



Kauno technologijos universitetas

Informatikos fakultetas

Nuotolinis krašto apsaugos sistemos personalo kibernetinio saugumo įgūdžių ugdymas

Baigiamasis magistro projektas

Vytautas Krivelis

Projekto autorius

Doc. prakt. dr. Vytenis Punys

Vadovas

Kaunas, 2026



Kauno technologijos universitetas

Informatikos fakultetas

Nuotolinis krašto apsaugos sistemos personalo kibernetinio saugumo įgūdžių ugdymas

Baigiamasis magistro projektas

Nuotolinio mokymosi informacinės technologijos (6211BX010)

Vytautas Krivelis

Projekto autorius

Doc. prakt. dr. Vytenis Punys

Vadovas

Asist. dr. Ramūnas Kubiliūnas

Recenzentas

Kaunas, 2026



Kauno technologijos universitetas

Informatikos fakultetas

Vytautas Krivelis

Nuotolinis krašto apsaugos sistemos personalo kibernetinio saugumo įgūdžių ugdymas

Akademinio sąžiningumo deklaracija

Patvirtinu, kad:

1. baigiamąjį projektą parengiau savarankiškai ir sąžiningai, nepažeisdamas (-a) kitų asmenų autoriaus ar kitų teisių, laikydamasis (-i) Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo, Kauno technologijos universiteto (toliau – Universitetas) intelektinės nuosavybės valdymo ir perdavimo nuostatų bei Universiteto akademinės etikos kodekse nustatytų etikos reikalavimų;
2. visi baigiamajame projekte pateikti duomenys ir tyrimų rezultatai yra teisingi ir gauti teisėtai, nei viena projekto dalis nėra plagijuota nuo spausdintinių ar elektroninių šaltinių, o visos baigiamojo projekto tekste pateiktos citatos ir nuorodos yra nurodytos literatūros sąrašė;
3. baigiamajame projekte tinkamai laikiausi asmens duomenų apsaugos reikalavimų, nenaudojau neskelbtinų ar konfidencialių duomenų be teisėto pagrindo, o jei juos naudoju, jie yra tinkamai nuasmeninti;
4. jei rengiant baigiamąjį projektą naudojausi dirbtinio intelekto (toliau – DI) ar kitais automatizuotais įrankiais, juos taikiau pagal Universitete nustatytą tvarką, nepažeisdamas (-a) akademinio sąžiningumo principų;
5. nesumokėjau ir nesu įsipareigojęs (-usi) mokėti jokių įstatymų nenumatytų piniginių sumų už baigiamąjį projektą ar jo dalis jokiame fiziniame ar juridiniame asmeniui;
6. suprantu, kad išaiškėjus akademinio nesąžiningumo ar kitų asmenų teisių pažeidimo faktui, man bus taikoma atsakomybė pagal Universitete nustatytą tvarką ir galiu būti pašalintas (-a) iš Universiteto; akademinio nesąžiningumo atvejis gali būti nagrinėjamas ir po studijų baigimo, inicijuojant kvalifikacinio laipsnio atšaukimo procedūrą.

Krivelis, Vytautas. Nuotolinis krašto apsaugos sistemos personalo kibernetinio saugumo įgūdžių ugdymas. Baigiamasis magistro projektas / vadovas doc. prakt. dr. Vytenis Punys; Kauno technologijos universitetas, Informatikos fakultetas.

Studijų kryptis ir sritis: Programų sistemos (B03), Informatikos mokslai.

Reikšminiai žodžiai: Kibernetinis saugumas, kibernetinio saugumo įgūdžiai, virtualioji mokymosi aplinka, nuotolinis mokymas.

Kaunas, 2026. 57 p.

Santrauka

Kibernetinis saugumas valstybės ir Krašto apsaugos sistemoje tampa vis svarbesnis, nes darbas neįsivaizduojamas be informacinių technologijų. Tačiau atlikus tyrimą paaiškėjo, kad silpniausia saugumo grandimi išlieka žmogus, o didžioji dalis kibernetinių incidentų įvyksta dėl žmogiškųjų klaidų ir socialinės inžinerijos atakų. Šiandieninės esamos mokymosi priemonės dažniausiai orientuotos tik į teorinių žinių perteikimą, todėl sunkiai užtikrina tinkamą praktinių įgūdžių ugdymą bei besimokančiųjų motyvaciją.

Kibernetinio saugumo mokymosi aplinkos, pritaikytos organizacijos poreikiams, kūrimas yra kompleksinis procesas. Nors universalios platformos, tokios kaip „Moodle“ ar „Open eClass“, yra plačiai naudojamos ir funkcionalios, analizė parodė, kad jos ne visuomet leidžia pilnai realizuoti specifinius ar individualizuotus naudotojų elgsenos mokymo sprendimus.

Tiriamajame projekte buvo suprojektuota ir sukurta minimaliai veikiantis produktas bandomojo virtualioji mokymosi aplinka, skirta personalo kibernetinio saugumo įgūdžių ugdymui. Besimokančiųjų įgūdžiams lavinti sistemoje buvo integruoti struktūruoti kursai apie slaptažodžių saugumą, duomenų apsaugą ir socialinę inžineriją, taip pat testavimo posistemė su automatinio vertinimu, mokymosi progreso stebėjimo funkcijos, forumai bei automatinis sertifikatų išdavimas.

Sukurta bandomoji virtualioji mokymosi aplinka leidžia užtikrinti efektyvų, lankstų ir į praktiką orientuotą žinių įsisavinimą bei patikrinimą. Sistema pasižymi aukštu lankstumu ir lengvomis tobulinimo bei plėtojimo galimybėmis, nes buvo sukurta naudojant modernias internetinių aplikacijų kūrimo technologijas. Jos efektyvumą patvirtino ir vartotojų tyrimas – net 80,8 % respondentų nurodė, kad ši platforma padėjo pagerinti jų kibernetinio saugumo žinias.

Be to, sukurta sistema gali būti pritaikoma ir kitoms organizacijoms ar institucijoms, siekiančioms stiprinti darbuotojų kibernetinio saugumo kompetencijas. Ateityje numatoma plėsti platformos funkcionalumą, integruojant papildomas interaktyvias mokymosi priemones, tokias kaip simuliacijos ar praktinės užduotys, kurios dar labiau didintų mokymosi efektyvumą.

Krivelis, Vytautas. Remote Training in Cybersecurity Skills for National Defence System Personnel. Master's Final Degree Project / supervisor assoc. prof. pract. dr. Vytenis Punys; The Faculty of Informatics, Kaunas University of Technology.

Field of study: Software Engineering (B03), Computing.

Keywords: Cybersecurity, cybersecurity skills, virtual learning environment, distance learning.

Kaunas, 2026. 57 p.

Summary

Cybersecurity in the state and the National Defence System is becoming increasingly important, as work is inconceivable without information technologies. However, the conducted research revealed that the human factor remains the weakest link in security, and the majority of cybersecurity incidents occur due to human errors and social engineering attacks. Existing learning tools today are mostly focused on the delivery of theoretical knowledge, and therefore fail to adequately ensure the development of practical skills as well as learners' motivation.

The development of a cybersecurity learning environment tailored to the needs of an organization is a complex process. Although universal platforms such as "Moodle" or "Open eClass" are widely used and functional, the analysis showed that they do not always allow the full implementation of specific or individualized user behavior training solutions.

In this research project, a minimally viable product of a pilot virtual learning environment was designed and developed for the improvement of personnel cybersecurity skills. To enhance learners' competencies, the system integrates structured courses on password security, data protection, and social engineering, as well as a testing subsystem with automatic assessment, learning progress tracking features, forums, and automated certificate issuance.

The developed pilot virtual learning environment ensures efficient, flexible, and practice-oriented knowledge acquisition and assessment. The system is characterized by high flexibility and easy opportunities for improvement and further development, as it was created using modern web application development technologies. Its effectiveness was also confirmed by a user study, where as many as 80.8% of respondents indicated that the platform helped improve their cybersecurity knowledge.

In addition, the developed system can be adapted for other organizations or institutions seeking to strengthen employees' cybersecurity competencies. In the future, the platform's functionality is planned to be expanded by integrating additional interactive learning tools, such as simulations and practical tasks, which would further increase learning effectiveness.

Turinys

Lentelių sąrašas.....	8
Paveikslų sąrašas.....	9
Santrumpų ir terminų sąrašas.....	11
Įvadas	12
1. Krašto apsaugos sistemos personalo kibernetinio saugumo įgūdžių poreikis ir pažangių ugdymo sprendimų apžvalga.....	14
1.1. Kibernetinio saugumo samprata ir reikšmė krašto apsaugos sistemoje	14
1.2. Nuotolinio mokymosi raida ir aktualumas	15
1.3. Nuotolinio mokymosi platformos ir jų galimybės	15
1.4. Pažangių technologinių sprendimų klasifikacija	15
1.5. Technologinių sprendimų taikymo iššūkiai.....	16
1.6. Skyriaus išvados.....	16
2. Krašto apsaugos sistemos personalo kibernetinio saugumo ugdymo situacija ir tyrimo rezultatų analizė.....	17
2.1. Esamos kibernetinio saugumo ugdymo priemonės krašto apsaugos sistemoje	17
2.2. Esamų mokymo sprendimų trūkumai	17
2.3. Kibernetinio saugumo ugdymo tobulinimo kryptys	18
2.4. Tyrimo metodika.....	18
2.5. Apklauskos rezultatų analizė	18
2.6. Tyrimo rezultatų apibendrinimas ir rekomendacijos	19
2.7. Nacionalinio kibernetinio saugumo ataskaitų analizė.....	22
2.8. Skyriaus išvados.....	26
3. Virtualiųjų mokymosi aplinkų analizė ir taikymo galimybės	27
3.1. Moodle paskirtis ir pagrindinės savybės	27
3.2. Moodle ir Open eClass virtualiųjų mokymosi aplinkų palyginamoji analizė	29
3.3. Skyriaus išvados.....	31
4. Virtualios mokymosi aplinkos reikalavimų specifikacija ir modeliavimas.....	32
4.1. Virtualios mokymosi aplinkos reikalavimai.....	32
4.2. Sistemos funkcionalumo modeliavimas	34
4.3. Skyriaus išvados.....	38
5. Kibernetinio saugumo ugdymo poreikio pagrindimas remiantis KAS duomenų analize ..	39
5.1. Tyrimo metodas ir duomenų šaltiniai.....	39
5.2. Elektroninio pašto apsaugos duomenų analizė	40
5.3. Kibernetinių incidentų analizė	41
5.4. Kibernetinio saugumo įgūdžių ugdymo poreikių identifikavimas.....	42
5.5. Skyriaus išvados.....	42
6. Nuotolinio kibernetinio saugumo įgūdžių ugdymo paramos modelis	43
6.1. Nuotolinio mokymosi dalyvių vaidmenys, atsakomybės ir bendradarbiavimas	43
6.2. Kibernetinio saugumo įgūdžių ugdymo paramos teikimo planas.....	44
6.3. Kibernetinio saugumo įgūdžių ugdymo požymių diagrama.....	45
6.4. Kibernetinio saugumo ugdymo kontekstinis grafas	47
6.5. Skyriaus išvados.....	48
7. Virtualios mokymosi aplinkos realizacija	50
7.1. Sprendimo pagrindimas ir santykis su esamomis sistemomis.....	50
7.2. Sukurto produkto aprašas	51

7.3. Programinės įrangos priemonės sistemos realizacijai	51
7.4. Sistemos realizavimo eiga	52
7.5. Platformos taikymo ir poveikio vartotojų žinioms tyrimas	53
7.6. Tyrimo rezultatai.....	53
7.7. Skyriaus išvados.....	54
Išvados	55
Literatūros sąrašas.....	56
Priedai	58
1 priedas. Sistemų diegimo instrukcijos.....	58
2 priedas. DI įrankių naudojimas	67
3 priedas. Sistemos realizacijos fragmentai.....	70
4 priedas. Kibernetinio saugumo įgūdžių ir mokymosi poreikių anketa	85
5 priedas. Kibernetinio saugumo mokymosi platformos vertinimo anketa.....	91
6 priedas. Diegimo akto patvirtinimas	95

Lentelių sąrašas

1 lentelė. Panaudojimo atvejo specifikacija.....	36
2 lentelė. Moodle ir Open eClass funkcionalumų palyginimas	29
3 lentelė. Kibernetinio saugumo ugdymo nuotoliniu būdu paramos teikimo planas	45
4 lentelė. Kontekstinių sąlygų mazgai (C1–C6)	47
5 lentelė. Veiksmų mazgai (A1–A7).....	47
6 lentelė. Užklausa Claude AI:.....	67
7 lentelė. Gautas Claude AI atsakymas:	67
8 lentelė. Pateiktas atsakymas Claude AI:	69

