VADOVŲ VEIKLA UŽTIKRINANT KIBERNETINĮ SAUGUMĄ BENDROJO UGDYMO MOKYKOJE

Rasa Skališienė[1], Šarūnė Kazlauskė[2], Ilona Klanienė[3], Kęstutis Mockus[4]

Klaipėdos universitetas (Lietuva), Klaipėdos licėjus (Lietuva)

ANOTACIJA

Straipsnyje analizuojama kibernetinio saugumo svarba mokykloje ir mokyklos vadovo vaidmuo užtikrinant saugią skaitmeninę aplinką. Tyrimas atliktas vykdant pusiau struktūruotą interviu su bendrojo ugdymo mokyklų vadovais. Tyrimo rezultatai atskleidė, kad švietimo įstaigoms vis dažniau kyla kibernetinių grėsmių, tokių kaip apgaulingi elektroniniai laiškai, melagingos nuorodos ar klaidinančios žinutės apie tariamus pavojus, kurios trikdo ugdymo procesą, kelia riziką duomenų saugumui ir kenkia institucijos reputacijai. Atskleista, kad mokyklų vadovų veikla, užtikrinant kibernetinį saugumą, sutelkta ties prevencinių ir intervencinių veiklų organizavimu, bendruomenės telkimu, vidaus tvarkos, reagavimo algoritmų kūrimu bei bendradarbiavimu su institucijomis. Pastebima, kad dažnai vadovams trūksta patirties, jie jaučia psichologinę ir teisinę atsakomybę dėl galimų pasekmių. Išryškėjo skirtingos nuomonės dėl vadovo vaidmens – nuo esminio lyderio iki bendruomeninės atsakomybės dalijimosi modelio, tačiau sutariama, kad efektyvus kibernetinio saugumo užtikrinimas grindžiamas vadovo, kaip švietėjo, grėsmių valdytojo, prevencijos organizatoriaus bei telkėjo, aktyviai įtraukiant visą mokyklos bendruomenę į saugumo kultūros kūrimą.

RAKTAŽODŽIAI: *kibernetinis saugumas, ugdymas, vadovai, mokykla.*

ABSTRACT

The article analyses the importance of cybersecurity in schools and the role of the school principal in ensuring a safe digital environment. The study was conducted using semi-structured interviews with principals of general education schools. The research results revealed that educational institutions are increasingly facing cyberthreats, such as phishing emails, malicious links, or misleading messages about alleged dangers. These threats can disrupt the educational process, pose risks to data security, and damage the institution's reputation. The findings show that school leaders' activities in ensuring cybersecurity focus on organising preventative and interventional measures, mobilising the community, developing internal procedures and response algorithms, and cooperating with institutions. It was observed that principals often lack experience and feel psychological stress and legal responsibility for potential consequences. Different perspectives on the principal's role emerged, from that of a key leader to one in which there is a shared community responsibility model. However, there is agreement that effective cybersecurity assurance is based on the principal acting as an educator, threat manager, prevention organiser and community mobiliser, actively involving the entire school community in building a culture of security.

KEY WORDS: *cybersecurity, education, leadership, school*.

JEL KLASIFIKACIJA: I20

DOI: https://doi.org/10.15181/rfds.v49i2.2819

[1] Rasa Skališienė – Klaipėdos universiteto Socialinių ir humanitarinių mokslų fakulteto Pedagogikos katedros asistentė, socialinių mokslų (edukologijos) daktarė
Moksliniai interesai: socialinė pedagogika, saugumas internete, pažeidžiamas jaunimas
El. paštas: rasa.skalisiene@ku.lt

[2] Šarūnė Kazlauskė – Klaipėdos licėjaus teatro mokytoja, švietimo vadybos magistrė
Moksliniai interesai: kibernetinis saugumas, vadybos procesai, ugdymo įstaigos
El. paštas: sarune.m@klaipedoslicejus.lt

[3] Ilona Klanienė – Klaipėdos universiteto Socialinių ir humanitarinių mokslų fakulteto Pedagogikos katedros profesorė, socialinių mokslų (edukologijos) daktarė
Moksliniai interesai: socialinė pedagogika, savanorystė, diskriminacijos prevencija
El. paštas: ilona.klanienė@ku.lt

[4] Kęstutis Mockus – Klaipėdos universiteto Socialinių ir humanitarinių mokslų fakulteto Pedagogikos katedros lektorius. Šilutės rajono švietimo pagalbos tarnybos direktorius
Moksliniai interesai: edukologijos tyrimų metodologija, mokytojo tyrėjo kompetencija
El. paštas: k.mockus@gmail.com

Įvadas

Šiuolaikinėje visuomenėje dauguma žmogaus veiklų – nuo asmeninės informacijos saugojimo, socialinių ryšių palaikymo iki profesinės veiklos organizavimo – persikėlė į skaitmeninę erdvę. Plačiai prieinamas internetas ne tik sudarė efektyvesnio informacijos valdymo sąlygas, bet ir iš esmės pakeitė požiūrį į saugumą, nusikalstamai veiklai iš fizinės aplinkos iš dalies persikėlus į virtualią erdvę (Grigaitytė, Mackevičiūtė, 2020). Technologinė pažanga lėmė augančią kibernetinių grėsmių riziką, kuri didina tiek pavienių asmenų, tiek valstybinių ir privačių institucijų pažeidžiamumą (LR Krašto apsaugos ministerijos pranešimas, 2023), kadangi vis daugiau jautrios informacijos tampa prieinama nusikaltimus darantiems asmenims, siekiantiems finansinės naudos, duomenų pasisavinimo ar institucijų veiklos destabilizavimo. Saugumo situaciją dar labiau komplikuoja geopolitiniai veiksniai, ypač Rusijos ir Ukrainos karo kontekstas, kuriame kibernetinės atakos tampa svarbia informacinio ir psichologinio poveikio priemone. Tokios atakos pasižymi vis didesniu sudėtingumu, yra orientuotos į socialinę inžineriją bei sisteminio pažeidžiamumo išnaudojimą (Šidlauskas, Ungurytė-Ragauskienė, 2020).

Kibernetinių incidentų aktualumą švietimo sektoriuje iliustruoja 2023 m. spalio mėn. Lietuvoje ir kaimyninėse šalyse išplatinti koordinuoti grasinamieji pranešimai apie tariamai užminuotas ugdymo įstaigas, dėl kurių buvo vykdomos masinės evakuacijos, laikinai stabdomas ugdymo procesas ar pereinama prie nuotolinio mokymo. Tokie veiksmai, kaip pažymima LR Valstybės saugumo departamento ataskaitoje (2023), yra tikslingos atakos, skirtos kelti visuomenėje įtampą, trikdyti institucijų veiklą ir mažinti pasitikėjimą jomis. Didėjant visuomenės priklausomybei nuo skaitmeninių technologijų, nusikalstamos grupės vis aktyviau išnaudoja virtualios erdvės anonimiškumą ir galimybes manipuliuoti informacija (Kuklytė, Ūsas, 2017). Siekiant efektyviai mažinti kibernetinių grėsmių poveikį, kibernetinis saugumas turėtų būti vertinamas kompleksiškai, apimant politikos formavimą, teisinį reguliavimą, saugumo kultūros puoselėjimą, gerosios praktikos taikymą bei švietimą (Giniotienė, 2019), kartu pripažįstant, kad absoliutus saugumas nepasiekiamas. Šiame kontekste ypatingas vaidmuo tenka švietimo sistemai, kuri prisideda prie visuomenės kritinio mąstymo ugdymo, mokinių supažindinimo su kibernetinėmis grėsmėmis ir saugaus elgesio principais (Rahman, Sairi ir kt., 2020). Tai akcentuojama ir Nacionalinėje kibernetinio saugumo strategijoje (2022), kurioje pabrėžiama būtinybė sistemingai ugdyti mokinių kibernetinio saugumo kompetencijas visais ugdymo lygmenimis bei stiprinti pedagogų pasirengimą šioje srityje. Taigi švietimo įstaigoms tenka esminė atsakomybė ne tik ugdyti mokinių gebėjimus atpažinti ir valdyti kibernetines grėsmes, bet ir užtikrinti visos mokyklos bendruomenės saugumą skaitmeninėje aplinkoje.

