltėlių.
A3	Manau, kad kiekvienas mokykloje turi atlikti savo vaidmenį siekiant apsisaugoti nuo kibernetinių nusikaltėlių grėsmių.
A4 *	Sunku pasakyti, kaip galėčiau padėti apsaugoti mokyklą nuo elektroninių nusikaltimų.
A5 *	Aš neturiu tinkamų įgūdžių, kad galėčiau apsaugoti mokyklą nuo elektroninių nusikaltimų.
A6	Manau, kad asmeninė informacija neturėtų būti atskleidžiama internete, būtent tai, kas aš esu, kur gyvenu ar kurią mokyklą lankau.
A7 *	Kompiuterinės sistemos suteikia visą apsaugą, kurios reikia mokyklai.
A8 *	Manau, kad pranešimas apie elektroninius nusikaltimus yra laiko švaistymas.
A9 *	Policijai trūksta pajėgumų veiksmingai kovoti su elektroniniais nusikaltimais.
A10 *	Manau, kad kibernetiniai nusikaltėliai yra labiau pažengę nei žmonės, kurie turėtų mus apsaugoti.
A11 *	Atsisiųsčiau medžiagą, kuriai taikomos autorinės teisės (vaizdus, dokumentus, vaizdo įrašus).
A12	Manau, kad kai žiūriu į su smurtu susijusį turinį mokykloje, skatinu tai dalindamasis ar komentuodamas.
A13 *	Nerimauju, kad jei pranešiu apie kibernetinę ataką policijai, tai gali pakenkti mokyklos reputacijai.
A14 *	Manau, kad būtų galima padaryti daugiau, siekiant bendrauti / skleisti / jautrinti kibernetinių nusikaltimų riziką asmenims mokykloje.
A15	Aš žinau, kad mokyklos naudoja IT politiką ir bando jos laikytis.
A16 *	Aš nežinau kaip pranešti apie kibernetinę ataką jei ji įvyktų.
A17 *	Nemanau, kad pranešti apie kibernetinę ataką, pradėtą iš mokyklos, yra mano atsakomybė.
A18 *	Nekreipiu dėmesio į mokyklos medžiagą apie kibernetinių nusikaltimų grėsmes.
A19	Esu įsitikinęs, kad galėčiau pastebėti kibernetinės atakos požymius.
A20	Manau, kai netinkamas turinys pasirodo internete turėčiau paprašyti pagalbos iš suaugusiojo.
A21	Manau, bet kuris asmuo mokykloje rizikuoja būti manipuliuojamas pasitikėjimą sukėlusių apgavikų.
A22 *	Manau, kad kibernetiniai nusikaltėliai taikosi į mokyklą tik tada, kai yra didelė finansinė nauda.
A23 *	Manau, kad programišiai ir kibernetiniai nusikaltėliai taikosi tik į įmones.
A24 *	Manau, kad tik tos įmonės, kurios atlieka mokėjimus naudodamiesi internetinėmis sistemomis, rizikuoja tapti kibernetinių nusikaltimų aukomis.
A25 *	Manau, kad turiu teisę visada būti internete, turėdamas prieigą prie visų interneto paslaugų.

* Neigiamai suformuluoti elementai buvo įvertinti priešingai, kad būtų galima atlikti tolesnę analizę.
Šaltinis: adaptuota pagal Antunes ir kt., 2021