Paveikslų sąrašas

1 pav. Problemų medis	20
2 pav. Tikslų medis.....	21
3 pav. Kibernetinių incidentų statistika [9-13].....	22
4 pav. Informacinių incidentų skaičius strateginėse srityse [12]	23
5 pav. Informacinių incidentų pasiskirstymas pagal strategines sritis 2022 metais [12]	23
6 pav. Incidentų grupės [12-13]	24
7 pav. Asmens duomenų saugumo pažeidimų priežastys [12-13]	25
8 pav. Administratoriaus, dėstytojo ir studento panaudojimo atvejų diagrama.....	35
9 pav. Studento panaudojimo atvejų diagrama	36
10 pav. Pagrindinio ir alterantivaus scenarijaus veiklos diagrama	38
11 pav. El. pašto apsaugos statistika	40
12 pav. Kibernetinių incidentų statistika	41
13 pav. Kibernetinio saugumo ugdymo požymių diagrama	46
14 pav. KAS personalo kibernetinio saugumo ugdymo kontekstinis grafas	48
15 pav. Pagrindinės programinės įrangos.....	52
16 pav. Prisijungimas „GitHub“ sukurtas.....	58
17 pav. „Git“ atsisiuntimas	59
18 pav. „Git“ įdiegimas	59
19 pav. „Git“ įdiegimas baigtas	60
20 pav. „Node.js“ atsisiuntimas	61
21 pav. „Node.js“ įdiegimas	61
22 pav. „Node.js“ įdiegimas baigtas.....	62
23 pav. Prisijungimas prie „Supabase“	63
24 pav. Prisijunta prie „Supabase“	63
25 pav. Prisijunta prie „Vercel“	64
26 pav. „Cursor“ programos parsisiuntimas	65
27 pav. „Cursor“ įdiegimas.....	66
28 pav. „Cursor“ įdiegtas.....	66
29 pav. Sukuriame naują projektą.....	70
30 pav. PRD įkėlimas į „Cursor“	70
31 pav. Užduočių ir subužduočių planas	71
32 pav. Projekto failų struktūra integruotoje programavimo aplinkoje	71
33 pav. Duomenų bazės lentelių sąrašas „Supabase“ aplinkoje	72
34 pav. Kursų duomenų bazės lentelių ir jų tarpusavio ryšių diagrama.....	72
35 pav. „Supabase“ įgalintos prisijungimo funkcijos.....	73
36 pav. Sistemos publikavimo ir versijavimo procesas.....	73
37 pav. Prisijungimo langas su el. paštu arba „google“	74
38 pav. Pagrindinio puslapio vaizdas prisijungus vartotojui	74
39 pav. Mokymosi platformos kursų peržiūros ir pasirinkimo puslapis	75
40 pav. Pamokos mokomosios medžiagos pateikimo puslapis.....	75
41 pav. Kurso peržiūros puslapis su pamokų sąrašu	76
42 pav. Pamokos žinių patikrinimo (testo) puslapis.....	76
43 pav. Žinių patikrinimo (testo) rezultatų puslapis.....	77
44 pav. Galutinio kibernetinio saugumo žinių patikrinimo testo puslapis	77

45 pav. Galutinio žinių patikrinimo testo rezultatai ir sertifikato suteikimas.....	78
46 pav. Diskusijų forumo puslapis mokymosi platformoje.....	78
47 pav. Vidinių žinučių (pranešimų) sistemos puslapis	79
48 pav. Vartotojo profilio puslapis su mokymosi pažanga ir sertifikatais	79
49 pav. Vartotojo testų istorijos ir sertifikatų peržiūros puslapis.....	80
50 pav. Automatiškai sugeneruoto mokymų sertifikato su rezultatais ir galiojimo informacija vaizdas	80
51 pav. Atsisiųsto kibernetinio saugumo mokymų sertifikato vaizdas	81
52 pav. Administratoriaus pagrindinis puslapis prisijungus prie sistemos.....	81
53 pav. Administratoriaus kurso valdymo puslapis su pamokų redagavimo funkcijomis	82
54 pav. Administratoriaus valdymo panelė mokymosi platformoje	82
55 pav. Vartotojų valdymo puslapis administratoriaus aplinkoje.....	83
56 pav. Sertifikatų stebėjimo ir valdymo panelė administratoriaus aplinkoje.....	83
57 pav. Administratoriaus vartotojo veiklos ir mokymosi pažangos stebėsenos puslapis	84
58 pav. Vartotojo atlikto testo atsakymų analizės puslapis	84
59 pav. Anketos klausimai 1-4.....	85
60 pav. Anketos klausimai 5-9.....	86
61 pav. Anketos klausimai 10-14.....	87
62 pav. Anketos klausimai 15-18.....	88
63 pav. Anketos klausimai 19-22.....	89
64 pav. Anketos klausimai 23-25.....	90
65 pav. Vertinimo anketos klausimai 1-2	91
66 pav. Vertinimo anketos klausimai 3-6.....	92
67 pav. Vertinimo anketos klausimai 7-10	93
68 pav. Vertinimo anketos klausimai 11-14	94

Santrumpų ir terminų sąrašas

Santrumpos:

NM – nuotolinis mokymasis;

VM – virtualusis mokymasis;

VMA – virtualioji mokymosi aplinka;

KAS – Krašto apsaugos sistema;

NKSC – Nacionalinio kibernetinio saugumo centras;

MVP – Minimalus veikiantis produktas;

ADSP – Asmens duomenų saugumo pažeidimų;

RIS – Ryšių ir informacinės sistemos;

PRD – Produkto reikalavimų dokumentas;

DI – Dirbtinis intelektas.

Terminai:

Prototipas – (angl. prototype) priminis, ankstyvas sistemos ar programos pavyzdys, pagal kurį daromi kiti sistemos patobulinai, programos.

Įvadas

Kibernetinis saugumas tampa vienu svarbiausių veiksnių užtikrinant valstybės institucijų veiklos stabilumą ir informacinių sistemų patikimumą. Krašto apsaugos sistemoje naudojamos informacinės sistemos yra kritiškai svarbios, todėl jų pažeidžiamumas gali turėti tiesioginę įtaką nacionaliniam saugumui. Didelė dalis kibernetinių incidentų kyla ne dėl technologinių spragų, bet dėl žmogiškojo faktoriaus – darbuotojų klaidų, nepakankamų žinių ar netinkamų saugumo įpročių.

Remiantis Nacionalinio kibernetinio saugumo centro (toliau – NKSC) ataskaitomis bei krašto apsaugos sistemos institucijų duomenimis, pastebima, kad kibernetinių incidentų skaičius išlieka reikšmingas, o jų sudėtingumas didėja. Tai rodo, kad esamos prevencinės priemonės nėra pakankamai efektyvios, ypač ugdant personalo kibernetinio saugumo įgūdžius.

Tradiciniai mokymo metodai ne visada užtikrina nuolatinį ir efektyvų žinių atnaujinimą, todėl atsiranda poreikis taikyti modernesnius sprendimus. Vienas iš tokių sprendimų – virtualiosios mokymosi aplinkos (toliau – VMA), leidžiančios organizuoti lankstų, nuolatinį ir individualizuotą mokymosi procesą.

Darbo problema

Krašto apsaugos sistemos personalas susiduria su informacinių sistemų ir duomenų pažeidžiamumo rizika, kuri didina kibernetinių atakų tikimybę, o esami tradiciniai mokymo metodai neužtikrina pakankamo praktinių įgūdžių ugdymo.

Darbo objektas

Krašto apsaugos sistemos personalo kibernetinio saugumo įgūdžių ugdymo procesas.

Darbo tikslas – pagerinti krašto apsaugos sistemos personalo kibernetinio saugumo įgūdžius, sukuriant virtualiąją mokymosi aplinką.

Darbo uždaviniai:

1. išanalizuoti kibernetinių grėsmių dinamiką ir incidentų duomenis krašto apsaugos sistemoje;
2. ištirti krašto apsaugos sistemos personalo kibernetinio saugumo įgūdžių lygi bei nuotolinio mokymosi poreikius;
3. įvertinti esamų virtualiųjų mokymosi aplinkų funkcionalumą ir pagrįsti mokymosi sprendimo poreikį;
4. suprojektuoti virtualiąją mokymosi aplinką ir suformuoti nuotolinio mokymosi paramos modelį;
5. realizuoti virtualiąją mokymosi platformą ir įvertinti jos efektyvumą atliekant vartotojų testavimą.

Tyrimo metodai:

1. mokslinės literatūros ir kitų dokumentų analizė;
2. kiekybinis tyrimas, taikant anketinės apklausos metodą;
3. statistinė duomenų analizė;
4. lyginamoji analizė;
5. modeliavimo metodas;
6. eksperimentinis tyrimas.

Darbo rezultatas – pagerinti personalo kibernetinio saugumo įgūdžiai ir gebėjimai atpažinti bei tinkamai reaguoti į kibernetines grėsmes, taip sustiprinant organizacijos atsparumą kibernetinėms atakoms.

Darbo produktas – sukurta virtualioji mokymosi aplinka, skirta kibernetinio saugumo įgūdžių mokymams (produkto diegimą patvirtinantis aktas pateiktas 6 priede).

Dokumento struktūra

Šį magistro baigiamąjį projektą sudaro įvadas, 7 pagrindiniai skyriai, išvados, naudotos literatūros sąrašas ir 6 priedai. Pirmajame skyriuje apžvelgiamas kibernetinio saugumo įgūdžių poreikis KAS bei analizuojami pažangūs nuotolinio mokymosi technologiniai sprendimai. Antrajame skyriuje analizuojama esama KAS personalo ugdymo situacija, pristatomi darbuotojų apklausos rezultatai, atliekama nacionalinių incidentų ataskaitų analizė bei sudaromi problemų ir tikslų medžiai. Trečiajame skyriuje atliekama virtualių mokymosi aplinkų („Moodle“ ir „Open eClass“) taikymo galimybių bei palyginamoji analizė. Ketvirtajame skyriuje suformuluojami kuriamos mokymosi aplinkos funkciniai bei nefunkciniai reikalavimai ir atliekamas sistemos funkcionalumo modeliavimas pagal UML panaudojimo atvejų metodiką. Penktajame skyriuje, remiantis KAS elektroninio pašto apsaugos ir incidentų duomenimis, detalai pagrindžiamas kibernetinio saugumo mokymų poreikis organizacijos viduje. Šeštajame skyriuje suprojektuojamas nuotolinio mokymosi paramos modelis, apibrėžiantis dalyvių vaidmenis, atsakomybes ir ugdymo procesų sąveiką. Galiausiai, septintajame skyriuje aprašoma specializuotos virtualiosios mokymosi aplinkos programinė realizacija bei pateikiami sukurto produkto testavimo su vartotojais rezultatai ir jų kokybinė analizė. Darbo pabaigoje suformuluotos išvados bei pateikti tiriamąjį darbą papildantys priedai. Antrajame priede yra pateiktas dirbtinio intelekto naudojimo rengiant baigiamąjį projektą aprašas.

1. Krašto apsaugos sistemos personalo kibernetinio saugumo įgūdžių poreikis ir pažangių ugdymo sprendimų apžvalga

Šiame skyriuje nagrinėjamas kibernetinio saugumo įgūdžių poreikis krašto apsaugos sistemoje, analizuojama jų samprata bei reikšmė valstybės gynybai. Aptariamas kibernetinių grėsmių pobūdis ir mastas, pateikiama Lietuvos kibernetinių incidentų statistinė analizė bei vertinama žmogiškojo faktoriaus įtaka organizacijos atsparumui grėsmėms, pabrėžiant, kad vien technologinių apsaugos priemonių nepakanka sistemų saugumui užtikrinti. Taip pat apžvelgiami technologiniai sprendimai, skirti efektyviam personalo kibernetinio saugumo įgūdžių ugdymui nuotoliniu būdu. Analizuojama nuotolinio mokymosi raida ir aktualumas, įvairių mokymosi platformų teikiamos galimybės, sisteminiams šiuolaikiniams mokymo sprendimams, įskaitant dirbtinio intelekto įrankius, bei įvertinami pagrindiniai iššūkiai, kylantys juos diegiant ir pritaikant organizacijos poreikiams.

1.1. Kibernetinio saugumo samprata ir reikšmė krašto apsaugos sistemoje

Kibernetinis saugumas apima gebėjimą naudotis informacinėmis technologijomis saugiai, efektyviai bei etiškai. KAS šie gebėjimai yra ypač svarbūs, nes personalas kasdien susiduria su jautria informacija, kurios apsauga yra kritinė siekiant užtikrinti valstybės gynybą [1].

KAS įdiegta daug pažangių informacinių technologijų sprendimų, tačiau jų saugumas tiesiogiai priklauso nuo personalo gebėjimo tinkamai jomis naudotis. Tai rodo, kad net ir turint pažangias technologijas, jų efektyvumas gali būti ribotas, jei personalas neturi pakankamų kibernetinio saugumo žinių ir praktinių įgūdžių.

Kibernetinių grėsmių pobūdis ir mastas. Kibernetinės grėsmės yra viena iš dažniausiai pasitaikančių šiuolaikinių saugumo problemų. Jų poveikis gali būti pražūtingas ne tik civilinėms, bet ir gynybos struktūroms. Statistikos duomenimis, daugiau nei 70 % kibernetinių atakų yra nukreiptos į strateginės svarbos infrastruktūrą, įskaitant karines sistemas [2]. Lietuvoje taip pat stebima didėjanti grėsmių tendencija, kai organizacijos, įskaitant KAS, susiduria su duomenų nutekėjimu ar kitais saugumo incidentais [3]. KAS įdiegta daugybė pažangių technologijų, tačiau personalo pasirengimas jas naudoti saugiai labai priklauso nuo jų patirties, išsilavinimo ir turimų žinių [4].

Tai leidžia daryti išvadą, kad kibernetinės grėsmės tampa vis sudėtingesnės ir sunkiau atpažįstamos, todėl vien tik technologinės apsaugos priemonės gali būti nepakankamos.