Mokyklos vadovo vaidmuo užtikrinant kibernetinį saugumą yra esminis, nes jis veikia kaip organizacijos lyderis, kuris formuoja bendruomenės požiūrį į saugumą, inicijuoja prevencines priemones ir koordinuoja tiek techninius, tiek organizacinius sprendimus (Melnikova, 2012; Batuchina, Melnikova, 2023). Vadovo kompetencijos ir strateginiai sprendimai tiesiogiai lemia, kaip efektyviai mokykla gali apsaugoti savo informacines sistemas ir duomenis, sumažinti žmogiškųjų klaidų riziką bei užtikrinti bendruomenės pasitikėjimą skaitmenine aplinka (Šidlauskas, 2024; Richardson, Lemoine, Stephens, Waller, 2020). Atsižvelgiant į tai, kad mokyklos dažnai yra kibernetinių atakų taikiniai dėl jautrių duomenų ir ribotų saugumo išteklių, vadovo vaidmens tyrimas ypač aktualus, jis leidžia įvertinti, kaip lyderystė gali didinti mokyklos atsparumą skaitmeninėms grėsmėms ir plėtoti nuolatinio kibernetinio saugumo kultūrą (AlDaajeha, Saleous, Alrabaeea, Barkaa, Breitinger, 2022).

Tyrimo teorinis pagrindimas remiasi rizikos visuomenės teorija (Beck, 1992), kuri akcentuoja, kad šiuolaikinėje visuomenėje vis didesnę reikšmę įgyja technologinės pažangos nulemtos rizikos, kurių mastas dažnai peržengia lokalų ar nacionalinį lygmenį ir tampa globalus. Ši teorinė perspektyva ypač aktuali analizuojant kibernetinio saugumo problematiką, nes kibernetinės grėsmės pasižymi gebėjimu plisti tarptautiniu mastu, nepaisant geografinių ribų, ir paveikti įvairias institucijas, įskaitant švietimo sektorių. Atsižvelgiant į tai, mokyklos laikytinos ne izoliuotomis sistemomis, o platesnio rizikų tinklo dalimi, kai būtina sistemingai vertinti galimas grėsmes ir jų pasekmes. Be to, teorijoje akcentuojamas technologinių pokyčių nulemtas neapibrėžtumas, kuris apsunkina rizikų prognozavimą ir valdymą, todėl kibernetinio saugumo srityje svarbus

nuolatinis pasirengimas reaguoti į įvairialypes ir kintančias atakų formas. Šiame kontekste išryškėja poreikis švietimo institucijoms kryptingai užtikrinti kibernetinį saugumą, reguliariai atnaujinti saugumo strategijas, ugdymo turinį bei technines priemones, siekiant efektyviai valdyti kylančias grėsmes ir mažinti jų galimą poveikį tiek organizacijos, tiek visos visuomenės lygmeniu.

Mokslinė problema. Vykdant tyrimą siekiama atskleisti vadovų veiklą, siekiant užtikrinti kibernetinį saugumą bendrojo ugdymo mokykloje.

Straipsnio objektas – vadovų veikla, siekiant užtikrinti kibernetinį saugumą bendrojo ugdymo mokykloje.

Straipsnio tikslas – aptarti vadovų veiklą, siekiant užtikrinti kibernetinį saugumą bendrojo ugdymo mokykloje.

Uždaviniai:

1) atskleisti vadovų veiklos, užtikrinant kibernetinį saugumą bendrojo ugdymo mokykloje, teorines prielaidas;
2) išryškinti vadovų patirtis ir veiksmus, siekiant sukurti saugią kibernetinę aplinką mokykloje.

Tyrimo metodai: mokslinės literatūras analizė, pusiau struktūruotas interviu su mokyklų vadovais, duomenys analizuoti taikant turinio (*content*) analizę.

1. Mokyklos vadovų veiklos užtikrinant kibernetinį saugumą mokykloje teorinės prielaidos

Kibernetinis saugumas – šiandien plačiai vartojama sąvoka tiek politikos, tiek visos visuomenės kontekste, tiek komunikuojant saugumą užtikrinančioms institucijoms. Vis dėlto jo samprata gerokai skiriasi ir tai priklauso nuo konteksto bei taikymo srities. Lietuvos Respublikos Kibernetinio saugumo įstatymo redakcijoje (2024) kibernetinis saugumas apibrėžiamas kaip veikla, nukreipta į tinklų ir informacinių sistemų bei kitų susijusių asmenų saugumą nuo bet kokių įvykių, siekiant gaunamų paslaugų prieinamumo, autentiškumo, vientisumo ar konfidencialumo.

Tarptautiniu mastu dažnai naudojamas D. Craigen'o, N. Diakun-Thibault'o, R. Purse (2014, 13) pasiūlytas holistinis, visą sistemą apimantis kibernetinio saugumo apibrėžimas: „Kibernetinis saugumas – tai išteklių, procesų ir organizacinių struktūrų telkimas bei valdymas, siekiant apsaugoti kibernetinę erdvę ir jos pagrindu veikiančias sistemas nuo įvykių, pažeidžiančių teisėtas nuosavybės, prieigos ir naudojimosi teises." Šioje koncepcijoje kibernetinis saugumas skirstomas į informacinį, operacinių technologijų saugumą bei apsaugą nuo puolamųjų atakų, siekiant sumažinti vartotojų pažeidžiamumą ir užtikrinti adekvačią apsaugą (Komaraitė, Vincelovič, 2023).

Kalbant apie kibernetinį saugumą švietimo įstaigose, būtina pabrėžti, kad tai gana nauja sritis, kuri vystėsi kartu su informacinių technologijų integracija į ugdymo procesus. Todėl švietimo kontekste dažniausiai vartojama globali, laipsniškai susiformavusi kibernetinio saugumo samprata: kibernetinis saugumas mokykloje – tai kompleksinių priemonių, kurios turėtų apsaugoti mokyklos informacines sistemas, tinklus ir informaciją nuo neteisėto naudojimo, atskleidimo, pakeitimo ar sunaikinimo, visuma. Tai užtikrina visų skaitmeninių įrankių ir informacijos saugumą bei tinkamą valdomumą (Nassoura, 2022).

Šiuolaikinėje organizacijų veikloje informacinės technologijos tapo esminiu elementu, leidžiančiu sisteminti duomenis, didinti produktyvumą, automatizuoti procesus ir užtikrinti informacijos sklaidą. Nors technologijos suteikia galimybę efektyviau vykdyti veiklą, jos kartu kelia reikšmingus iššūkius saugant organizacijos duomenis, kurių praradimas gali pakenkti visai veiklai (Komaraitė, Vincelovič, 2023).

A. Šidlausko (2024) teigimu, organizacijos dažnai klaidingai mano, kad saugumą gali užtikrinti vien techninės priemonės, tokios kaip antivirusinės programos. Tyrimai atskleidžia, kad didžiausią grėsmę kelia žmogiškosios klaidos: net ir įdiegus pažangias technologijas, jų apsauginis poveikis bus ribotas tinkamai neapmokius darbuotojų jas taikyti. Taigi efektyvi kibernetinio saugumo politika turi apimti ne tik technines

priemones, bet ir darbuotojų mokymus bei organizacinius procesus, kurie užtikrintų asmens duomenų apsaugą pagal Bendrąjį duomenų apsaugos reglamentą (BDAR) (Šidlauskas, 2024).

Mokyklų kontekste kibernetinis saugumas yra ypač svarbus, nes šiose institucijose kaupiami dideli, vertingi ir jautrūs duomenys apie mokinius, jų tėvus bei darbuotojus, įskaitant asmens kodus, gimimo datas, kontaktinę informaciją ir medicininius įrašus (Richardson, Lemoine, Stephens, Waller, 2020; Davis, 2018). Dėl ribotų išteklių ir dažnai nepakankamos specialistų kompetencijos, mokyklos tampa lengvais kibernetinių atakų taikiniais, o nutekinta informacija gali turėti daugialypių pasekmių: ugdymo trikdžiai, konfidencialios informacijos praradimas, reputacijos pažeidimas bei finansiniai nuostoliai (AlDaajeha, Saleous, Alrabaeea, Barkaa, Breitinger, 2022).

Nors kibernetinio saugumo užtikrinimas yra brangus ir reikia nuolat investuoti į technologijas bei žinių atnaujinimą, jis yra būtinas. Lietuvos statistikos departamento (2022) duomenimis, dauguma nedidelių organizacijų, įskaitant mokyklas, saugumo priemones diegia minimaliai, dažniau jas naudoja tik didelės įmonės, turinčios daugiau kaip 250 darbuotojų. Taigi kibernetinio saugumo svarba dažnai suprantama tik patyrus realią ataką.

Bendrojo ugdymo mokyklos yra ypač pažeidžiamos kibernetinių atakų, nes jose kaupiami dideli duomenų masyvai, kuriuose saugoma mokyklos bendruomenės informacija, kartais net dešimtmečius. Toks informacijos ilgalaikiškumas ir jos vertė daro mokyklas patraukliais taikiniais (Torres, Thompson, 2020). Kibernetinio saugumo sistemų diegimas švietimo įstaigose kelia papildomų iššūkių, nes siekiant veiksmingos apsaugos būtinas nuoseklus ir aktyvus bendradarbiavimas su visa mokyklos bendruomene. Saugumo užtikrinimą apsunkina ir mokyklos atvirumas: didelė dalis informacijos apie mokyklos tvarkas, veiklą ar renginius yra viešai prieinama, siekiant skaidrumo ir bendruomenės informuotumo. Be to, mokyklose plačiai naudojamos internetinės priemonės bei skaitmeniniai ištekliai, kurie gali turėti kenkėjiškų programų arba būti nesaugūs.