2. Kibernetinio saugumo elgesys mokyklose (CSB-S) klausimynas

Numeris	Klausimas
B1	Slaptažodžių bendrinimas su draugais ir kolegomis.
B2	Slaptažodžių, kurie nėra labai sudėtingi(pvz., šeimos vardas ir gimimo data, raidžių eilutės), naudojimas arba kūrimas.
B3	To paties slaptažodžio naudojimas kelioms svetainėms.
B4	Internetinių saugojimo sistemų naudojimas keičiantis asmenine ar slapta informacija ir ją saugant.
B5	Mokėjimo informacijos įvedimas svetainėse, kuriose nėra aiškios saugos informacijos / sertifikavimo.
B6	Nemokamas viešasis Wi-Fi naudojimas.
B7	Pasikliaunate patikimų draugų ar kolegų patarimas dėl aspektų, susijusių su saugumu internete.
B8	Nemokamos antivirusinės programinės įrangos / programų atsisiuntimas iš nežinomo šaltinio.
B9	Išjungiu antivirusinę programinę įrangą savo kompiuteryje, kad galėčiau atsisiųsti informaciją iš svetainių.
B10	Naudojatės savo USB mokykloje, siekiant perkelti duomenis į jį.
B11 *	Tikrinate, ar jūsų išmaniajame telefone / planšetiniame kompiuteryje / nešiojamajame kompiuteryje / kompiuteryje yra atnaujinta programinė įranga.
B12	Skaitmeninės žiniasklaidos (muzikos, filmų, žaidimų) atsisiuntimas iš nelicencijuotų šaltinių.
B13	Dalinuosi savo dabartine buvimo vieta socialinėje erdvėje.
B14	Priimate draugų prašymus socialinėje erdvėje, nes atpažįstate nuotrauką.
B15	Spaudžiate nuorodas esančias nepageidaujamuose el. laiškuose iš nežinomo šaltinio.
B16	Siunčiate asmeninę informaciją nežinomiems asmenims internetu.
B17	Spustelėjate el. laiško gauto iš patikimo draugo ar kolegos saitus.
B18 *	Tikrinate ar nėra įdiegtos bet kokios antivirusinės programinės įrangos naujinimų.
B19	Siunčiatės duomenis ir medžiagą interneto svetainių nepatikrinant jų autentiškumo.
B20	Saugojate asmenines, šeimos ir draugo informaciją asmeniniame elektroniniame įrenginyje (pvz., išmaniajame telefone / planšetiniame kompiuteryje / nešiojamajame kompiuteryje).

***** Neigiamai suformuluoti elementai buvo įvertinti priešingai, kad būtų galima atlikti tolesnę analizę.
Šaltinis: adaptuota pagal Antunes ir kt., 2021

Chochlova L. (2022). *Kibernetinio saugumo kultūros plėtra švietimo srityje: ikimokyklinio ir bendrojo ugdymo įstaigų programų pagrindu.* Vilnius: Mykolo Romerio Universitetas.

ANOTACIJA

Magistro baigiamajame darbe išanalizuotas kibernetinio saugumo kultūros plėtojimas ikimokyklinio ir bendrojo ugdymo įstaigų programų pagrindu. Pirmajame skyriuje nagrinėjama kibernetinio saugumo kultūros koncepcija ir jos atributai. Pateikiama kibernetinės erdvės apibrėžties problematika ir jos įtaka kibernetinio saugumo sampratos vystymui. Apibrėžiami kibernetinio saugumo kultūros plėtojimo aspektai. Antrajame skyriuje pateikiama tyrimo metodologija. Kokybiniu tyrimu analizuojamas IT srities pedagogų požiūris į kibernetinio saugumo kultūros plėtojimą bendrojo ugdymo IT programose. Trečiame skyriuje analizuojamas Lietuvos ikimokyklinio ir bendrojo ugdymo programų turinys kibernetinio saugumo kultūros aspektu. Lietuvos ikimokyklinio ugdymo ir bendrojo IT ugdymo programų turinys lyginamas su Jungtinės Karalystės nacionaline kompiuterijos ugdymo programa. Skyriuje pateikiamos išvados ir problematika, kurios pagrindu formuluojamos pagrindinės kibernetinio saugumo vystymo kryptys ikimokyklinio ir bendrojo ugdymo programų pagrindu.

Pagrindiniai žodžiai: kibernetinio saugumo kultūra, kibernetinis saugumas, ugdymo programos.

Chochlova L. (2022). *Development of cyber security culture in the field of education on the basis of pre-school and general education institutions programmes.* Vilnius: Mykolas Romeris University.

ANNOTATION

The Master thesis analyzed the development of cybersecurity culture based on preschool and general education institutions programs. The first chapter deals with the concept of a cybersecurity culture and its attributes. The problems of the definition of cyberspace and its impact on the development of the cybersecurity concept are presented. Development aspects of a cybersecurity culture are defined. The second section provides a methodology for the study. Qualitative research analyses the attitude of IT educators to the development of cybersecurity culture in education IT programs. The third chapter analyses the content of Lithuanian pre-school and general education programs from the point of view of cybersecurity culture. The content of Lithuanian pre-school and general IT education programs are compared with the National Computing Curriculum of the United Kingdom. The section presents conclusions and issues, based on which the main directions of cybersecurity development are formulated for pre-school and general education curricula.

Key words: cybersecurity culture, cybersecurity, educational programs.

Chochlova L. (2022). *Kibernetinio saugumo kultūros plėtra švietimo srityje: ikimokyklinio ir bendrojo ugdymo įstaigų programų pagrindu.* Vilnius: Mykolo Romerio Universitetas.