Kibernetinių incidentų statistinė analizė Lietuvoje. Nacionalinis kibernetinio saugumo centras 2023 metais užregistravo 2 378 kibernetinius incidentus [5]. Palyginus šiuos duomenis su ankstesniais metais, galime teigti, kad bendras kibernetinių incidentų skaičius mažėja. Tačiau analizuojant incidentų pavojingumo rodiklius, pastebėtas 12 % padidėjimas. Tai reiškia, kad incidentai tampa sudėtingesni ir pavojingesni.

2023 metais Lietuvoje dėl asmens duomenų saugumo pažeidimų (toliau – ADSP) paveiktų duomenų subjektų skaičius siekė 57 833. Tai yra triskart mažiau nei ankstesniais metais, rodantis teigiamą tendenciją. Tačiau tarp paveiktų objektų 49 % pažeidimų įvyko dėl kibernetinių atakų, o 51 % – dėl kitų priežasčių. ADSP analizė rodo, kad pagrindinė priežastis yra žmogiškoji klaida 72 % atvejų, likę 28 % buvo nulemti kitų veiksnių [5].

Tai rodo, kad žmogiškasis faktorius yra viena iš pagrindinių kibernetinio saugumo rizikų priežasčių, todėl būtina skirti didesnę dėmesį personalo mokymui ir įgūdžių ugdymui.

Žmogiškojo faktoriaus įtaka. Pagal ADSP pobūdį, didžioji dalis pažeidimų 76 % buvo susijusi su konfidencialumo užtikrinimo trūkumais. Be to, žmogiškosios klaidos atvejų skaičius per 2023 metus pastebimai išaugo net 12 % palyginus su praėjusiais metais.

Šie duomenys atskleidžia ne tik kibernetinio saugumo iššūkių mastą, bet ir būtinybę nuosekliai stiprinti personalo kompetencijas, siekiant užtikrinti efektyvią ir saugią KAS veiklą. Tai rodo, kad žmogiškasis faktorius yra viena iš pagrindinių kibernetinio saugumo rizikų priežasčių, todėl būtina skirti didesnę dėmesį personalo mokymui ir įgūdžių ugdymui.

1.2. Nuotolinio mokymosi raida ir aktualumas

Nuotolinis mokymasis (toliau – NM) tampa vis aktualesnis ir patrauklesnis būdas įgyti žinių. 2020 metais, kai visoje šalyje buvo įvestas karantinas dėl užkrečiamos ligos COVID-19, daugelis darbuotojų ir mokslo įstaigų perėjo prie nuotolinio darbo ir mokymosi. Pradžioje tai sukėlė nemažai nepatogumų, nes toks mokymosi būdas anksčiau nebuvo plačiai propaguojamas. Tačiau per dvejus metus tiek darbuotojams, tiek moksleiviams teko prisitaikyti prie informacinių technologijų naudojimo kasdieniame gyvenime. Pasibaigus pandemijai, daugelis darbdavių vis dar taiko nuotolinius kursus, siekdami kelti savo darbuotojų kvalifikaciją.

Siekiant efektyviai ugdyti šiuos įgūdžius, būtina taikyti pažangius technologinius sprendimus, kurie ne tik perteikia teorines žinias, bet ir suteikia praktinių įgūdžių.

Nuotolinio mokymosi plėtra rodo, kad šis mokymo būdas tapo ne laikinu sprendimu, o nuolatine mokymosi forma. Tai leidžia daryti prielaidą, kad KAS taip pat galima efektyviai taikyti nuotolinio mokymo sprendimus, ypač siekiant užtikrinti nuolatinį personalo kibernetinio saugumo įgūdžių atnaujinimą.

1.3. Nuotolinio mokymosi platformos ir jų galimybės

Nuotolinio mokymosi platformos, tokios kaip „Moodle“ ar „Blackboard“, leidžia kurti struktūrizuotus kursus su įvairiomis mokymosi priemonėmis. Jos suteikia galimybę integruoti vaizdo įrašus, interaktyvias užduotis bei testus, skatinančius aktyvų mokymąsi. Tyrimai rodo, kad tokios platformos padeda efektyviai perduoti kibernetinio saugumo žinias ir ugdyti praktinius įgūdžius [6].

Virtualiosios laboratorijos suteikia galimybę praktikuoti kibernetinio saugumo įgūdžius realistiškoje aplinkoje. Pavyzdžiui, „Cyber Range“ platformos leidžia vartotojams imituoti kibernetines atakas ir gynybos strategijas, taip ugdant praktinius gebėjimus. Tyrimai pabrėžia, kad tokios simuliacijos padidina mokymosi efektyvumą ir pasirengimą realioms grėsmėms [7].

Šios platformos rodo, kad šiuolaikinės mokymosi technologijos leidžia pereiti nuo pasyvaus žinių perteikimo prie aktyvaus ir praktinio mokymosi. Tai ypač svarbu kibernetinio saugumo srityje, kur vien teorinės žinios nėra pakankamos, o gebėjimas atpažinti ir valdyti realias grėsmes yra esminis.

1.4. Pažangių technologinių sprendimų klasifikacija

Šiandien informacinių technologijų erdvė siūlo įvairius pažangius technologinius sprendimus, skirtus nuotoliniam mokymuisi. Tarp jų galima išskirti šias kategorijas [8]:

- Atviri internetiniai kursai;
- Mobilųjų įrenginių programėlės;

- Nuotolinio mokymosi platformos;
- Edukaciniai žaidimai ir simuliacijos;
- Virtualioji realybė ir papildyta realybė;
- Dirbtinis intelektas ir personalizuotas mokymas;
- Debesijos pagrindu veikiančios mokymosi platformos.

Šių technologijų įvairovė leidžia pritaikyti mokymosi procesą skirtingiems naudotojų poreikiams ir kompetencijų lygiams. Tai suteikia galimybę kurti individualizuotus mokymo sprendimus, kurie yra efektyvesni nei vienodi visiems skirti mokymo metodai.

1.5. Technologinių sprendimų taikymo iššūkiai

Pažangūs technologiniai sprendimai leidžia efektyviai ugdyti žinias nuotoliniu būdu. Tačiau svarbu pažymėti, kad tinkamas kiekvienos technologijos naudojimas reikalauja mokymosi. Technologijos vystosi itin sparčiai, todėl kartais gali būti sudėtinga suspėti su jų pažanga. Kai pripranti dirbti su viena informacine sistema, pereiti prie kitos, apie kurią dar nieko nežinai, gali būti nemenkas iššūkis.

Tai rodo, kad technologijų diegimas savaime neužtikrina efektyvaus mokymosi proceso. Svarbu ne tik pasirinkti tinkamus sprendimus, bet ir užtikrinti jų prieinamumą, paprastumą bei vartotojų pasirengimą jais naudotis. Priešingu atveju net pažangios technologijos gali būti neefektyvios.

1.6. Skyriaus išvados

1. Atlikta analizė parodė, kad KAS kibernetinis saugumas yra kritiškai svarbus dėl naudojamų informacinių sistemų reikšmės valstybės saugumui. Nustatyta, kad kibernetinių grėsmių sudėtingumas nuolat didėja, o reikšminga dalis incidentų yra susijusi su žmogiškuoju faktoriumi. Tai leidžia teigti, kad vien technologinės saugumo priemonės nėra pakankamos užtikrinti efektyvią apsaugą. Siekiant mažinti kibernetinių incidentų riziką, būtina sistemingai ugdyti personalo kibernetinio saugumo įgūdžius.
2. Atlikta pažangių technologinių sprendimų analizė parodė, kad NM tapo plačiai taikomu ir efektyviu žinių perdavimo būdu, kuris gali būti sėkmingai pritaikytas ir KAS. Nustatyta, kad šiuolaikinės mokymosi platformos ir technologiniai sprendimai leidžia ne tik perteikti teorines žinias, bet ir ugdyti praktinius kibernetinio saugumo įgūdžius.
3. Taip pat nustatyta, kad technologijų įvairovė suteikia galimybę kurti lankstų ir individualizuotą mokymosi procesą, kuris geriau atitinka skirtingų naudotojų poreikius. Tačiau pažymėtina, kad vien technologinių sprendimų taikymas nėra pakankamas – būtina atsižvelgti į naudotojų pasirengimą ir gebėjimą efektyviai naudotis šiomis technologijomis.
4. Atsižvelgiant į tai, galima teigti, kad pažangūs technologiniai sprendimai sudaro prielaidas efektyviam kibernetinio saugumo įgūdžių ugdymui, tačiau jų taikymas turi būti derinamas su tinkamai organizuotu mokymosi procesu ir naudotojų parama.

2. Krašto apsaugos sistemos personalo kibernetinio saugumo ugdymo situacija ir tyrimo rezultatų analizė

Įvertinus technologinių sprendimų įvairovę, šiame skyriuje analizuojamos konkrečios krašto apsaugos sistemos personalo kibernetinio saugumo įgūdžių ugdymo galimybės bei esama situacija. Pirmiausia apžvelgiamos KAS taikomos kibernetinio saugumo ugdymo priemonės ir atliekama kritinė jų analizė, identifikuojant pagrindinius esamų mokymo sprendimų trūkumus, ypatingą dėmesį skiriant praktinių įgūdžių bei motyvacijos stokai. Siekiant išsamiau įvertinti problematiką, pristatomas tyrimas, kurio tikslas – nustatyti KAS personalo kibernetinio saugumo žinių lygį, saugumo įpročius ir mokymosi poreikius. Aprašoma pasirinkta tyrimo metodika, analizuojami apklausos rezultatai, vertinamas darbuotojų požiūris į nuotolinį mokymąsi bei pateikiamos problemų ir tikslų medžių analizės. Tyrimas papildomas Nacionalinio kibernetinio saugumo centro ataskaitų analize, leidžiančia nustatyti strateginių sričių pažeidžiamumą, dažniausias incidentų grupes ir pagrindines asmens duomenų saugumo pažeidimų priežastis. Remiantis gautais rezultatais, skyriaus pabaigoje suformuluojamos pagrindinės tobulinimo kryptys, skirtos lankstesnio, efektyvesnio ir personalizuoto mokymosi proceso kūrimui.

2.1. Esamos kibernetinio saugumo ugdymo priemonės krašto apsaugos sistemoje

KAS kibernetinio saugumo ugdymas nuotoliniu būdu vyksta naudojant tokias platformas kaip NKSC ir ILIAS, kurios leidžia įsisavinti teorines žinias. Taip pat organizuojamos kibernetinės pratybos „Gintarinė migla“, kuriose dalyvauja ryšių ir informacinių sistemų (toliau – RIS) specialistai. Pratybų metu simuliuojami kibernetiniai išpuoliai, o personalas lavina savo reakcijas ir gebėjimus spręsti praktines problemas.

Nacionalinis kibernetinio saugumo centras taip pat siūlo nemokamus kibernetinio saugumo mokymus, kurie yra prieinami visiems norintiems. Šie kursai apima pagrindines temas, tokias kaip duomenų apsauga, grėsmių prevencija ir saugaus elgesio internete praktikos. Ši iniciatyva ne tik stiprina nacionalinį kibernetinį atsparumą, bet ir skatina bendrą žinių plėtrą [9].

Tai rodo, kad KAS jau egzistuoja įvairios kibernetinio saugumo ugdymo priemonės, apimančios tiek teorinius mokymus, tiek praktines veiklas. Tačiau šios priemonės dažniausiai yra fragmentuotos ir nėra integruotos į vieningą, nuoseklią mokymosi sistemą, kuri užtikrintų nuolatinį personalo kompetencijų ugdymą.

2.2. Esamų mokymo sprendimų trūkumai

Dabartiniuose mokymuose pastebimos kelios problemos. Pirmą, mokymo turinys dažnai apsiriboja teorinėmis žiniomis, kurios kai kam gali atrodyti visiškai neįdomios ir sunkiai suprantamos. Antra, trūksta personalizuotų mokymo modulių ir motyvacinės sistemos, kuri skatintų aktyvų darbuotojų dalyvavimą bei tobulėjimą.

Šie trūkumai rodo, kad esami mokymo sprendimai nėra pakankamai orientuoti į praktinių įgūdžių formavimą ir individualius besimokančiųjų poreikius. Dėl to mokymosi procesas gali būti neefektyvus, o įgytos žinios – sunkiai pritaikomos realiose situacijose, susijusiose su kibernetinėmis grėsmėmis.

2.3. Kibernetinio saugumo ugdymo tobulinimo kryptys

Siekiant efektyviai tobulinti kibernetinio saugumo ugdymą nuotoliniu būdu, būtina atlikti darbuotojų apklausas, siekiant nustatyti esamas spragas ir tobulintinas sritis. Taip pat svarbu kurti personalizuotus mokymus, kurie apimtų tiek teorinius, tiek praktinius aspektus.

Rekomenduojama organizuoti bandomuosius mokymus, rinkti grįžtamąjį ryšį ir jį panaudoti mokymo programų bei procesų tobulinimui.

Šios kryptys rodo, kad efektyvus kibernetinio saugumo ugdymas turi būti grindžiamas duomenimis ir nuolatiniu grįžtamoju ryšiu. Tai leidžia pereiti nuo vienkartinį mokymų prie nuoseklaus ir adaptuojamo mokymosi proceso, kuris geriau atitinka realius organizacijos poreikius ir kintančią kibernetinių grėsmių aplinką.