Švietimo įstaigos vadovas šiuolaikinėje organizacijoje laikomas centrine figūra, nuo kurios lyderystės tiesiogiai priklauso ne tik ugdymo kokybė, bet ir visos bendruomenės saugumas, įskaitant kibernetinę aplinką. Vadovo vaidmuo apima strateginį planavimą, išteklių valdymą ir bendruomenės telkimą siekiant bendrų tikslų (Melnikova, 2012). Lyderystė šiuo atveju reiškiasi gebėjimu organizuoti procesus, motyvuoti darbuotojus, skatinti jų profesinį tobulėjimą ir formuoti bendrą vertybinį pagrindą, orientuotą į nuolatinį mokyklos tobulėjimą (Batuchina, Melnikova, 2023). Vadovas turi būti ne tik autoritetingas, bet ir aktyvus pokyčių iniciatorius, gebantis priimti sprendimus neapibrėžtumo sąlygomis ir telkti bendruomenę veikti koordinuotai (Padgurskytė, 2020). Ši lyderystė tampa ypač reikšminga kibernetinio saugumo kontekste, nes būtent vadovas prisiima atsakomybę už saugios skaitmeninės aplinkos kūrimą ir palaikymą mokykloje.

Kibernetinių grėsmių mastui augant, mokyklos vadovo funkcijos plečiasi – jis tampa ne tik ugdymo proceso organizatoriumi, bet ir kibernetinio saugumo politikos formuotoju bei įgyvendintoju institucijos lygmeniu. Europos Sąjungos (European Union, 2020) rekomendacijos atskleidžia, kad nors dalis kibernetinio saugumo priemonių inicijuojamos nacionaliniu mastu, praktinis jų įgyvendinimas didele dalimi priklauso nuo organizacijos vadovo. Būtent vadovas turi inicijuoti reagavimo į kibernetinius incidentus planų rengimą, užtikrinti bazinių saugumo priemonių diegimą, organizuoti pratybas, didinti bendruomenės informuotumą bei kurti bendradarbiavimo tinklus. Taigi vadovas veikia kaip pagrindinis nacionalinės politikos ir praktinio jos įgyvendinimo mokykloje tarpininkas.

Tarptautinė praktika atskleidžia vadovo atsakomybę šiuo aspektu. Kibernetinio ir infrastruktūros saugumo agentūra (Cybersecurity and Infrastructure Security Agency, 2023) pateikia rekomendacijų būtent švietimo įstaigų vadovams, pabrėžiant jų vaidmenį priimant sprendimus dėl technologinių sprendimų, tokių kaip daugiapakopė autentifikacija, sistemų atnaujinimas ar duomenų atsarginių kopijų valdymas, diegimo. Be to, vadovas yra atsakingas už aiškaus reagavimo plano rengimą ir jo praktinį testavimą, nuoseklų bendruomenės švietimą. Taigi kibernetinio saugumo užtikrinimas mokykloje – ne vien techninis procesas, tai lyderystės klausimas, kurį sprendžiant būtinas strateginis mąstymas ir gebėjimas įtraukti visus bendruomenės narius.

Vadovo veiklą ypač išryškina praktinio veikimo dimensija, kuri siejama su John'o Dewey'aus pragmatizmo teorija. Remiantis šia teorine prieiga, vadovas turi veikti kaip aktyvus praktikas, gebantis mokytis iš patirties ir taikyti žinias realiose situacijose. Taigi mokyklos vadovas turi ne tik suvokti kibernetinio saugumo

principus, bet ir inicijuoti konkrečias priemones, adaptuotas organizacijos poreikiams, bei nuolat reflektuoti jų veiksmingumą. Taip jis tampa nuolatinio organizacinio mokymosi ir saugumo kultūros kūrimo lyderiu.

Mokslinėje literatūroje pabrėžiama, kad būtent vadovas yra atsakingas už rizikų nustatymą ir strateginį jų valdymą. M. Richardson'as, P. Lemoine, W. Stephens'as, R. Waller'is (2020) akcentuoja, kad mokyklos vadovas turi inicijuoti rizikų vertinimą, analizuoti galimus grėsmių scenarijus ir parengti jų padarinių mažinimo veiksmų planus. Vadovo gebėjimas pereiti nuo pasyvios pozicijos („tai mūsų nepalies") prie aktyvaus veikimo („tai gali nutikti mūsų mokykloje") laikomas esminiu kibernetinio saugumo kultūros formavimo veiksniu. Be to, vadovas turi užtikrinti, kad visa bendruomenė aiškiai suprastų savo vaidmenis ir atsakomybę esant kibernetinių incidentų, organizuoti mokymus ir skatinti atvirą komunikaciją šia tema.

Lietuvos kontekste mokyklos vadovo veikla akcentuojama ir strateginiuose dokumentuose. Skaitmeninio švietimo gairės (2023) išryškina vadovo atsakomybę kuriant ir įgyvendinant kibernetinio saugumo politiką mokykloje. Vadovas turi inicijuoti vidaus dokumentų rengimą, nustatyti reagavimo į incidentus tvarką, užtikrinti darbuotojų atitinkamų kompetencijų tobulinimą ir skatinti bendruomenės įsitraukimą. Be to, būtent vadovas priima sprendimus dėl techninių priemonių diegimo: nuo saugios programinės įrangos naudojimo iki prieigos kontrolės ir duomenų apsaugos užtikrinimo. Vis dėlto Nacionalinė kibernetinio saugumo ataskaita (2020) rodo, kad praktikoje vadovų vaidmuo neretai apsiriboja formaliu dokumentų rengimu, o realus jų įgyvendinimas išlieka ribotas, tad kyla poreikis tobulinti vadovų lyderystės kompetencijas šiuo aspektu.

Svarbus vadovo vaidmens aspektas – mokinių ir visos bendruomenės švietimo inicijavimas. Nors tyrimai atskleidžia gana aukštą mokinių skaitmeninio aktyvumo lygį (Europian Commission, 2019; Karosienė, Skerniškytė, 2022), vien technologijų naudojimas neužtikrina gebėjimo saugiai veikti skaitmeninėje erdvėje. Tad būtent mokyklos vadovas turi inicijuoti ankstyvą ir nuoseklų kibernetinio saugumo kompetencijų ugdymą, integruojant šias temas į ugdymo turinį ir skatinant mokytojų rengimą. Tai apima ne tik formalių programų įgyvendinimą (Nacionalinio saugumo ir krašto gynybos bendroji ugdymo programa, 2023), bet ir papildomas iniciatyvas, kurios padėtų mokiniams tapti sąmoningais skaitmeninės visuomenės nariais.

Būtina pastebėti, kad mokyklos vadovas kibernetinio saugumo kontekste veikia kaip strategas, organizatorius, edukatorius ir pokyčių lyderis. Jo vaidmuo apima ne tik formalių reikalavimų įgyvendinimą, bet ir aktyvų saugumo kultūros kūrimą, bendruomenės telkimą bei nuolatinį reagavimą į kintančias grėsmes. Todėl efektyvus kibernetinio saugumo užtikrinimas mokykloje pirmiausia priklauso nuo vadovo lyderystės, gebėjimo veikti kompleksiškai ir inicijuoti tvarius pokyčius organizacijoje.

2. Tyrimo metodologija

Siekiant išsiaiškinti, kaip valdyti kibernetines grėsmes mokykloje, pasirinkta kokybinio tyrimo strategija. Straipsnyje analizuojama dalis duomenų, kurie atskleidžia kibernetinį saugumą bendrojo ugdymo mokykloje užtikrinančią vadovų veiklą. Pasirinkta kokybinio tyrimo strategija labiausiai tinka analizuoti naujus reiškinius, atskleisti asmenų požiūrį į juos, išsiaiškinti ne tik žinių lygį, bet ir analizuoti patirtį, jausmus (Creswell, 2014). Siekiant išsamiai išnagrinėti švietimo įstaigų vadovų darbą didinant kibernetinį saugumą, pasirinktas iš dalies struktūruotas, individualus interviu, kuris apėmė keturias temas: demografinės charakteristikos, kibernetinio saugumo iššūkiai ir svarba, kibernetinio saugumo užtikrinimas mokykloje, vadovo veikla valdant kibernetines grėsmes. Interviu klausimynas sudarytas remiantis analizuota moksline literatūra (Mickevičiūtė, 2020; Richardson ir kt., 2020; Torres, Thompson, 2020; Nassoura, 2022; Šidlauskas, 2024). Tyrimas vykdytas 2024 m. spalio mėn. Interviu vyko tyrimo dalyviams patogioje vietoje, t. y. darbo vietoje arba nuotoliu per Zoom platformą. Interviu trukmė – iki 40 min.