SANTRAUKA

Kibernetinio saugumo kultūros vystymo aspektai ir priemonės analizuojami, vertinami ir taikomi ekspertiniame lygyje. Šios tematikos specifiškumas, globalumas, problematika ir visuomenės informuotumo trūkumas suponuoja darbo problemą - kaip ikimokyklinio ir bendrojo ugdymo programos plėtoja kibernetinio saugumo kultūrą Lietuvoje? Darbo objektas - kibernetinio saugumo kultūros plėtra švietimo srityje. Šio darbo tikslas įvertinti kibernetinio saugumo kultūros plėtrą švietimo srityje: ikimokyklinio ir bendrojo ugdymo programų pagrindu. Nustatyti šie darbo uždaviniai: išanalizuoti kibernetinio saugumo kultūros teorinius aspektus, atlikti kokybinį ekspertų nuomonės tyrimą, kurio pagrindu galima vertinti kibernetinio saugumo kultūros aspektą ikimokyklinio ir bendrojo ugdymo programose ir nustatyti kibernetinio saugumo kultūros plėtojimo kryptis ir išanalizuoti Lietuvos ikimokyklinio ir bendrojo ugdymo programas lyginamuoju pagrindu ir pateikti programų vystymo kryptis kibernetinio saugumo srityje. Taikyti darbo metodai: mokslinės literatūros sisteminimas, dokumentų kokybinio turinio (content) analizė, antrinių statistinių šaltinių analizė ir pusiau struktūruotas interviu.

Tyrimo metu buvo iškeltos dvi hipotezės. Pirmoji: Lietuvos ikimokyklinio ir bendrojo ugdymo programų koncepcija įtakoja saugumo kultūros plėtojimo problematiką švietimo sistemoje. Atlikus kokybinį tyrimą ši hipotezė buvo patvirtinta. Šiuo metu IT bendrojo ugdymo programų turinys neįtraukia įvairiapusiško kibernetinio saugumo traktavimo ir su juo siejamų saugumo elgesio normų. Tačiau pedagogai įtraukia IRT saugumo pagrindus į dėstomas temas savo kompetencijų ribose. Antrojo hipotezė: Lietuvos kibernetinio saugumo teisinė bazė lemia kibernetinio saugumo kultūros plėtojimo problematiką švietimo sistemoje. Ši hipotezė taip pat buvo patvirtinta, Kibernetinio saugumo įstatymas neapibrėžia centralizuoto ir sistemingo informuotumo didinimo švietimo srityje.

Magistro baigiamojo darbo pabaigoje pateikiamos išvados įtraukiančios nustatytą problematiką kibernetinio saugumo kultūros vystymo švietimo srityje bei galimų sprendimų kryptys.

Chochlova L. (2022). *Development of cyber security culture in the field of education: on the basis of pre-school and general education institutions programmes.* Vilnius: Mykolas Romeris University.

SUMMARY

Cybersecurity culture development aspects are analyzed, evaluated, and applied at the expert level. The specificity of this topic, globality, problematics and lack of public awareness presupposes the problem of work – how do preschool and general education programs develop the culture of cybersecurity in Lithuania? The object of the work is the development of cybersecurity culture in the field of education. The following tasks of the work have been identified: to analyze the theoretical aspects of the cybersecurity culture, to conduct a qualitative study of the opinion of experts, on the basis of which it is possible to evaluate the aspect of the culture of cybersecurity in pre-school and general education curricula and to determine the directions of development of the cybersecurity culture, and to analyze Lithuanian pre-school and general education programs on a comparative basis and to present the directions of program development in the field of cybersecurity. Applied working methods: systematization of scientific literature, analysis of the qualitative content of documents, analysis of secondary statistical sources and semi-structured interviews.

Two hypotheses were raised in the study. First: The concept of Lithuanian preschool and general education programs influences the problem of the development of security culture in the education system. A qualitative study confirmed this hypothesis. Currently, the content of IT general education program does not include the diverse treatment of cybersecurity and the norms of security behavior associated with it. However, educators incorporate the basics of ICT security into the topics taught within the limits of their competences. Hypothesis of the second: The legal framework of Lithuania's cybersecurity determines the problem of the development of cybersecurity culture in the education system.

At the end of the Master thesis, conclusions are presented that include the established problems in the field of cybersecurity culture development in the field of education and the directions of possible solutions.