2.4. Tyrimo metodika

Apklausa buvo skirta nustatyti KAS dirbančių asmenų kibernetinio saugumo lygį, mokymosi poreikius ir požiūrį į nuotolinio mokymosi galimybes. Pagrindiniai klausimai apėmė kibernetinio saugumo supratimą, mokymosi poreikių ir prioritetų įvertinimą, atsižvelgiant į kibernetinio saugumo grėsmes, bei darbuotojų požiūrį į nuotolinio mokymosi efektyvumą.

NM populiarėjantis dėl technologinės pažangos ir patogumo, gali tapti efektyvia priemone tobulinti kibernetinio saugumo įgūdžius KAS, kur informacinių technologijų naudojimas yra esminis.

Tyrime dalyvavo 20 respondentų, kurie atsakė į 25 klausimų anketą (žr. 4 priedą), apimančią demografinę informaciją, kibernetinės saugos principų supratimą, kibernetinio saugumo praktiką bei nuotolinio mokymosi galimybes. Duomenys buvo surinkti naudojant „Google Forms“ platformą.

Pasirinkta tyrimo metodika leidžia įvertinti bendrą KAS personalo kibernetinio saugumo situaciją bei identifikuoti pagrindines problemas. Nors respondentų skaičius nėra didelis, gauti duomenys leidžia nustatyti pagrindines tendencijas ir suformuoti tolesnes kibernetinio saugumo ugdymo kryptis.

2.5. Apklausos rezultatų analizė

Apklausos rezultatai parodė, kad KAS personalo kibernetinio saugumo lygis nėra pakankamas. 25 % respondentų įvertino savo kibernetinio saugumo lygį kaip žemą arba labai žemą, o tik 35 % – kaip labai aukštą.

Be to, 65 % apklaustųjų nenaudoja skirtingų slaptažodžių skirtingoms paskyroms, o 45 % nenaudoja dviejų veiksmų autentifikacijos, taip didindami sistemų pažeidžiamumą.

Žinių apie kibernetinio saugumo principus trūkumas yra reikšmingas – 35 % respondentų nežino, kas yra konfidencialumas, o 50 % – prieinamumas.

Didelė žmogiškosios klaidos rizika taip pat išryškėjo, kai 50 % apklaustųjų paspaudė ant apgaulingų SMS nuorodų, o 35 % sąmoningai ar per klaidą atidarė melagingus elektroninius laiškus.

Šie rezultatai aiškiai rodo, kad pagrindinė kibernetinio saugumo problema yra susijusi su žmogiškuoju faktoriumi. Net ir esant technologinėms apsaugos priemonėms, netinkamas naudotojų

elgesys išlieka viena didžiausių rizikų. Tai patvirtina būtinybę stiprinti praktinius įgūdžius ir keisti naudotojų elgseną, o ne tik perteikti teorines žinias.

Nuotolinio mokymosi vertinimas. Nuotolinį mokymą 35 % respondentų vertina kaip labai efektyvų, tačiau 15 % – kaip visiškai neefektyvų. Tuo tarpu 50 % apklaustųjų nurodė motyvacijos stoką kaip pagrindinę kliūtį dalyvauti mokymuose.

Gauti rezultatai rodo, kad NM yra vertinamas nevienareikšmiškai. Nors dalis respondentų jį vertina teigiamai, motyvacijos trūkumas išlieka esminė problema. Tai leidžia daryti išvadą, kad vien technologinių sprendimų nepakanka – būtina užtikrinti įtraukiantį, interaktyvų ir motyvuojantį mokymosi procesą.

2.6. Tyrimo rezultatų apibendrinimas ir rekomendacijos

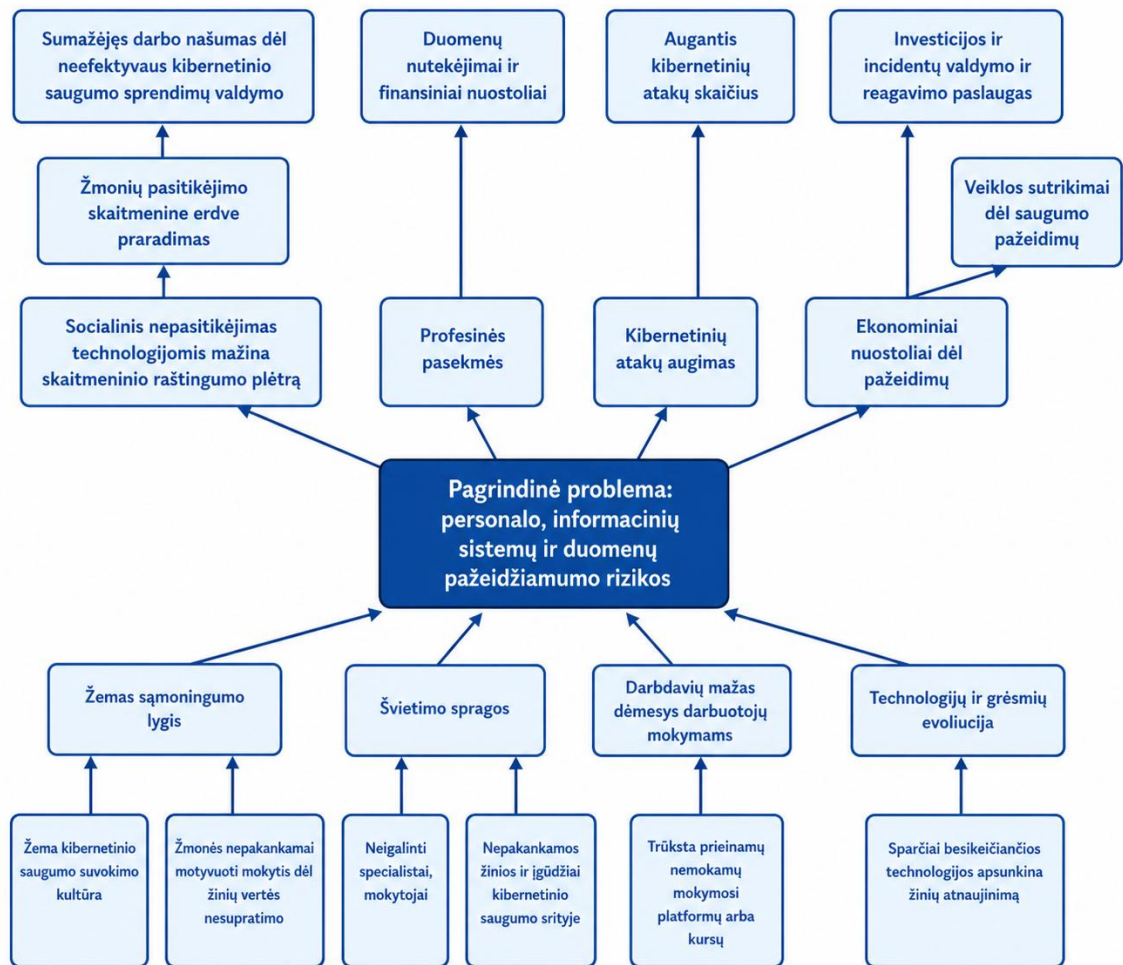
Siekiant pagerinti kibernetinio saugumo ugdymą, būtina tobulinti mokymo programas, integruoti daugiau praktinių užduočių ir pažangių technologijų, tokių kaip virtualiosios laboratorijos ir simuliacijos, bei skatinti mišrių mokymo formų taikymą, kurios geriau atitiktų darbuotojų poreikius.

Šios priemonės padėtų efektyviau ugdyti personalo gebėjimus, sumažinti žmogiškosios klaidos tikimybę ir užtikrinti didesnę atsparumą kibernetinėms grėsmėms.

Rekomendacijos tiesiogiai susijusios su nustatytomis problemomis ir atspindi būtinybę pereiti prie modernesnių, į praktiką orientuotų mokymo sprendimų. Tai sudaro pagrindą tolimesniam virtualiosios mokymosi aplinkos projektavimui.

Problemų medžio analizė. Problemų medis parodo iššūkius, su kuriais susiduria KAS personalas, informacinės sistemos ir duomenų saugumas. Jo centre išskiriama pagrindinė problema – personalo, informacinių sistemų ir duomenų pažeidžiamumo rizika. Šios problemos šaknys siejamos su personalo žinių trūkumu, kibernetinio saugumo mokymo programų spragomis ir žemu mokymosi motyvacijos lygiu.

Problemų medžio viršutinėje dalyje pateikiamos pasekmės – padidėjusi kibernetinių incidentų rizika, duomenų nutekėjimas bei grėsmė nacionaliniam saugumui (žr. 1 pav.).



1 pav. Problemų medis

Apklausoje rezultatai parodė glaudžią sąsają su problemų medžiu, atskleidžiant tiek esamas problemas, tiek jų priežastis. Žemas kibernetinio saugumo lygis išryškėjo, kai 25 % respondentų savo žinias įvertino kaip žemas arba labai žemas, o tik 35 % – kaip labai aukštas. Tai atspindi problemų medžio šaknis, kuriose nurodomas žinių ir mokymo spragų trūkumas.

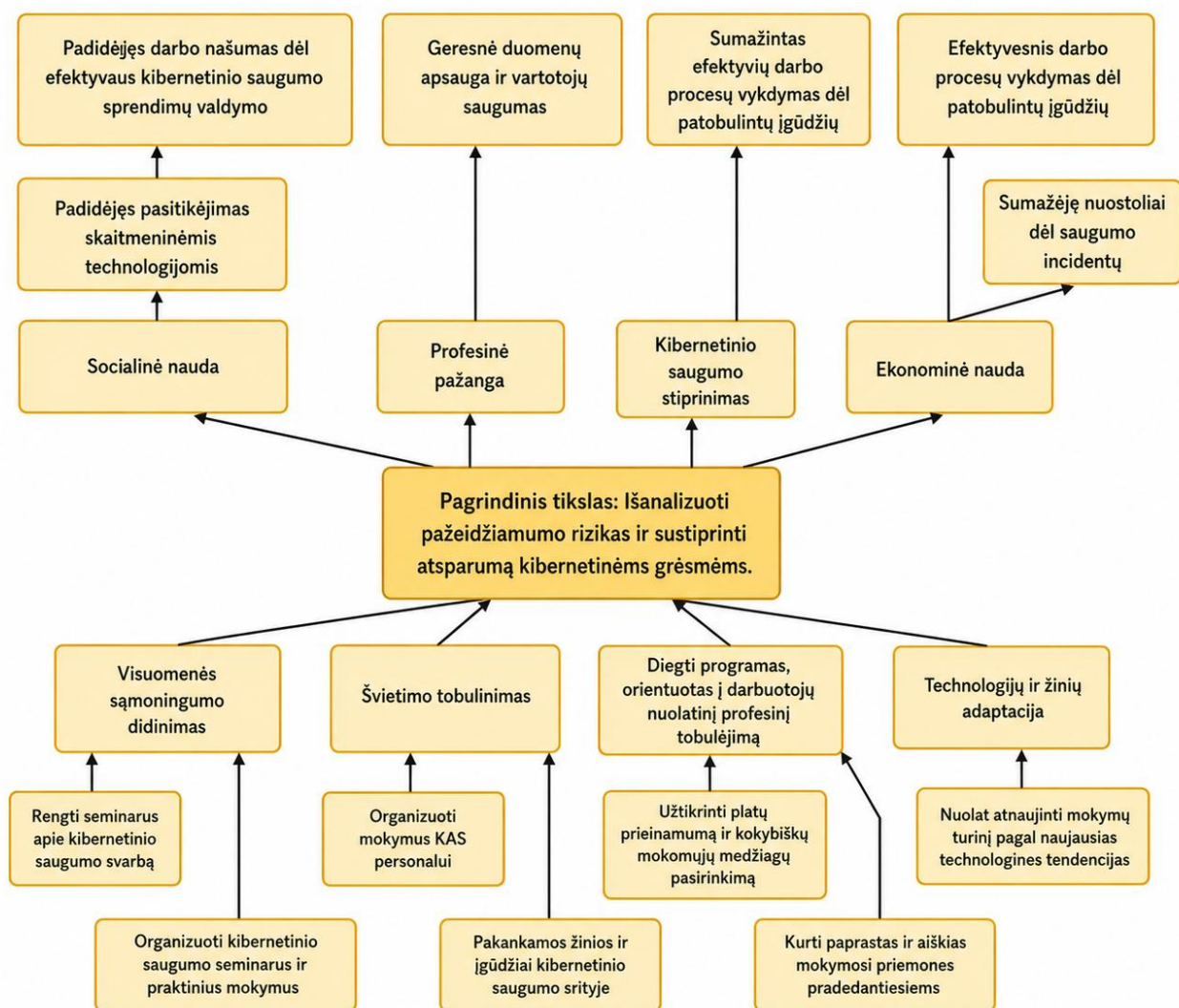
Be to, 65 % respondentų nenaudoja skirtingų slaptažodžių, o 30 % visiškai nenaudoja dviejų veiksmų autentifikacijos, kas rodo praktinių įgūdžių stoką. Pasmės, išryškintos problemų medyje, atspindi ir apklausoje rezultatuose – 50 % apklaustųjų paspaudė ant apgaulingų SMS nuorodų, o 35 % atidarė melagingus elektroninius laiškus, taip didindami kibernetinių incidentų riziką.