J. Aleknevičienė, A. Pocienė, M. Šupa (2020) rekomenduoja vykdant kokybinius tyrimus, kurie orientuoti į naujos, specifinės problemos analizę, pasirinkti nedideles imtis iki 12-os informantų. I. Gaižauskaitė, N. Valavičienė (2016) pažymi, kad sudarant tyrimo imtį reikia remtis prisotinimo principu, interviu atlikti tol, kol duomenys ima kartotis. Remiantis rekomendacijoms, atrinkti septyni tyrimo dalyviai iš įvairių ugdymo įstaigų, kol buvo pasiektas duomenų prisotinimas. Informantai atrinkti tikslinės kriterinės imties būdu, renkantis informantus taikyti šie kriterijai: aukštasis išsilavinimas; ne mažiau kaip dvejų metų darbo

stažas; mokyklos vadovo arba jo pavaduotojo pareigos. Informantų atsakymai koduoti (I1, I2, I3, I4, I5, I6, I7). Informantų pedagoginio darbo stažas svyruoja nuo 7 iki 34 metų, vadybinio darbo stažas apima nuo 3 metų iki 25 metų. Informantai dirba: vidurinio ugdymo pakopoje (4), pradinio ugdymo (2), pagrindinio (1). Vertinant vadovų kvalifikaciją, 4 turi vyr. mokytojo kvalifikaciją, 2 – mokytojo metodininko ir 1 – mokytojo. Duomenys analizuoti turinio analizės metodu. Turinio analizė padeda atpažinti ir išgryninti giluminius aspektus, kurie slypi už dalyvių išsakytų minčių (Žydžiūnaitė, Sabaliauskas, 2017). Turinio analizė panaudota atliekant pagrindinius žingsnius: dokumentų atranka analizei atlikti, suformuotos pagrindinės kategorijos ir subkategorijos, išskirti skaičiavimo vienetai, atlikta duomenų interpretacija, gilinantis į nustatytų kategorijų tarpusavio sąsajas.

Užtikrinant tyrimo etiką, prieš pradedant tyrimą gauti visų tyrimo dalyvių raštiški sutikimai dalyvauti tyrime ir įrašyti interviu, informacija apie informantus užkoduota. Tyrimo dalyviai supažindinti su tyrimo procedūromis, duomenų rinkimo metodais, priminta jų teisė bet kada pasitraukti iš tyrimo, aptartas anonimiškumo ir konfidencialumo užtikrinimas (Creswell, 2014). Ypač svarbu laikytis sutikimo principo, kuris reiškia, jog tyrimo dalyviai buvo išsamiai supažindinti su tyrimo sąlygomis, paaiškinta, kur ir kaip bus naudojami jų atsakymai, aptartas tyrimo tikslas (Žydžiūnaitė, Sabaliauskas, 2017).

3. Tyrimo rezultatai

Siekiant išanalizuoti vadovo veiklą užtikrinant kibernetinį saugumą, pirmiausia siekta išsiaiškinti, kokias kibernetines grėsmes mokyklos patiria dažniausiai. Remiantis tyrimo duomenų analize, išskirta viena kategorija – mokykloje patiriamos kibernetinės grėsmės, ir keturios subkategorijos: *grasinančių laiškų siuntimas elektoriniu paštu; nuorodų siuntimas, kurias atidarius, kyla rizika nutekinti informaciją; skambučiai, žinutės, kur informuojama apie pavojų mokyklai; kenkėjiškų, virusinių programų siuntimas.*

Iš surinktų duomenų aiškėja, kad mokykloms kyla įvairaus pobūdžio kibernetinių grėsmių. Informantai mini gana dažnai gaunantys bauginančius, grasinančius laiškus elektroniniu paštu, jų turinys dažniausiai susijęs su grasinimu bausme už nusikalstamo pobūdžio veiklas („...administracijos darbuotojai gavome laiškus, kuriuose nurodyta, jog esame įtraukti į baudžiamąją atsakomybę dėl vaikų tvirkinimo...); kituose laiškuose grasinama pakenkti mokyklos bendruomenės nariams: „...kaip ir daugelis Lietuvos mokyklų, 2023–2024 metais susidūrėme su el. laiškų ataka. Laiškuose būdavo grasinimai, perspėjimai dėl įstaigos susprogdinimo“ (I3). Dalis informantų gauna elektroninius laiškus, kuriose bandoma pateikti klaidinančią informaciją: „Tai klaidingi laiškai, kviečiantys kažką paspausti, atidaryti...“ (I2). Kita kibernetinių grėsmių rūšis, su kuria susiduria mokyklų vadovai – informacijos nutekinimas ir įsilaužimai: „...mes suprantame, kokia plona riba tarp kibernetinio saugumo, kur nutekėjo informacija, kad būtent tokiu tikslu buvo siųstas laiškas“ (I1); „...beveik kas mėnesį ateina elektroniniai laiškai direktoriaus vardu buhalteriui, kuriuose prašoma patikslinti lėšų likutį ir tam tikrą sumą pervesti, paspaudžiant nuorodas...“ (I3). Šie pasisakymai atskleidžia, kad didelė rizika mokyklose nutekinti tiek asmeninius, tiek institucijos duomenis. Retesnė informantų patiriama kibernetinės grėsmės forma – skambučiai ar žinučių siuntimas mokykloms: „...gauname įvairius laiškus, žinutes, skambučius...“ (I1); „...man reikia minimalizuoti pavojų, kuris gali būti žinučių pavidalu...“ (I5). Keletas informantų nurodė patiriantys kibernetines grėsmes gaudami kenkėjiškas, virusines programas. Vadovai suvokia būtinybę mokyti bendruomenės narius saugiai naudoti įvairias programas: „...nesisiųsti įvairių programų ir mokytojai negali naudoti asmeninėms reikmėms darbo įrankių...“ (I6). Tyrimo rezultatai atskleidė, kad mokyklos bendruomenės patiria įvairių kibernetinių grėsmių – nuo bauginimų nubausti už menamus nusikaltimus iki asmeninių duomenų nutekinimo, informacijos naikinimo siunčiant kenkėjiškas, virusines programas. Taigi vadovams ypač svarbu užtikrinti įvairių technologijų naudojimo saugumą ir mokyti personalą vykdant kibernetinio saugumo prevenciją. Nacionalinėje kibernetinio saugumo ataskaitoje (2023) teigiama, kad kibernetinės atakos buvo nukreiptos į mokyklų elektroninį TAMO dienyną, tačiau tyrime dalyvavę vadovai su tokio pobūdžio atakomis nesusidūrė. Galbūt dėl to, kad ne visos įstaigos šiuo elektroniniu dienynu naudojasi, be to, pačios mokyklos šio dienyno neadministruoja, todėl informacija apie grėsmes vadovų nepasiekia.

Vadovų teirautasi dėl kibernetinių atakų pasekmių mokykloje. Interviu rezultatai atskleidė, kad kibernetinės atakos sutrikdo tiek mokinių, tiek mokytojų, tiek tėvų darbo ritmą, nes mokykloje sukelia sumaištį. Informantų teigimu, tokios grėsmės išderina visą dienos ritmą, sukelia chaosą ir sumaištį: „...grėsmė išmuša iš rutinos visą veiklą, priverčia imtis veiksmų“ (I3); „...tai yra sąmyšis ir vaikams, ir tėvams...“ (I4); „...sutrikdomas elementarus darbo ritmas, savo energiją turi investuoti į visai kitus dalykus...“ (I5). Tai kelia nepasitenkinimą: „...įvestas nemažas chaosas ir nepasitenkinimas“ (I2). Kita informantų nurodyta pasekmė – baimės, nesaugumo jausmas. Dauguma informantų teigė, kad kaip vadovai jie jaučia kaltę dėl to, kas vyksta („...jautiesi kaltas, kad kažko nepadarei“ (I1)); kitiems kyla nesaugumo jausmas dėl duomenų apsaugos („...atsiranda nesaugumo jausmas, aš jaučiuosi neapsaugotas, mano duomenys neapsaugoti ir jaučiasi pažeidžiamas žmogus“ (I1)); dėl realios grėsmės ne tik mokyklai, bet ir visai bendruomenei („...bendruomenės baimės šalies ir miestelio mastu...“ (I3)); „...sukeliamas nerimas, šurmulys <...>, ar čia tikra grėsmė, ar ne“ (I7)). Vadovai iškėlė ir kitą problemą – tėvų ir vaikų nepasitikėjimas mokykla dėl grėsmės saugumui. Vaikams, tėvams ir mokytojams kibernetinės atakos sukelia stresą: „...išskirčiau psichologines, tai tariamos baimės ir tikros baimės, kurios pas vaikus galėjo atsirasti, ir baimė į mokyklą eiti...“ (I5); „...taip pat iškart iškyla tėvų ir bendruomenės nepasitikėjimas...“ (I7). Su šia grėsme glaudžiai siejai ir kita pasekmė – mokyklos reputacijos sumenkinimas: „...nepasitikėjimas įstaigos gebėjimais susidoroti su susidariusiomis situacijomis“ (I3); „...žinoma reputacinė žala kaip įstaigai“ (I7).