Problemų medis leidžia struktūruotai susieti nustatytas problemas su jų priežastimis ir pasekmėmis. Tai padeda aiškiai pagrįsti, kad pagrindinė problema yra ne technologijų trūkumas, o nepakankamas personalo pasirengimas ir motyvacija.

Tikslų medžio analizė. Tikslų medis iš problemų medžio išskiria siektinus rezultatus ir sprendimo kryptis. Pagrindinis tikslas – stiprinti KAS kibernetinį atsparumą, mažinant informacinių sistemų pažeidžiamumą ir didinant organizacijos atsparumą kibernetinėms grėsmėms.

Tikslų medžio šaknys transformuojamos į konkrečias strategijas ir veiksmus, skirtus problemoms spręsti: nuotolinio mokymo programų tobulinimą, pažangių technologijų (virtualiųjų laboratorijų, simuliacijų, platformų) integravimą bei personalo motyvacijos skatinimą.

Viršutinėje dalyje pateikiami siektini rezultatai – aukštesnis personalo žinių lygis, efektyvesnis informacinių sistemų naudojimas ir sumažėjusi kibernetinių incidentų rizika (žr. 2 pav.).



2 pav. Tikslų medis

Tikslų medis tiesiogiai siejasi su apklausos respondentų išvalgomis apie nuotolinio mokymo efektyvumą. 35 % respondentų nuotolinį mokymą vertina kaip labai efektyvų, tačiau 50 % nurodė motyvacijos stoką kaip pagrindinę kliūtį mokytis. Tai pagrindžia poreikį į mokymo programas integruoti pažangius sprendimus bei taikyti mišrius mokymo metodus.

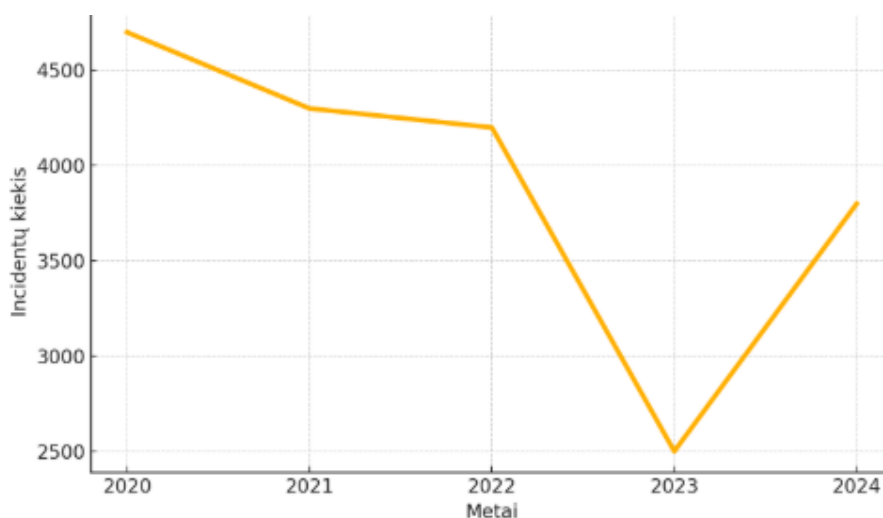
Apklausos rezultatai ir tikslų medžio analizė pabrėžia mokymo programų tobulinimo ir individualizuotų sprendimų būtinybę, siekiant užtikrinti aukštesnį kibernetinio saugumo lygį ir mažinti nacionalinio saugumo rizikas.

Tikslų medis leidžia transformuoti identifikuotas problemas į konkrečius sprendimus. Tai sudaro pagrindą sisteminiam kibernetinio saugumo ugdymo modelio kūrimui.

2.7. Nacionalinio kibernetinio saugumo ataskaitų analizė

Buvo išanalizuotos penkios NKSC ataskaitos, apimančios 2020–2024 metus. 2020 metais užfiksuotas didžiausias kibernetinių atakų skaičius (žr. 3 pav.). 2021 ir 2022 metais jų skaičius buvo panašus, o dauguma atakų buvo nukreiptos prieš strateginės svarbos sektorius.

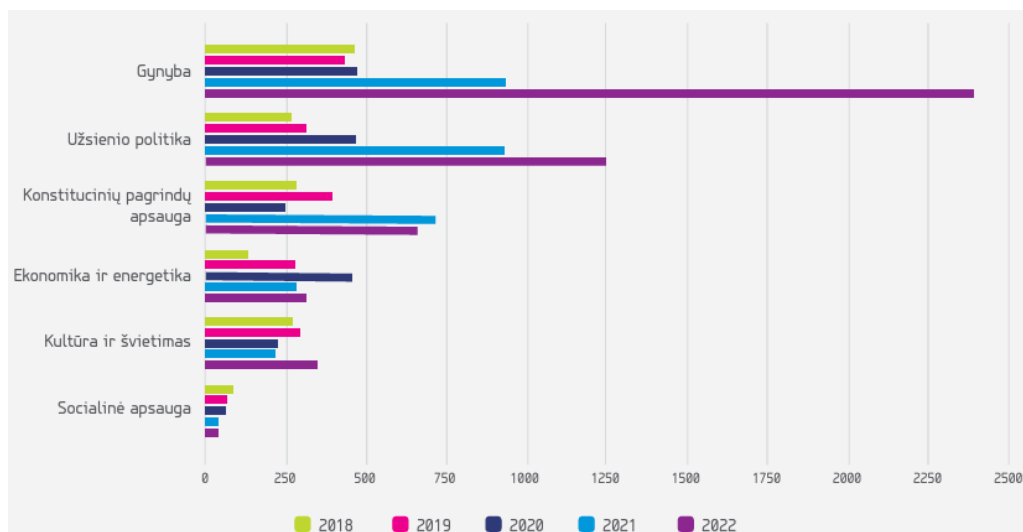
2023 metais incidentų kiekis ženkliai sumažėjo beveik perpus, tikėtina, dėl Rusijos karo prieš Ukrainą ir pasikeitusios kibernetinio saugumo situacijos. Visgi stabilizavusis situacijai, 2024 metais kibernetinių incidentų skaičius vėl ėmė augti. Nors bendras incidentų kiekis vis dar mažesnis nei 2020-aisiais, šiuolaikinės atakos tampa vis sudėtingesnės ir sunkiau aptinkamos.



3 pav. Kibernetinių incidentų statistika [9-13]

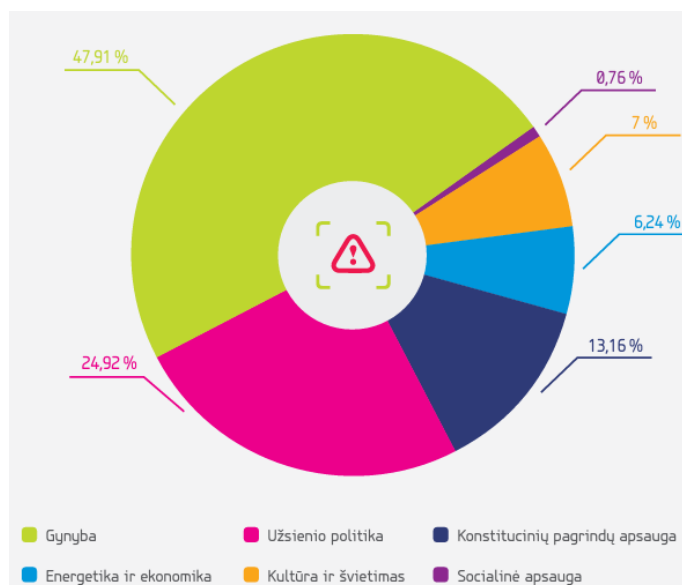
Ši analizė rodo, kad kibernetinių grėsmių dinamika yra glaudžiai susijusi su geopolitine situacija. Nepaisant bendro incidentų skaičiaus mažėjimo tam tikrais laikotarpiais, jų sudėtingumas didėja, todėl organizacijos turi būti pasirengusios ne tik dažnesnėms, bet ir labiau pažangioms atakoms.

Strateginių sričių pažeidžiamumas. Kibernetinių incidentų skaičius strateginėse srityse nuo 2018 iki 2022 metų buvo didžiausias gynybos sektoriuje (žr. 4 pav.). 2022 metais, prasidėjus karui tarp Ukrainos ir Rusijos, incidentų skaičius gynybos srityje padidėjo daugiau nei dvigubai. Tai rodo, kad gynybos sektorius išlieka vienu pagrindinių kibernetinių atakų taikinių.



4 pav. Informacinių incidentų skaičius strateginėse srityse [12]

2022 metų duomenys rodo (žr. 5 pav.), kad gynybos sektorius patyrė net 47,91 % visų incidentų. Antroje vietoje yra užsienio politikos sritis (24,92 %). Tai patvirtina, kad kibernetinės grėsmės apima tiek vidaus, tiek tarptautines valstybės veiklos sritis.

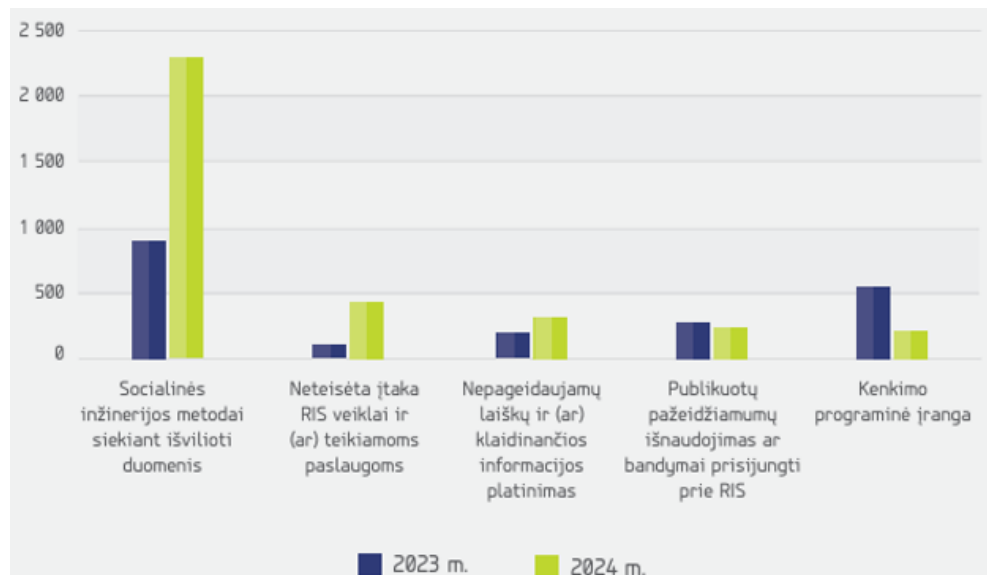


5 pav. Informacinių incidentų pasiskirstymas pagal strategines sritis 2022 metais [12]

Šie duomenys aiškiai parodo, kad KAS yra prioritetas taikinyse kibernetinėse atakose. Tai pagrindžia būtinybę skirti ypatingą dėmesį šio sektoriaus personalo kibernetinio saugumo kompetencijų stiprinimui.

Dažniausiai pasitaikančios incidentų grupės. Analizuojant 2023–2024 metų duomenis, nustatyta, kad dominuoja socialinės inžinerijos atakos, kuriomis siekiama išvilioti jautrią informaciją.

Antroje vietoje yra bandymai trikdyti informacinių sistemų veiklą, o kenkėjiškos programinės įrangos atvejų skaičius šiek tiek sumažėjo. Tai rodo, kad kibernetiniai veikėjai vis dažniau renkasi manipuluoti žmonėmis, o ne techninėmis priemonėmis.



6 pav. Incidentų grupės [12-13]

Analizuojant kibernetinio saugumo situaciją Lietuvoje 2023–2024 metais, svarbu išskirti pagrindines incidentų grupes, kurios dominuoja nacionalinėje kibernetinėje erdvėje. Aukščiau pateikiamoje diagramoje išskirtos penkios dažniausiai fiksuotos incidentų grupės (žr. 6 pav.). Kiekviena iš jų atspindi skirtingą grėsmės tipą ir reikalauja specifinių saugumo priemonių:

1. Socialinės inžinerijos metodai siekiant išvilioti duomenis, tai psichologinio manipuliavimo technikos, kuriomis siekiama apgauti žmones ir išvilioti jautrią informaciją (slaptažodžius, prisijungimus, vidinius dokumentus). Dažniausi pavyzdžiai:

- „Phishing“ el. laiškai (apsimetama, pvz., saugumo tarnyba ar kolega);
- „Smishing“ – tokie pat laiškai per SMS;
- „Vishing“ – melagingi skambučiai.

2. Neteisėta įtaka RIS veiklai ir (ar) teikiamoms paslaugoms, tai bandymai trikdyti, sulėtinti arba visiškai sustabdyti organizacijos informacinių sistemų veikimą. Tai gali būti:

- „DDoS“ atakos srautų užtvindymas);
- sistemų perrakinimas;
- loginiai trikdžiai, išjungiantys ar stabdantys svarbias funkcijas.

3. Nepageidaujamų laiškų ir klaidinančios informacijos platinimas, tai masinis el. laiškų siuntimas, siekiant suklaidinti, dezinformuoti ar išprovokuoti vartotojo veiksmą:

- reklaminis „spam“;
- politinė dezinformacija;
- melagingi pranešimai apie saugumą, infekcijas ir pan.