Mokyklos vadovai išsakė apgailestavimą, kad dėl kibernetinių grėsmių trikdomas ugdymo procesas: „Mokyklos lygmeniu sukeliami nepatogumai, stabdomas ugdymo procesas, vėliau reikia vytis pagal programą“ (I4); „...jeigu kibernetinė ataka vyktų <...> per valstybinius brandos egzaminus, tai būtų iššūkiai, kurių maža nepasirodys“ (I5); „Dažniausiai tai būtų mokymo proceso sutrikimai, prasta informacijos sklaida, pavyzdžiui, jeigu MOODLE sugestų, netektume prieigos prie jos...“ (I7). Kita mokyklos darbuotojų patiriama pasekmė – duomenų nutekinimas: „...yra nutekinami duomenys, ir jais pasinaudojama; „...galima turėti bėdų su asmeninių duomenų nutekinimu, jeigu tu pradėsi naudoti asmeninius duomenis, yra ir asmeninių duomenų vagysčių, ir su el. bankininkyste yra vagysčių...“ (I6). Vadovus neramina ir finansinės baudos bei teisinė atsakomybė už kibernetinių grėsmių padarytas žalas: „Manau, kad didžiausios pasekmės, kas galėtų nutikti, tai finansinės išlaidos, įvairiausios baudos, dėl nutekėjusių duomenų, tokie kaip asmens duomenys, banko sąskaitos, kodai ir pan. <...> labai dažnai gali nutikti įvairios teisinės pasekmės, mokykla gali gauti sankcijas, prasidėti tyrimai ir atsakomybės“ (I7). Taigi kibernetinės atakos lemia pasekmes tiek individualiu (kelia nepasitenkinimą dėl įprastos veiklos sutrikdymo, nemalonius jausmus, kaip baimę, sumišimą dėl saugumo), tiek mokyklos (sutrikdomas ugdymo procesas, nutekinami mokyklos duomenys, formuojamas nepasitikėjimas mokykla) lygmeniu. Šias problemas išdėstė U. Beck’as, sukūręs rizikos visuomenės teoriją, kurioje akcentuojama, kad šiuolaikinis pasaulis bendruomenėms kelia grėsmes, tad ypač svarbu mokytis valdyti riziką.

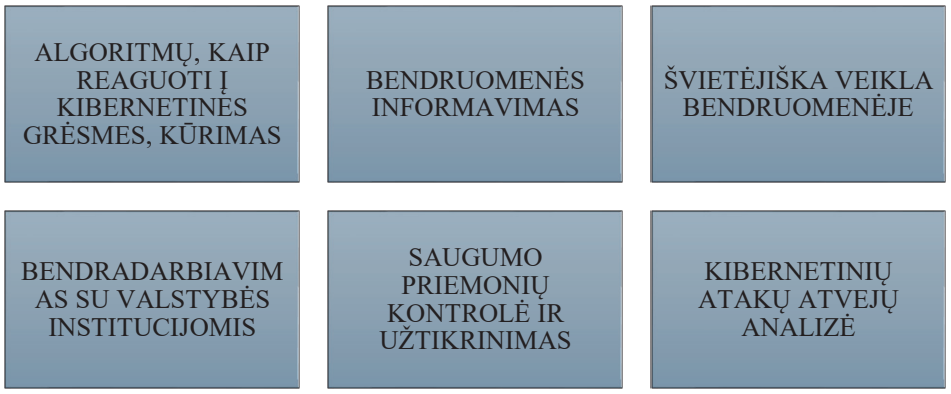
Mokyklos vadovas turi reaguoti į iššūkius mokykloje ir užtikrinti visų bendruomenės narių saugumą, tad buvo svarbu išsiaiškinti, kaip vadovai suvokia savo vaidmenį šioje situacijoje. Tyrimo rezultatai leido išskirti du skirtingus požiūrius į vadovo vaidmenį užtikrinant kibernetinį saugumą: vieni informantai pagrindinį vaidmenį priskiria vadovui („...vadovas turi būti iniciatorius <...> daug kas priklauso nuo vadovo, koks jo požiūris yra“ (I6)), kiti teigia, kad vadovo vaidmuo ne pats svarbiausias („Iniciatoriumi nepavadinčiau, <...> pasakyčiau daugiau statinis, <...> bet tai gali bet kada pasikeisti, reaguojame į pasekmes“ (I5)). Informantai vadovui pirmiausia priskiria žinių apie kibernetinį saugumą teikėjo vaidmenį, jų teigimu, vadovas turėtų: „Šviesti bendruomenę...“ (I2); „...vadovas turi tik supažindinti darbuotojus ir mokinius su galimomis kibernetinio saugumo grėsmėmis...“ (I3). Kitas vaidmuo, kurį išskyrė vadovai, – kibernetinių grėsmių valdytojo ir saugumo užtikrinimo organizatoriaus. Tai iliustruoja šio informanto pasisakymas: „...esu parengęs ir patvirtinęs kibernetinio saugumo procedūras ir tvarkas, paskyręs keletą IT specialistų, kurie yra atsakingi už kibernetinį saugumą, ir įvykus incidentui jo valdymą ir likvidavimą. Visada vertinu rizikas, organizuoju mokyklos IT technologijų auditą, kasmet, tiksliau, kelis kartus per metus organizuoju infrastruktūros auditą, siekiant nustatyti galimas grėsmes...“ (I7). Informantai vadovui priskiria ir vieną iš valdymo funkcijų – kontrolę: „...Kibernetinio saugumo temoje jis tik atlieka kontrolę

prižiūrėdamas, ar teisingai IT specialistas atlieka savo pareigas“ (I1). Visi informantai sutinka, kad vadovas turi atlikti švietėjo, vadybininko, vertintojo vaidmenis, užtikrinant kibernetinį saugumą mokykloje, skiriasi tik to vaidmens stiprumo vertinimas: vieniems atrodo, kad vadovo, kaip lyderio, vaidmuo yra pagrindinis, nes nuo jo inciatyvumo priklauso kibernetinio saugumo kultūra mokykloje, kitų nuomone, vadovo vaidmuo nėra išskirtinis. Europos Sąjungos kibernetinio saugumo agentūros (ENISA) (2020) nurodymu, Sąjungos narės ir jose veikiančios organizacijos, tarp jų ir mokyklos bei jų vadovai, turi imtis iniciatyvos užtikrinant kibernetinį saugumą, tad vadovo vaidmuo šiame kontekste ypač svarbus.

Išsiaiškinus mokyklos vadovui priskiriamus vaidmenis, svarbu buvo išanalizuoti, kokių veiksmų imasi mokyklos vadovai, siekdami užtikrinti kibernetinį saugumą. Remiantis informantų atsakymų analize, išskirtos šešios subkategorijos: *algoritmų, kaip reaguoti į kibernetines grėsmes, kūrimas; bendruomenės informavimas; švietėjiška veikla bendruomenėje; bendradarbiavimas su valstybės institucijomis; saugumo priemonių kontrolė ir užtikrinimas; kibernetinių atakų atvejų analizė.* Duomenų analizės rezultatai pateikti paveiksle.