4. Paskelbtų pažeidžiamumų išnaudojimas ar bandymai prisijungti prie RIS, tai techninės atakos, kurios naudojami programinės įrangos silpnybėmis pvz., nepašalintos saugumo spragos:

- „Exploitai“ naudojamos žinomos spragos;
- „Brute-force“ bandymai prisijungti;
- automatizuoti įsilaužimo įrankiai.

5. Kenkimo programinė įranga, tai virusai, „trojanai“, „ransomware“, kurie įdiegiami į įrenginius per laiškus, USB, naršyklės spragas ir gali rinkti duomenis, blokuoti sistemas ar reikalauti išpirkos.

Ši klasifikacija rodo aiškią tendenciją – pagrindinis atakų taikinytampa žmogus, o ne technologijos. Tai dar kartą patvirtina, kad kibernetinio saugumo srityje svarbiausias veiksnys yra naudotojo kompetencija ir gebėjimas atpažinti grėsmes.

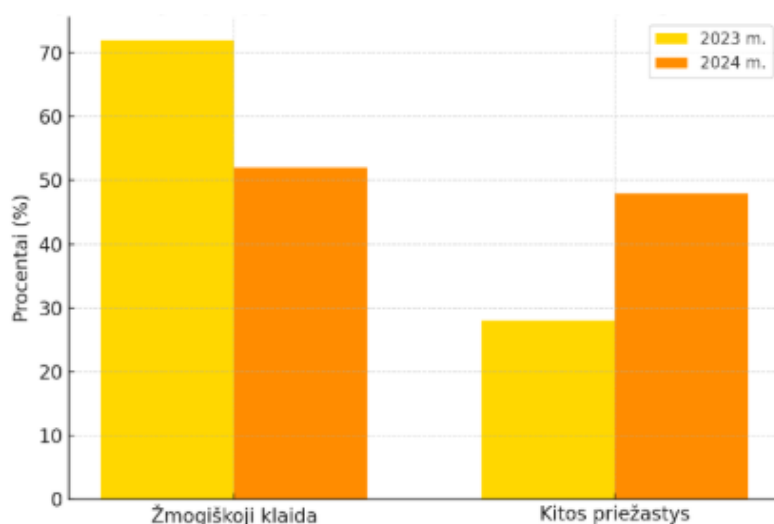
Asmens duomenų saugumo pažeidimų priežasčių analizė. Asmens duomenų saugumo pažeidimų (toliau - ADSP) analizė yra itin svarbi siekiant įvertinti, kokie veiksniai kelia didžiausią grėsmę duomenų apsaugai tiek viešajame, tiek gynybos sektoriuje. Krašto apsaugos srityje, kur tvarkoma itin jautri ir riboto naudojimo informacija, šių pažeidimų priežastys gali turėti reikšmingų pasekmių institucijų veiklai bei nacionaliniam saugumui.

Žemiau pateikta diagrama (žr. 7 pav.) parodo pagrindinių ADSP priežasčių pasiskirstymą 2023 ir 2024 metais, leidžiantį įvertinti jų reikšmingumo pokyčius.

2023 m. net 72 % visų duomenų saugumo pažeidimų sudarė žmogiškosios klaidos. Tai dažniausiai susiję su neatsargiu dokumentų siuntimu, netinkamu duomenų saugojimu ar netyčiniu jų nutekiniu. Likę 28 % buvo priskiriami kitoms priežastims, tokioms kaip techninės klaidos, organizaciniai trūkumai ar kibernetinės grėsmės.

2024 m. situacija pasikeitė – žmogiškųjų klaidų dalis sumažėjo iki 52 %, o kitų priežasčių dalis išaugo iki 48 %. Šie duomenys rodo aiškią tendenciją, kad nors žmogiškoji klaida išlieka pagrindine ADSP priežastimi, vis didesnę pavojų kelia ir kibernetiniai incidentai.

Krašto apsaugos sektoriuje tai ypač aktualu, nes priešiškos valstybės vis dažniau taikosi į asmens ir organizacinius duomenis, siekdamos sukelti žalą ar gauti slaptos informacijos. Tai pabrėžia būtinybę stiprinti personalo mokymus, tobulinti vidines procedūras bei didinti bendrą organizacijos kibernetinį atsparumą.



7 pav. Asmens duomenų saugumo pažeidimų priežastys [12-13]

Šie duomenys patvirtina, kad žmogiškasis faktorius išlieka pagrindine saugumo pažeidimų priežastimi, tačiau kibernetinės grėsmės tampa vis sudėtingesnės ir dažnesnės. Tai rodo būtinybę derinti technines saugumo priemones su nuolatiniu personalo mokymu ir elgsenos formavimu.

2.8. Skyriaus išvados

1. Atlikta analizė parodė, kad KAS jau taikomos įvairios kibernetinio saugumo ugdymo priemonės, apimančios teorinius mokymus ir praktines pratybas, tačiau šios priemonės nėra pakankamai integruotos bei orientuotos į nuoseklų ir individualizuotą mokymosi procesą. Taip pat nustatyta, kad esami mokymo sprendimai turi trūkumų, susijusių su praktinių įgūdžių stoka, ribotu personalizavimu ir motyvacijos trūkumu.
2. Atliktas tyrimas ir kibernetinio saugumo ataskaitų analizė parodė, kad KAS personalo kibernetinio saugumo lygis nėra pakankamas, o pagrindinės problemos yra susijusios su žmogiškuoju faktoriumi, žinių trūkumu ir netinkamais saugumo įpročiais. Nustatyta, kad kibernetinės grėsmės tampa vis sudėtingesnės ir vis dažniau orientuotos į naudotojo elgsenos išnaudojimą, todėl vien technologinių apsaugos priemonių nepakanka.
3. Analizė taip pat parodė, kad krašto apsaugos sektorius išlieka vienu pagrindinių kibernetinių atakų taikinių, todėl būtina skirti ypatingą dėmesį personalo kibernetinio saugumo kompetencijų ugdymui bei nuolatiniam jų tobulinimui.
4. Problemų ir tikslų medžių analizė bei tyrimo rezultatai leidžia teigti, kad efektyvus kibernetinio saugumo užtikrinimas turi būti grindžiamas kompleksiniu požiūriu, apimančiu pažangius technologinius sprendimus, nuoseklų ir personalizuotą mokymosi procesą bei praktika paremtą kibernetinio saugumo įgūdžių ugdymą.

3. Virtualiųjų mokymosi aplinkų analizė ir taikymo galimybės

Atsižvelgiant į 2 skyriaus tyrimo rezultatus, šiame skyriuje analizuojama virtualiosios mokymosi aplinkos (toliau – VMA) „Moodle“ ir „Open eClass“ ir jų taikymo galimybės kibernetinio saugumo mokymuose. Šios analizės tikslas – įvertinti, kaip esamos mokymosi valdymo sistemos gali būti pritaikytos efektyviam personalo kibernetinio saugumo įgūdžių ugdymui.

3.1. Moodle paskirtis ir pagrindinės savybės

„Moodle“ yra atvirojo kodo mokymosi valdymo sistema, plačiai naudojama aukštosiose mokyklose, profesinėse įstaigose ir organizacijose darbuotojų kvalifikacijai kelti. Ši sistema leidžia kurti struktūruotus kursus, valdyti mokymosi turinį, organizuoti vertinimą bei užtikrinti dalyvių tarpusavio komunikaciją.

„Moodle“ architektūra yra modulinė, todėl sistema gali būti lengvai pritaikoma skirtingiems mokymosi poreikiams. Dėstytojai ar kursų kūrėjai gali konfigūruoti aplinką pagal konkretaus kurso tikslus, integruoti papildinius ir plėsti sistemos funkcionalumą.

Pagrindinės „Moodle“ funkcijos:

- kurso kūrimo ir valdymo galimybės;
- mokymosi medžiagos pateikimas įvairiais formatais;
- testų, apklausų ir užduočių kūrimas;
- grįžtamojo ryšio teikimas;
- komunikacijos priemonės (forumai, pranešimai, pokalbiai);
- individualizuoto mokymosi taikymas (sąlyginis prieinamumas, grupės);
- mokymosi pažangos stebėseną ir analizę.

„Moodle“ funkcionalumas tiesiogiai atitinka 2 skyriuje identifikuotas problemas, susijusias su praktinių įgūdžių trūkumu ir mokymosi personalizavimo stoka. Sistemos galimybė integruoti interaktyvias užduotis ir stebėti pažangą sudaro prielaidas efektyvesniam kibernetinio saugumo ugdymui.

Dalyviai ir jų vaidmenys. „Moodle“ sistema palaiko kelias naudotojų grupes, kurių kiekvienas turi aiškiai apibrėžtas funkcijas, teises ir atsakomybes:

1. Studentas:

- prisijungia prie kurso;
- peržiūri mokymosi medžiagą;
- atlieka užduotis ir testus;
- dalyvauja diskusijose;
- stebi savo pažangą ir gauna grįžtamąjį ryšį.

2. Dėstytojas:

- kuria ir administruoja kursą;
- įkelia mokomąją medžiagą;
- rengia užduotis ir testus;
- vertina studentų darbus;
- stebi mokymosi procesą;

- palaiko ryšį su dalyviais.

3. Administratorius:

- valdo naudotojų paskyras ir teises;
- prižiūri sistemos veikimą;
- diegia papildinius ir atnaujinimus;
- užtikrina sistemos saugumą.

Aiškiai apibrėžti vaidmenys leidžia efektyviai organizuoti mokymosi procesą ir paskirstyti atsakomybes. Tai ypač svarbu KAS, kur reikalingas struktūruotas ir kontroliuojamas mokymosi procesas bei aiški atsakomybės hierarchija.

Mokymosi procesai ir sąveika. „Moodle“ platformoje mokymosi procesas organizuojamas temomis arba savaitėmis, kurios sudaro kurso struktūrą. Kiekvienoje temoje pateikiama mokomoji medžiaga, užduotys, testai bei diskusijų temos.

Kibernetinio saugumo mokymuose tai gali apimti:

- vaizdo paskaitas apie slaptažodžių saugumą ir socialinės inžinerijos grėsmes;
- testus žinioms patikrinti;
- diskusijas apie saugų elgesį internete;
- praktines užduotis, skirtas atpažinti kibernetines grėsmes.

Dėstytojas turi galimybę taikyti sąlyginį prieinamumą, leidžiantis atverti tam tikras veiklas tik įvykdžius ankstesnes užduotis. Tai skatina nuoseklų mokymąsi ir didina dalyvių motyvaciją.

Struktūrizuotas mokymosi procesas leidžia užtikrinti nuoseklų žinių įsisavinimą, o sąlyginio prieinamumo funkcija padeda kontroliuoti mokymosi eigą. Tai sprendžia vieną iš pagrindinių problemų – nesisteminę mokymąsi ir motyvacijos stoką.

Sistemos struktūra ir posistemiai. „Moodle“ sistemoje galima išskirti kelis pagrindinius posistemius, kurie užtikrina mokymosi proceso veikimą:

1. Administravimo posistemė:

- naudotojų valdymas;
- kursų administravimas;
- statistika ir ataskaitos;
- pažangos stebėjimas.

2. Turinio rengimo posistemė:

- kursų struktūros kūrimas;
- temų ir modulių valdymas;
- leidimų nustatymas.

3. Turinio pateikimo posistemė:

- įvairių formatų failų įkėlimas (tekstai, vaizdo medžiaga, PDF);
- išorinių nuorodų integravimas.

4. Vertinimo posistemė:

- testų kūrimas;

- užduočių vertinimas;
- grįžtamojo ryšio teikimas.

5. Komunikacijos posistemė:

- forumai;
- pranešimai;
- diskusijos.

Šių posistemių visuma leidžia užtikrinti visapusišką mokymosi procesą. „Moodle“ dėl savo lankstumo, modulinės struktūros ir plataus funkcionalumo yra tinkama platforma kibernetinio saugumo mokymams organizuoti bei tobulinti. Moodle posistemių struktūra rodo, kad sistema gali pilnai padengti visą mokymosi ciklą – nuo turinio pateikimo iki vertinimo ir komunikacijos. Tai leidžia kurti integruotą mokymosi aplinką, kuri atitinka šiuolaikinius kibernetinio saugumo ugdymo reikalavimus.

3.2. Moodle ir Open eClass virtualiųjų mokymosi aplinkų palyginamoji analizė

Siekiant įvertinti virtualiųjų mokymosi aplinkų tinkamumą kibernetinio saugumo mokymams, būtina ne tik analizuoti jų funkcionalumą, bet ir palyginti skirtingas sistemas tarpusavyje.

Šiame darbe buvo nagrinėjamos dvi virtualiosios mokymosi aplinkos – „Moodle“ ir „Open eClass“, todėl šiame skyriuje pateikiamas jų funkcionalumo palyginimas (žr. 2 lent.). Palyginimas atliktas remiantis praktiniu sistemų naudojimu bei kibernetinio saugumo kurso reikalavimais, kurie buvo suformuluoti remiantis ankstesnių skyrių analize.

Lyginamos abi sistemos pagal pagrindinius virtualiosios mokymosi aplinkos posistemius:

- administravimo;
- turinio pateikimo;
- testavimo ir vertinimo;
- komunikacijos;
- nefunkcinius reikalavimus.