Penki informantai akcentavo, kad jų esminė veikla – vidaus dokumentų, aprašų ir kt. rengimas, tai leidžia parengti reagavimo į kibernetines grėsmes mokykloje algoritmą: „Kai buvo spalio mėnuo, buvo sudaryta schema ir mes visi žinojome, kaip elgtis tokiu atveju...“ (I1); „Turime žingsnius, kuriais vadovausimės, yra evakuacijos planas“ (I2). Vienas informantas tokių dokumentų rengimą minėjo labiau kaip prievolę atakų atveju: „...tiesiog yra dokumentas, kuris tiesiog yra, nes taip turi būti...“ (I5). Taigi dalis mokyklos vadovų abejoja tokių dokumentų veiksmingumu. Kita veikla, išryškėjusi analizuojant vadovo veiklą, – bendruomenės informavimas. Mokyklos vadovai tiek įvykus incidentui, tiek prevencijos tikslais teikia informaciją mokyklos bendruomenei: „...informuoju kitus, <...> informuoju savo bendruomenę, nuraminu“ (I1). Svarbi ir švietėjiška veikla: „Pagrindinis būdas – švietimas, priminimai, sklaida...“ (I3); „Įtraukiame tėvus šviečiant apie vaikų saugumą, šviečiame apie priemones ir kaip jos gali padėti namuose ugdyti jų vaiką...“ (I7). Keletas informantų išskyrė bendradarbiavimą su valstybės institucijomis, kas privaloma laikantis valstybės nurodymų kibernetinės atakos atveju. Bendradarbiavimas paprastai apsiriboja informacijos perdavimu: „...pirmiausia kreiptis į policiją, <...> perduoti duomenis...“ (I1). Du mokyklos vadovai akcentavo vykdantys kontrolės ir saugumo priemonių užtikrinimo funkciją: „Prižiūrėti darbuotojų, IT specialistų darbą...“ (I1); „Inicijuoju, kad slaptažodžiai būtų patikimi, metų eigoje prižiūriu, kada yra įsigytos tos antivirusinės programos, taip pat lėšas nusimatyti tiems dalykams, taip pat formuojant metų tikslus IT specialistui, kad būtų operacinių sistemų atnaujinimas...“ (I6). Vienas vadovas minėjo, kad jam svarbi įvairių kibernetinio saugumo atvejų analizė: „Pagrindinis būdas <...> atvejų analizės“ (I3). Nors atvejų analizė yra efektyvus kibernetinio saugumo mokykloje užtikrinimo būdas, ši veikla vykdoma rečiausiai. Apibendrinus tyrimo rezultatus paaiškėjo, kad dažniausiai vadovai rengia kibernetinio saugumo užtikrinimo algoritmus, kurdami įvairias tvarkas, tvirtindami vidaus dokumentus.

Kibernetinio saugumo klausimas aktualus visai bendruomenei, todėl vadovas į kibernetinio saugumo kultūros kūrimą mokykloje turi įtraukti visus bendruomenės narius. Vadovams buvo užduotas klausimas, kokią jie vykdo veiklą įtraukdami bendruomenę, kad būtų užtikrintas visų saugumas. Pirma vadovų paminėta veikla – pagalba mokiniams, integruojant kibernetinio saugumo temas į ugdymo programas: „...vaikai mokomi, kaip prisijungti, kokie slaptažodžiai turi būti naudojami, koks yra saugus slaptažodis, kokiais duomenimis galime ar negalime dalintis viešoje erdvėje. Ir klasių vadovai, ir IT mokytojai, ir gyvenimo įgūdžių programoje mes esame įsitraukę šias temas apie kibernetinį saugumą“ (I4). Kita veikla nukreipta į mokytojų švietimą. Vadovai organizuoja mokymus mokytojams, tačiau visi akcentavo praktinių kokybiškų mokymų trūkumą: „Vis tiek tai turėtų būti mokymai, bet ne bet kokie, <...> mums visiems reikia praktikos“ (I5). Kita veikla – aktyvi komunikacija su tėvais vykdant prevencinę veiklą: „... informuojami tėvai, yra prevencinės reklamos, programos, plakatai...“ (I1); „Pagrindinė priemonė – komunikacija, tėvams teikiama informacija elektroninio dienyno pagalba, kalbama susirinkimų metu apie višingą, fišingą, smišingą ir kitas situacijas, tėvų prašome stebėti vaikus, kokiais portalais jie naudojasi, su kuo bendrauja“ (I4). Dauguma informantų mano, kad vienas iš bendruomenės įtraukimo būdų yra supažindinimas su parengtais dokumentais ir vidinėmis tvarkomis: „...Mokyklos bendruomenė yra supažindinta



1 pav. Mokyklos vadovo veiklos kryptys, siekiant užtikrinti kibernetinį saugumą

su mūsų parengtomis tvarkomis...“ (I2); „...mes turime kompiuterių naudojimo tvarką savo įstaigoje...“ (I6). Keletas informantų pažymėjo, kad labiausiai įsitraukia darbuotojai, kurie yra darbo grupės nariai, todėl vadovai dažnai sudaro komandas, kurioms deleguoja atsakomybę už kibernetinį saugumą. Tai padeda vadovui užtikrinti saugumą: „Organizuoju reguliarius susitikimus su IT specialistais, mokytojais ir administracija, kad aptartume IT saugumo būklę mūsų mokykloje, ir esame parengę krizių valdymo komandą, atsakingą už kibernetinį saugumą mokykloje“ (I7). Vienam informantui atrodo ypač svarbus asmeninis vadovo pavyzdys, įtraukiant bendruomenę į kibernetinio saugumo kultūros kūrimą: „Aš, kaip vadovas, visada asmeniškai parodau pavyzdį, kaip reikia laikytis kibernetinio saugumo taisyklių, visą laiką stengiuosi jomis vadovautis“ (I7). Taigi mokyklos vadovai kibernetinio saugumo kultūrą puoselėja kibernetinio saugumo klausimus integruodami į bendrųjų ugdymo programų turinį, mokymų pedagogams organizavimą, prevencinę veiklą su tėvais, darbo grupių kūrimą, kontrolę ir kt. Vadovų minėti bendruomenės įtraukimo būdai atliepia Skaitmeninio švietimo gairių (2023) rekomendacijas, kuriose akcentuojama, kad visa bendruomenė turi atsakingai dalyvauti kurdama kibernetinio saugumo kultūrą.

Apibendrinant tyrimų duomenis galima teigti, kad mokyklų vadovams nuolat kyla kibernetinio saugumo užtikrinimo problema. Esminės mokyklai kylančios grėsmės dėl kibernetinių atakų susijusios su grasinančių elektroninių laiškų siuntimu, įsilaužimu į mokyklos ir darbuotojų paskyras, kenkėjiškų programų siuntimu ir kt. Vadovų teigimu, tokio pobūdžio atakos trikdo mokymosi procesą, o tai paveikia visų bendruomenės narių jauseną, kyla baimės, lemiančios nepasitenkinimą mokyklą, nepasitikėjimo aplinka jausmas, dėl ko prastėja mokyklos reputacija. Mokyklos vadovai, reaguodami į šias problemas, vykdo įvairią saugumą užtikrinančią veiklą. Pagrindinė veikla yra algoritmo rengimas sprendžiant kibernetinio saugumo klausimus, be to, švietėjiška veikla, siekiant išvengti grėsmių, bendradarbiavimas su mokyklos bendruomenės nariais ir kitomis institucijomis. Vadovai šia atsakomybe dalijasi su bendruomene, aktyviai įtraukdami visus bendruomenės narius (mokinius, mokytojus, tėvus ir kt.) į kibernetinio saugumo atmosferos mokykloje kūrimą.

Diskusija ir išvados

Šiandienė visuomenė, remiantis U. Beck’o (1992) rizikos visuomenės teorija, susiduria su įvairiomis rizikomis, tarp kurių yra ir kibernetinės atakos, tad ypač svarbu įvairiais lygmenimis – tarptautiniu, nacionaliniu, instituciniu – kurti saugumo kultūrą. Kibernetinis saugumas užtikrinamas įvairiomis priemonėmis, siekiant užkirsti kelią neteisėtiems veiksmams skaitmeninėje erdvėje ir iš to kylančioms grėsmėms. Kibernetinio saugumo klausimas ypač aktualus mokyklai, kuri pastaruoju metu vis dažniau patiria kibernetinių atakų, kurių pasekmės yra sutrikdytas ugdymo procesas, asmeninių ir institucinių duomenų praradimas, žala mokyklos reputacijai ir kt. (Torres, Thompson, 2020; AlDaajeha, Saleous, Alrabaeea, Barkaa, Breitinger, 2022). Todėl

mokyklų vadovams tenka papildoma funkcija – prisiimti atsakomybę už mokyklos kibernetinį saugumą. Vadovo veikla nukreipta į bendruomenės narių telkimą, mokymų, kaip elgtis kilus kibernetinių grėsmių, organizavimą, tvarkos aprašų, kaip reaguoti ir veikti tokiais atvejais, rengimą, saugumo patikrų organizavimą, vaikų ir tėvų supažindinimą su mokyklos kibernetinio saugumo politika (Batuchina, Melnikova, 2023).