Palyginimo tikslas – nustatyti, kuri sistema yra labiau tinkama kibernetinio saugumo mokymams organizuoti, atsižvelgiant į nustatytus personalo mokymosi poreikius ir kibernetinio saugumo ugdymo specifiką.

1 lentelė. „Moodle“ ir „Open eClass“ funkcionalumų palyginimas

FUNKCIONALUMAS	„MOODLE“	„OPEN ECLASS“	KOMENTARAS
Administravimo posistemė			
Naudotojų paskyrų valdymas	1	1	
Teisių konfigūravimas	1	1	
Kursų ataskaitos ir analizė	1	1	
Nustatyti lokalizuotą aplinką	1	0,5	„Open eClass“ sistemoje nėra galimybės lokalizuoti aplinką į lietuvių kalbą

Mokymosi turinio rengimo ir pateikimo posistemė			
Failų įkėlimas	1	1	
Įšorinių šaltinių integracija	1	0,75	„Moodle“ palaiko (H5P ir SCORM); „Open eClass“ – tik nuorodas.
Kurti ir pasiekti įvairias mokymosi veiklas.	1	1	
Sąlyginio turinio rodymas	1	1	
Testavimo ir vertinimo posistemė			
Kurti klausimų banką	1	1	
Testų tipų įvairovė	1	1	
Vertinimo galimybės	1	1	
Grįžtamasis ryšys studentui	1	1	
Komunikacijos posistemė			
Forumai ir žinutės	1	1	
Tiesioginis bendravimas	1	1	
Grupinis darbas	1	1	
Nefunkciniai reikalavimai			
Naudoji paprastumas	1	0,75	„Moodle“ patogesnė sistema.
Veikimo greitis	0,75	1	„Open eClass“ dirba greičiau, nes neturi tiek daug įskiepių kaip „Moodle“.
Pritaikymas lietuvių kalbai	1	0	„Open eClass“ neturi lietuvių kalbos.
Plėtojimo galimybės	1	0,75	Open eClass turi mažiau papildinių.
Pasiekiamumas	1	1	
Nemokama	1	1	
Atsarginės kopijos	1	1	
Saugumas	0,75	0,75	Visos sistemos turi spragų, reikia visuomet įdiegti naujausius įskiepius, norint užtikrinti saugumą.
Viso balų:	22,5	20,5	Daugiau balų surinko „Moodle“.

Pagal pateiktus vertinimo kriterijus ir surinktus balus nustatyta, kad „Moodle“ sistema surinko daugiau balų nei „Open eClass“ (atitinkamai 22,5 ir 20,5 balo). Nors skirtumas nėra didelis, jis rodo platesnes „Moodle“ galimybes ir lankstesnį pritaikymą sudėtingesniems mokymosi scenarijams.

„Moodle“ išsiskiria funkcionalumo įvairove – ypač testavimo, vertinimo, grįžtamojo ryšio ir sąlyginio turinio rodymo srityse. Taip pat sistema palaiko daugiau papildomų integracijų (pvz., H5P, SCORM, vaizdo konferencijas), kurios leidžia kurti interaktyvius ir praktika grįstus mokymus.

Tuo tarpu „Open eClass“ pasižymi paprastesniu naudojimu ir didesniu veikimo greičiu, todėl gali būti tinkamesnė paprastesniems kursams, orientuotiems į turinio pateikimą ir bazinę komunikaciją.

Vertinant nefunkcinius reikalavimus, abi sistemos turi savų privalumų: „Moodle“ suteikia daugiau galimybių, tačiau reikalauja didesnių administravimo resursų, o „Open eClass“ yra paprastesnė ir greitesnė, tačiau ribotesnio funkcionalumo.

Analizuojant gautus rezultatus taip pat svarbu atsižvelgti į 2 skyriaus tyrimo išvadas, kurios parodė, kad KAS personalui trūksta praktinių kibernetinio saugumo įgūdžių, o mokymuose dažnai stokojama interaktyvumo ir individualizavimo. Šiuo aspektu „Moodle“ sistema geriau atitinka iškeltus reikalavimus, nes leidžia kurti struktūruotus, interaktyvius ir pažangą sekančius mokymosi scenarijus.

Tačiau svarbu pažymėti, kad abi analizuotos platformos yra universalios paskirties mokymosi valdymo sistemos, skirtos plačiam mokymosi scenarijų spektrui. Jos nėra orientuotos į specifinius KAS poreikius, susijusius su realių kibernetinių grėsmių simuliacija, naudotojų elgsenos analize ar personalizuotais mokymosi scenarijais.

Dėl šios priežasties galima teigti, kad esamos virtualiosios mokymosi aplinkos ne visuomet leidžia pilnai realizuoti visus kibernetinio saugumo ugdymui keliamus reikalavimus. Tai pagrindžia poreikį kurti specializuotą virtualiąją mokymosi aplinką, orientuotą į konkrečius KAS personalo kibernetinio saugumo ugdymo tikslus.

3.3. Skyriaus išvados

1. Atlikta virtualiosios mokymosi aplinkos „Moodle“ analizė parodė, kad ši sistema pasižymi plačiu funkcionalumu, lankstumu ir suteikia galimybę organizuoti struktūruotą bei nuoseklų kibernetinio saugumo mokymosi procesą KAS personalui. Sistema leidžia integruoti teorinius ir praktinius mokymosi elementus, stebėti besimokančiųjų pažangą bei taikyti individualizuotą mokymąsi, atsižvelgiant į skirtingą personalo pasirengimo lygį.
2. Analizė parodė, kad „Moodle“ funkcionalumas gali padėti spręsti tyrimo metu identifikuotas problemas, susijusias su motyvacijos stoka, praktinių įgūdžių trūkumu ir nepakankamu mokymosi personalizavimu, todėl ši sistema gali būti laikoma tinkama platforma kibernetinio saugumo mokymams organizuoti.
3. Atlikus „Moodle“ ir „Open eClass“ virtualiųjų mokymosi aplinkų palyginamąją analizę nustatyta, kad abi sistemos atitinka pagrindinius virtualiosios mokymosi aplinkos reikalavimus, tačiau „Moodle“ pasižymi platesniu funkcionalumu ir lankstesniu pritaikymu sudėtingesniems mokymosi scenarijams.
4. Tačiau analizė taip pat parodė, kad esamos virtualiosios mokymosi aplinkos yra universalios paskirties ir ne visuomet pilnai atitinka specifinius KAS poreikius, susijusius su personalizuotu mokymu, realių kibernetinių grėsmių simuliacija bei naudotojų elgsenos analize.
5. Todėl galima teigti, kad nors „Moodle“ sistema yra tinkama bazinė platforma kibernetinio saugumo mokymams organizuoti, egzistuoja poreikis kurti specializuotus sprendimus, orientuotus į konkrečius KAS personalo kibernetinio saugumo ugdymo tikslus, kas pagrindžia šiame darbe siūlomos virtualiosios mokymosi aplinkos kūrimą.

4. Virtualios mokymosi aplinkos reikalavimų specifikacija ir modeliavimas

Remiantis 2 skyriaus tyrimo rezultatais ir 3 skyriuje analizuotomis „Moodle“ ir „Open eClass“ virtualiųjų mokymosi aplinkų galimybėmis, šiame skyriuje apibrėžiami pagrindiniai virtualiosios mokymosi aplinkos reikalavimai, skirti kibernetinio saugumo mokymams organizuoti. Šie reikalavimai formuojami atsižvelgiant į studentų, dėstytojų ir administratorių poreikius bei siekiant užtikrinti efektyvų, saugų ir patogų mokymosi procesą. Reikalavimai skirstomi į funkcinius, nusakančius, kokias funkcijas sistema turi atlikti, ir nefunkcinius, apibrėžiančius sistemos veikimo principus bei kokybinius aspektus.

Virtualioji mokymosi aplinka veikia pagal aiškiai apibrėžtus naudotojų vaidmenis – studento, dėstytojo ir administratoriaus. Kiekvienas naudotojas sistemoje atlieka skirtingas funkcijas, kurios realizuojamos per panaudojimo atvejus. Todėl šiame skyriuje taip pat pateikiamas virtualiosios mokymosi aplinkos panaudojimo atvejų modelis, atspindintis „Kibernetinio saugumo kurso“ vykdymą. Modeliavimas leidžia struktūruotai apibrėžti naudotojų sąveiką su sistema, išskirti pagrindines funkcijas bei geriau suprasti sistemos veikimo principus. Modelis sudarytas remiantis analizuotų virtualiųjų mokymosi aplinkų, tokių kaip „Moodle“ ir „Open eClass“, galimybėmis, 2 skyriaus tyrimo rezultatais ir šiame skyriuje apibrėžtais sistemos reikalavimais, siekiant užtikrinti, kad kuriama sistema atitiktų realius KAS personalo kibernetinio saugumo ugdymo poreikius.

4.1. Virtualios mokymosi aplinkos reikalavimai

Funkciniai reikalavimai. Nurodo, kokias konkrečias funkcijas turi atlikti VMA, kad būtų patenkinti visų naudotojų poreikiai. Sistemos funkcijos priklauso nuo vartotojo vaidmens, todėl išskiriamos trys pagrindinės naudotojų grupės: administratorius, dėstytojas ir studentas:

1. Administratorius:

- kurti ir valdyti naudotojų paskyras;
- priskirti vartotojus prie kursų;
- valdyti teisių lygius ir prieigos kontrolę;
- prižiūrėti sistemos veikimą;
- diegti papildinius ir modulius;
- užtikrinti sistemos saugumą.

2. Dėstytojas:

- kurti ir administruoti kursą;
- įkelti mokomąją medžiagą;
- kurti testus ir užduotis;
- vertinti studentų darbus;
- skelbti pranešimus;
- stebėti studentų aktyvumą ir pažangą;
- teikti grįžtamąjį ryšį.

3. Studentas:

- prisijungti prie sistemos;
- peržiūrėti kurso medžiagą;
- atlikti testus ir užduotis;

- peržiūrėti vertinimus;
- dalyvauti diskusijose;
- gauti dėstytojo grįžtamąjį ryšį.

Šie funkciniai reikalavimai užtikrina, kad kiekvienas sistemos naudotojas galėtų efektyviai atlikti savo veiklą ir dalyvauti mokymosi procese. Analizuojant 2 skyriaus tyrimo rezultatus matyti, kad personalui trūksta praktinių įgūdžių bei nuoseklaus mokymosi proceso, todėl tokios funkcijos kaip testų kūrimas, pažangos stebėjimas ir grįžtamojo ryšio teikimas yra būtinos siekiant efektyvaus kibernetinio saugumo ugdymo.

Nefunkciniai reikalavimai. Apibrėžia sistemos veikimo savybes, kurios lemia naudotojo patirtį, sistemos patikimumą ir saugumą.

Pagrindiniai nefunkciniai reikalavimai:

- Naudojimo paprastumas. Sistema turi būti aiški, intuityvi ir lengvai suprantama net technologiskai mažiau pažengusiems vartotojams.
- Kalbos pritaikymas. Sistema turi būti pritaikyta lietuvių kalbai, kad naudotojai galėtų lengvai suprasti pateikiamą informaciją.
- Pasiiekiamumas. Sistema turi būti prieinama visą parą (24/7) iš įvairių įrenginių, įskaitant kompiuterius, planšetes ir išmaniuosius telefonus.
- Saugumas. Prieiga prie duomenų turi būti apsaugota, naudojant autentifikavimo ir autorizacijos priemones.
- Veikimo greitis. Sistemos funkcijos turi veikti sklandžiai, be reikšmingų uždelimų.
- Plėtojimo galimybės. Sistema turi palaikyti papildinių diegimą ir funkcionalumo plėtrą.
- Duomenų saugojimas. Turi būti užtikrinta galimybė kurti atsargines kopijas ir prireikus atkurti duomenis.

Šie reikalavimai užtikrina, kad sistema būtų patikima, saugi ir patogi naudoti. Atsižvelgiant į nustatytą motyvacijos stoką ir nevienodą personalo pasirengimo lygį, nefunkciniai reikalavimai, tokie kaip naudojimo paprastumas, prieinamumas ir sistemos patikimumas, tampa itin svarbūs siekiant užtikrinti nuolatinį ir patogų mokymosi procesą.

Reikalavimai posistemiams. VMA susideda iš kelių pagrindinių posistemų, kuriems taip pat keliami specifiniai reikalavimai:

1. Turinio pateikimo posistemė:

- galimybė įkelti įvairių formatų failus (PDF, DOCX, vaizdo įrašus);
- galimybė naudoti išorines nuorodas (pvz., „YouTube“);
- galimybė riboti turinio prieinamumą pagal nustatytas sąlygas.

2. Testavimo ir vertinimo posistemė:

- įvairių tipų testų kūrimas (vieno pasirinkimo, kelių pasirinkimų, atviri klausimai);
- galimybė nustatyti laiko limitus ir bandymų skaičių;
- automatinis vertinimas ir rezultatų analizė;
- grįžtamojo ryšio teikimas.

3. Komunikacijos posistemė:

- forumai diskusijoms;
- galimybė siųsti žinutes individualiems naudotojams ar grupėms;
- pranešimų sistema svarbiai informacijai pateikti.

4. Valdymo posistemė:

- galimybė eksportuoti duomenis (pvz., pažymių suvestines);
- naudotojų grupių ir teisių valdymas;
- naudotojų veiklos stebėjimas ir registravimas (logai).