Kokybinio tyrimo rezultatai atskleidė, kad dažniausiai mokykla susiduria su tokiomis kibernetinėmis grėsmėmis, kaip nesaugūs elektroniniai laiškai darbuotojams, grasinant baudžiamąja atsakomybe, be to, siunčiamos melagingos nuorodos, kurias atidarius kyla rizika nutekinti tiek asmeninę, tiek institucijos informaciją, mokyklos atstovai gauna žinutes, kurios praneša apie melagingą pavojų mokyklai ir kt. A. Šidlauskas, S. Ungurytė-Ragauskienė (2020) išskiria panašias formas, kaip grasinantys laiškai, nepageidaujamų reklamų rodymas, kenkėjiškų programų su virusais siuntimas, informacijos vagystės ir kt. Tokio pobūdžio nusikalstama veikla veikia tiek mokyklos personalą, tiek mokinius ir jų tėvus, todėl vadovai privalo operatyviai reaguoti, nes sutrikdoma kasdienė veikla, nukenčia ugdymo procesas, jaučiamas nepasitenkinimas iš visų bendruomenės narių, o tai paveikia mokyklos reputaciją. Dauguma vadovų, neturinčių tokio pobūdžio problemų sprendimo patirties, išgyvena stiprų kaltės jausmą, nepavykus mokykloje užtikrinti kibernetinio saugumo. Vadovams ypač aktualu, kad už kibernetinių grėsmių pasekmes gali būti nubausti finansiškai, jiems gresia teisinė atsakomybė. Kibernetinių atakų sukeltų pasekmių žala yra ženkli visiems mokyklos bendruomenės nariams, tad investicijos turėtų būti nukreiptos į prevencijos priemonių kūrimą (Richardson ir kt., 2020).

Tyrimas išryškino dvi pozicijas dėl vadovo vaidmens: vieni vadovai teigė, kad jų veikla yra esminė užtikrinant kibernetinį saugumą, kiti pasisakė už pasyvesnį vaidmenį, nes, jų nuomone, už tai atsakomybę turėtų prisiimti visa bendruomenė. Dauguma informantų pasisakė už aktyvų vadovo vaidmenį reaguojant į realias kibernetinio saugumo užtikrinimo problemas, tuo tarpu kiti teigė, kad jų vaidmuo šioje situacijoje yra statinis, t. y. vadovo veikla teisiškai reglamentuota. Taigi galima daryti prielaidą, kad Lietuvoje dėmesio šiai temai nedaug teskiriama, vadovai individualiai sprendžia šią problemą, tuo tarpu užsienio valstybėse atliekami įvairūs tyrimai, kaip mokyklos pasirengusios reaguoti į kibernetines atakas, diskutuojama, kas ir per kiek laiko turi išsiaiškinti kibernetinius incidentus, analizuojami jų pavyzdžiai (Torres, Thompson, 2020).

Vadovų interviu duomenų analizė atskleidė tokius vadovo vaidmenis užtikrinant kibernetinį saugumą mokykloje: švietėjo, grėsmių valdytojo, prevencinės veiklos organizatoriaus ir kontrolieriaus. Šie vaidmenys siejasi su vadovų intervencine ir prevencine veikla, kurią jie organizuoja spręsdami kibernetinio saugumo klausimus. Vadovų teigimu, jie dažniausiai informuoja mokyklos bendruomenę apie grėsmes, kuria algoritmus, kaip į tai reaguoti, organizuoja mokymus bendruomenei, teikia informaciją, bendradarbiauja su valstybės institucijomis, rečiau vykdo kibernetinių grėsmių atvejų analizę. M. Richardson'as, P. Lemoine, W. Stephens'as, R. Waller'is (2020), remdamiesi mokslinių tyrimų rezultatais, rekomenduoja šias veiklas užtikrinant kibernetinį saugumą: pirmiausia vadovas turi įsivertinti rizikas, tada – turimas priemones ir kibernetinių grėsmių prevencijos būdus, vykdyti stebėseną ir svarbiausia – analizuoti kibernetines grėsmes modeliuodamas blogiausių atvejų scenarijus.

Kaip minėta, vadovai daugiausia susitelkia ties vidaus dokumentų, tvarkos aprašų rengimu, tačiau interviu atkleidė, kad jie patys abejoja šios veiklos efektyvumu. Tai siejasi su U. Grigaitytės, M. Mackevičiūtės (2020) mokslinėmis įžvalgomis, kurios teigia, kad mokyklos turi pasirengusios esmines kibernetinio saugumo užtikrinimo taisykles, tačiau jos taikomas nenuosekliai. Ta pati problema keliama ir Nacionalinėje kibernetinio saugumo ataskaitoje (2020), kur pažymima, kad mokyklos turi pasirengusios formalius dokumentus, algoritmus, tačiau jie neatitinka šiuolaikinių bendruomenės lūkesčių ir poreikių, nes realioje praktikoje sunkiai pritaikomi. Interviu rezultatai atskleidė, kad vadovai aktyviai įtraukia mokyklos bendruomenę į saugumo užtikrinimą mokykloje teikdami pagalbą mokiniams, mokytojams ir tėvams, informuodami juos apie algoritmus, integruodami saugumo temas į ugdymo turinį, vykdydami švietėjišką veiklą su tėvais, tobulindami mokytojų kompetencijas. Informantai atsakomybe už mokyklos saugumą dalijasi su bendruomene, organizuodami darbo grupes, kurios turėtų rūpintis kibernetinio saugumo kultūra mokykloje. Šių veiklų svarbą patvirtina A. Šidlausko (2024) tyrimo rezultatai, atskleidžiantys, kad organizacijų vadovai dažnai klysta manydami, jog nuo kibernetinių atakų gali apsaugoti tik programinė įranga. Pažymėtinas darbas su

visa mokyklos bendruomene, vykdant kibernetinio saugumo mokymus, nes moksliniai tyrimai atskleidė, kad didžiausią grėsmę kelia žmogiškosios klaidos. Taigi, jei personalas nebus apmokytas naudotis įvairiomis saugumo programomis, apsauginio poveikio jos neturės. T. Malhotra, M. Malhotra (2017) tyrimo rezultatai rodo, kad tik 10 proc. mokytojų turi pakankamai žinių apie kibernetinį saugumą.

Tyrimo ribotumai. Tyrimas atliktas tik su viena informantų grupe – mokyklų vadovais, todėl vadovo veiklos vertinimas analizuojamas tik jų pačių požiūriu, neatskleista kitų bendruomenės narių patirtis, ypač mokytojų, kurių atsakymų analizė leistų įvertinti, ar vadovo veikla atitinka jų lūkesčius. Tyrime dalyvavo 7 informantai, taigi nėra galimybių apibendrinti tyrimo duomenis visai populiacijai, nes interviu duomenys atskleidžia asmenines vadovų patirtis.

Rekomendacijos tolesniems tyrimams. Siekiant suvokti kibernetinio saugumo klausimus mokykloje, būtų pravartu į tyrimą įtraukti įvairesnes bendruomenės grupes (mokinius, mokytojus, tėvus), tai įgalintų plačiau įvertinti kylančias kibernetines grėsmes ir realiai taikomus prevencijos būdus. Be to, būtų naudinga atlikti kiekybinį tyrimą įtraukiant visos Lietuvos mokyklas, kad galima būtų vertinti kibernetinių atakų mastą, grėsmes, pasekmes, taikomas prevencijos ir intervencijos priemones. Siekiant gilesnių įžvalgų, būtų naudinga atlikti kokybinį tyrimą (grupinį interviu), kuriame galėtų dalyvauti įvairios grupės ir būtų galima įvertinti vadovo vaidmenį bei bendruomenės indėlį sprendžiant su kibernetiniu saugumu susijusius iššūkius.

Literatūra

AlDaajeha, S., Saleous, H., Alrabaeea, S., Barkaa, E., Breitinger, F. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers and Security*, *119*, 102754. DOI: https://doi.org/10.1016/j.cose.2022.102754

Aleknevičienė, J., Pocienė, A., Šupa, M. (2020). *Kaip parašyti mokslinį darbą?* Vilnius: Vilniaus universiteto leidykla.

Batuchina, A., Melnikova, J. (2023). Skaitmeninių technologijų integravimas į mokyklos, kaip organizacijos, procesus ir praktikas: teorinis modelis. *Regional Formation and Development Studies*, *1* (39), 5–15. DOI: https://doi.org/10.15181/rfds.v36i1.2506

Beck, U. (1992). *Risk Society: Towards a New Modernity.* SAGE Publications.

Cybersecurity and Infrastructure Security Agency. (2023). *K12 school cybersecurity recommendations*. https://www.cisa.gov/K12Cybersecurity?utm_source=chatgpt.com

Craigen, D., Diakun-Thibault, N., Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4* (10), 13–21. DOI: https://doi.org/10.22215/timreview/835

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches.* 4th ed. SAGE Publications.

European Union. (2020). *Cybersecurity guidelines for schools: Recommendations for safe and resilient digital education*. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=57894

European Commission. (2019). *2nd Survey of Schools: ICT in Education: Objective 1 – Benchmark progress in ICT in schools*. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=57894

Gaižauskaitė, I., Valavičienė, N. (2016). *Socialinių tyrimų metodai: kokybinis interviu*. Vilnius: MRU. https://cris.mruni.eu/server/api/core/bitstreams/6bc9b0c7-425b-4420-a2cd-e6ec2d12736a/content

Giniotienė, A. (2019). *NRD Cyber Security.* https://www.vz.lt/verslovaldymas/2019/11/15/kibernetinis-saugumas-prasideda-nuo-suvokimo

Grigaitytė, U., Mackevičiūtė, M. (2020). *Nusikaltimai virtualioje erdvėje – šiuolaikiniai iššūkiai ir prevencijos galimybės. Teisės mokslo pavasaris 2020,* 274–294. Vilniaus universiteto leidykla. DOI: https://doi.org/10.15388/OS.TMP.2020.13

Komaraitė, K., Vincelovič, A. (2023). *Kibernetinio saugumo teisinis reguliavimas: Teoriniai ir praktiniai aspektai*. *Verslo ir teisės aktualijos = Current Issues of Business and Law*, *1* (4), 53–61. https://talpykla.elaba.lt/elaba-fedora/objects/elaba%3A177709333/datastreams/MAIN/content

Karosienė, E., Skerniškytė, J. (2022). *Švietimo skaitmenizavimas. Esamos situacijos Lietuvoje analizė.* Kurk Lietuvai. https://data.kurklt.lt/wp-content/uploads/2023/04/Skaitmeninio-svietimo-gaires-_-esamos-situacijos-analize.pdf

Kuklytė, J., Ūsas, A. (2017). Informacinės visuomenės iššūkiai: kokios yra kibernetinių nusikaltimų formos? *Visuomenės saugumas ir viešoji tvarka*, *18*, 184–194. https://cris.mruni.eu/cris/entities/publication/03645e69-1bf6-4c9f-8dcf-d0a237aa4b96/details

LR Krašto apsaugos ministerija. (2022). *Nacionalinė kibernetinio saugumo strategija.* https://kam.lt/wp-content/up-

loads/2022/03/nacionaline-kibernetinio-saugumo-strategija.pdf

LR Krašto apsaugos ministerijos pranešimas. (2023). *Kibernetinis saugumas.* https://kam.lt/kibernetinis-saugumas/

LR Seimas. (2024). *Kibernetinio saugumo įstatymo Nr. XII1428 pakeitimo įstatymas*. https://eseimas.lrs.lt/portal/legalAct/lt/TAP/236f0e00fd6c11ee8e4be9fad87afa59?positionInSearchResults=0&searchModelUUID=65114f2d6e894a1f99c08d3868a4a704

Lietuvos statistikos departamentas. (2022). *Kibernetinės atakos – rizika ne tik reputacijai*. https://osp.stat.gov.lt/straipsniskibernetinesatakos

LR Švietimo, mokslo ir sporto ministerija. (2023). *Skaitmeninio švietimo gairės*. https://www.emokykla.lt/upload/media/public/Kita-aktuali-medziaga/Skaitmeninio%20%C5%A1vietimo%20gair%C4%97s%20_%20galutinis%20(2).pdf

LR Valstybės apsaugos departamento pranešimas visuomenei. (2023). *VSD vertinimu, grasinantys pranešimai ugdymo įstaigoms, tikėtina, yra tikslinga ir koordinuota ataka*. https://www.vsd.lt/2023/10/13/vsd-vertinimu-grasinantys-pranesimai-ugdymo-istaigoms-tiketina-yra-tikslinga-ir-koordinuota-ataka/

Malhotra, T., Malhotra, M. (2017). *Cyber Crime Awareness among Teacher Trainees. Scholarly Research Journal for Interdisciplinary Studies, 4* (31), 5249–5259. https://www.academia.edu/75369616/Cyber_Crime_Awareness_Among_Teacher_Trainees

Torres, M., Thompson, N. (2020). Toward a cyber security adoption framework for primary and secondary education providers. In *Proceedings of the 31st Australasian Conference on Information Systems* (Paper 93). Australasian Conference on Information Systems. https://aisel.aisnet.org/acis2020/93

Melnikova, J. (2012). Kokybiško mokyklų vadovų kompetencijų ugdymo komponentų projektavimas suaugusiųjų švietimo paslaugų optimizavimo kontekste. *Andragogika, 1* (3), 82–104. http://www.ku.lt/tsi/files/2012/10/Andragogika_2012_13_siuntimui.pdf

Nacionalinis kibernetinio saugumo centras. (2022). *Nacionalinė kibernetinio saugumo metinė ataskaita 2022*. https://kam.lt/wp-content/uploads/2023/05/Nacionalinekibernetiniosaugumobuklesataskaita2022.pdf

Nassoura, A. B. (2022). *Cybersecurity technologies and practices in higher education institutions: A systematic review. Webology, 19* (1), 1152–1167. https://www.researchgate.net/profile/Ayman-Nassuora-2/publication/360835004_Cybersecurity_Technologies_And_Practices_In_Higher_Education_Institutions_A_Systematic_Review/links/628dcf816773462154d7116e/Cybersecurity-Technologies-And-Practices-In-Higher-Education-Institutions-A-Systematic-Review.pdf

Padgurskytė, V. (2020). *Švietimo įstaigų vadovų kasmetinės veiklos vertinimo situacija. Jaunųjų mokslininkų darbai*, *50* (1), 38–45. DOI: https://doi.org/10.21277/jmd.v50i1.291

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., Khalid, F. (2020). *The importance of cybersecurity education in school. International Journal of Information and Education Technology, 10* (5), 378–382. DOI: https://doi.org/10.18178/ijiet.2020.10.5.1393

Richardson, M. D., Lemoine, P. A., Stephens, W. E., Waller, R. E. (2020). Planning for cyber security in schools: The human factor. *Educational Planning*, *27* (2), 23–39. https://eric.ed.gov/?id=EJ1252710

Šidlauskas, A. (2024). *Asmens duomenų saugaus valdymo elektroninėje erdvėje sistemos modelis.* Daktaro disertacija. Mykolo Romerio universitetas. https://cris.mruni.eu/cris/handle/007/47885

Šidlauskas, A., Ungurytė-Ragauskienė, S. (2020). *Iššūkiai kibernetiniam saugumui: socialinė inžinerija institucinio izomorfizmo kontekste. Visuomenės saugumas ir viešoji tvarka = Public Security and Public Order, 25*, 389–405. https://ojs.mruni.eu/ojs/index.php/vsvt/article/view/6286

Žydžiūnaitė V., Sabaliauskas S. (2017). *Kokybiniai tyrimai: principai ir metodai*. Vilnius: Vaga.

LEADERSHIP ACTIVITIES AIMED AT ENSURING CYBERSECURITY IN A GENERAL EDUCATION SCHOOL

Rasa Skališienė, Šarūnė Kazlauskė, Ilona Klanienė, Kęstutis Mockus
Klaipėda University (Lithuania), Klaipėda Lyceum (Lithuania)

Summary

Cybersecurity is becoming increasingly relevant in the contemporary educational environment, as general education schools store large amounts of data containing sensitive information about students, teachers and administrative staff. The development of technology and the integration of digital tools into the teaching process provide opportunities to enhance educational efficiency, but at the same time require measures to secure information. This situation highlights the need not only for security measures within the technology, but also for a comprehensive approach in which the school principal plays a crucial role in safeguarding the information of the entire institution.

Qualitative research findings indicate that schools face most frequently the following cybersecurity threats: threatening emails, phishing links that can compromise personal or institutional information, and messages reporting false incidents. These threats affect not only staff, but also students and their families, disrupting daily operations, the educational process, and the school's reputation. Many school leaders lack sufficient experience in managing such situations, which creates a significant sense of responsibility and psychological stress. Additionally, leaders may face financial or legal liability for the consequences of cyberthreats. Therefore, it is crucial for school administrators to invest in preventative measures, and strengthen cybersecurity across their entire educational community.

The study revealed that the principal's role in ensuring cybersecurity in schools can be ambiguous. Some principals adopt an active approach, by organising preventative activities, informing the community about threats, conducting training, and collaborating with external institutions. Other principals take a more passive, regulatory approach, in which their actions do not go beyond formal procedures, and responsibility is shared with the entire school community. Formal documentation and algorithms often do not correspond to real-world practice, thereby limiting their effectiveness.

Effective cybersecurity in schools importantly depends on community engagement and competence. Principals often initiate training for teachers, students and parents: providing information about risks, integrating security topics into the curriculum, and organising preventative and monitoring activities. Even with technical measures in place, human error poses the greatest threat; therefore, continuous community education and preparedness to respond to threats are essential aspects of school cybersecurity.

KEY WORDS: *cybersecurity, education, leadership, school*.

JEL CODE: 120.

Gauta: 2026.02.15

Priimta: 2026.03.25

Pasirašyta spaudai: 2026.04.20