Šių posistemių reikalavimai užtikrina, kad VMA galėtų efektyviai palaikyti visą mokymosi procesą – nuo turinio pateikimo iki vertinimo ir komunikacijos.

Šių posistemių svarba tiesiogiai siejasi su 2 skyriaus rezultatais, kurie parodė, kad vien teorinių žinių nepakanka, todėl būtina integruoti testavimo, praktinių užduočių ir komunikacijos sprendimus, leidžiančius formuoti realius kibernetinio saugumo įgūdžius.

4.2. Sistemos funkcionalumo modeliavimas

Panaudojimo atvejų sąrašas. Panaudojimo atvejai apibrėžia, kokius veiksmus gali atlikti skirtingi sistemos naudotojai. Virtualiojoje mokymosi aplinkoje išskiriamos trys pagrindinės naudotojų grupės: administratorius, dėstytojas ir studentas:

1. Administratorius:

- kuria naudotojų paskyras;
- priskiria vartotojus prie kursų;
- valdo naudotojų teises;
- diegia papildinius ir modulius;
- prižiūri sistemos veikimą.

2. Dėstytojas:

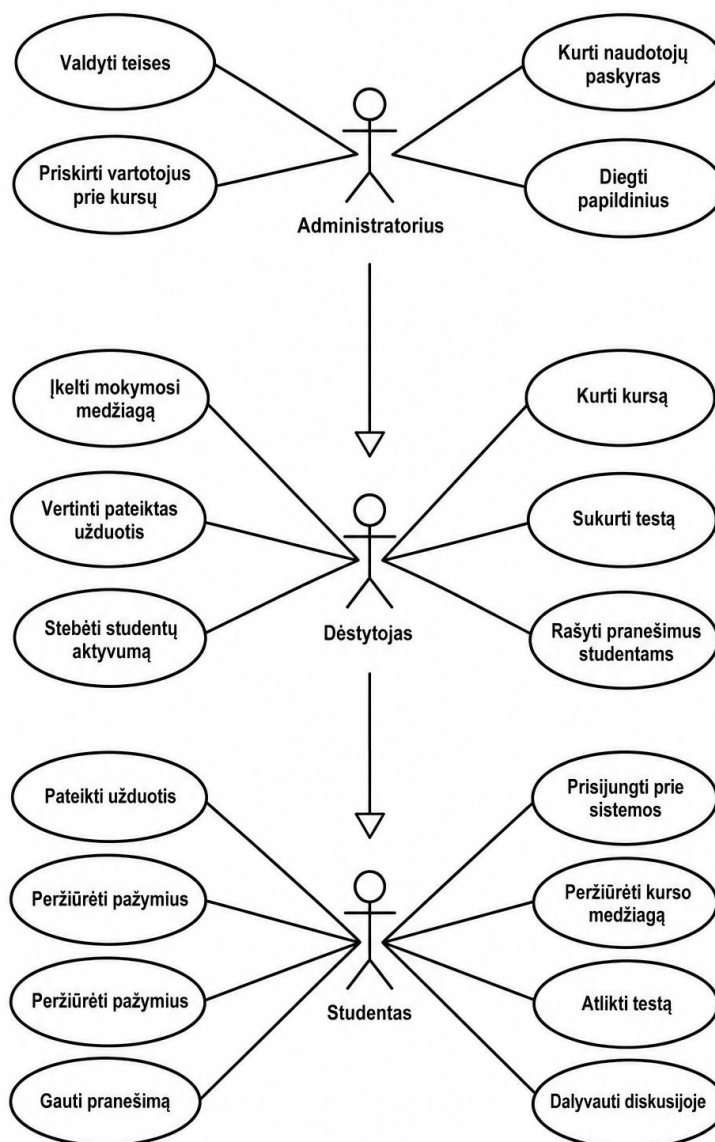
- kuria ir administruoja kursus;
- įkelia mokymosi medžiagą;
- kuria testus ir užduotis;
- vertina pateiktus darbus;
- skelbia pranešimus studentams;
- stebi studentų aktyvumą ir pažangą.

3. Studentas:

- prisijungia prie sistemos;
- peržiūri kurso medžiagą;
- atlieka testus;
- pateikia užduotis;
- peržiūri vertinimus;
- dalyvauja diskusijose;
- gauna pranešimus.

Šis panaudojimo atvejų sąrašas leidžia aiškiai identifikuoti sistemos funkcionalumą ir naudotojų vaidmenų pasiskirstymą. Atsižvelgiant į tyrimo rezultatus, ypatingas dėmesys skiriamas studento (besimokančiojo) veikloms, nes būtent šis naudotojas yra pagrindinis kibernetinio saugumo rizikų veiksnys ir kartu svarbiausias mokymosi proceso dalyvis.

UML panaudojimo atvejų diagrama. Yra vizualus modelis, naudojamas apibrėžti sistemos funkcionalumą iš naudotojo (aktoriaus) perspektyvos. Ji parodo, kokius veiksmus gali atlikti skirtingi sistemos naudotojai ir kaip šie veiksmai yra susiję su sistema. Diagrama padeda struktūruotai pavaizduoti pagrindines funkcijas, jų tarpusavio ryšius bei naudotojų sąveiką su sistema, todėl yra naudinga analizuojant ir projektuojant virtualiąją mokymosi aplinką.

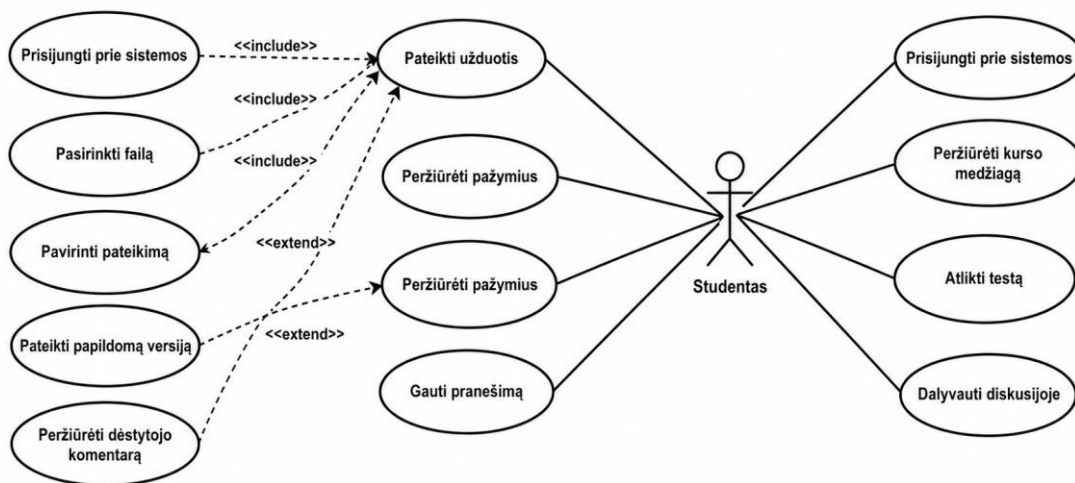


8 pav. Administratoriaus, dėstytojo ir studento panaudojimo atvejų diagrama

Pateiktame diagramoje (žr. 8 pav.) pavaizduota administratoriaus, dėstytojo ir studento panaudojimo atvejų diagrama. Joje atskleidžiama, kokius veiksmus gali atlikti kiekvienas naudotojas, administratorius valdo paskyras ir teises, dėstytojas kuria kursus ir vertina darbus, o studentas peržiūri medžiagą, atlieka užduotis ir dalyvauja komunikacijoje.

Taip pat matyti, kad studentas turi daugiausiai panaudojimo atvejų, nes jis yra pagrindinis mokymosi proceso dalyvis. Administratorius paveldi dėstytojo ir studento funkcijas, o dėstytojas – studento funkcijas. Toks funkcijų paveldimumas leidžia efektyviau valdyti naudotojų teises ir funkcionalumą sistemoje.

Toks modelis atitinka virtualiosios mokymosi aplinkos reikalavimus, apibrėžtus 4 skyriuje, ir užtikrina aiškų funkcionalumo paskirstymą tarp naudotojų, kas yra būtina siekiant efektyvaus mokymosi proceso organizavimo.



9 pav. Studento panaudojimo atvejų diagrama

Pateiktoje diagramoje (žr. 9 pav.) detaliau vaizduojama studento veikla. Joje išskiriamas panaudojimo atvejis „Pateikti užduotį“, kuris suskaidytas į sudėtinės dalis naudojant <<include>> ir <<extend>> ryšius.

Į diagramą įtraukti būtini veiksmai, tokie kaip prisijungimas prie sistemos, failo pasirinkimas ir pateikimo patvirtinimas (<<include>>), taip pat papildomi scenarijai, pavyzdžiui, galimybė pateikti užduotį pakartotinai ar peržiūrėti dėstytojo komentarą (<<extend>>). Šis modelis leidžia geriau suprasti, kaip veikia užduočių pateikimo procesas virtualiojoje mokymosi aplinkoje.

Panaudojimo atvejo specifikacija. Tai išsamus konkretaus sistemos veikimo scenarijaus aprašymas, pagrįstas naudotojo veiksmais ir sistemos atsaku. Ji padeda tiksliai apibrėžti, kaip turi veikti tam tikra funkcija, kokios sąlygos turi būti įvykdytos, kas ją inicijuoja, kaip ji vykdoma bei kaip sistema elgiasi esant tipinei ir alternatyviai eigai. Tokia specifikacija yra svarbi pritaikant ir tobulinant VMA, nes užtikrina, kad kiekvienas funkcionalumas būtų aprašytas ir suprantamas.

2 lentelė. Panaudojimo atvejo specifikacija

Panaudojimo atvejis	Pateikti užduotį
Tikslas	Studentas pateikia savo užduotį dėstytojui vertinimui
Dalyviai	Studentas
Ryšiai su kitais PA	Prisijungti prie sistemos, pasirinkti failą, patvirtinti pateikimą

Nefunkciniai reikalavimai	Naudojimo paprastumas, pasiekiamumas, aiškus pateikimo procesas
Išankstinė sąlyga	Studentas prisijungęs prie paskyros
Sužadinimo sąlyga	Paspaudžia mygtuką „Pateikti užduotį“
Įvykdymo sąlyga	Užduotis įkelta, pateikimas patvirtintas ir rodomas statusas „Pateikta“
Pagrindinis scenarijus	Studentas prisijungia prie sistemos, nueina į kursą ir pasirenka veiklą „Užduotis“. Paspaudžia „Pateikti užduotį“, įkelia failą arba įveda tekstą ir paspaudžia „Patvirtinti pateikimą“ ir sistema parodo apie sėkmingą pateikimą.
Alternatyvus scenarijus	Studentas prisijungia prie VMA, nueina į kursą ir pasirenka veiklą „Užduotis“. Paspaudžia „Pateikti užduotį“, užduoties nepateikia laiku ir sistema parodo apie vėluojamą užduoties pateikimą.

Specifikacijoje (žr. 1 lent.) pateikiamas panaudojimo atvejis „Pateikti užduotį“, kurio tikslas – sudaryti sąlygas studentui pateikti savo darbą dėstytojui vertinimui. Veiklos dalyvis yra studentas, kuris, naudodamasis virtualiąja mokymosi aplinka, inicijuoja veiksmų seką: prisijungia prie sistemos, pasirenka kursą, pereina į veiklą „Užduotis“ ir įkelia savo darbą.

Šis panaudojimo atvejis yra susijęs su kitais panaudojimo atvejais, tokiais kaip prisijungimas prie sistemos, failo pasirinkimas ir pateikimo patvirtinimas. Tai reiškia, kad nagrinėjama funkcija priklauso nuo kitų sistemos funkcijų ir papildo bendrą mokymosi proceso eigą.

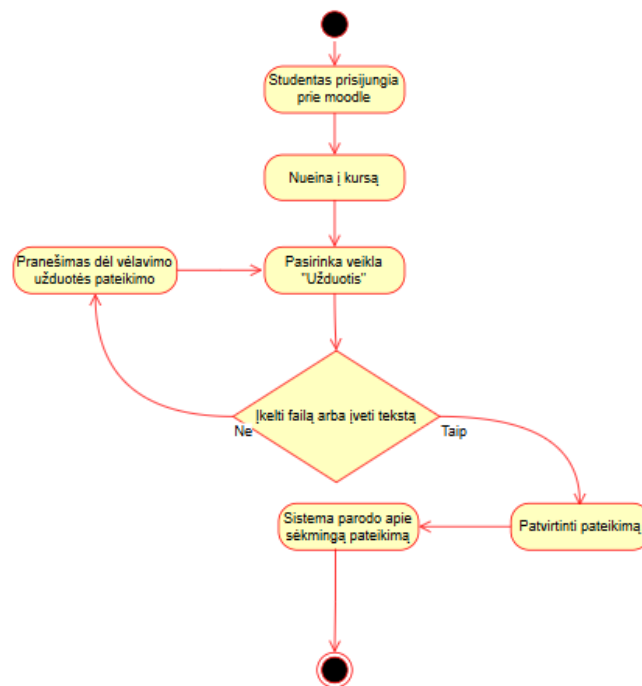
Specifikacijoje taip pat apibrėžiamos išankstinės ir sužadinimo sąlygos: išankstinė sąlyga – studentas turi būti prisijungęs prie sistemos, o sužadinimo sąlyga – paspaudžiamas mygtukas „Pateikti užduotį“. Pagrindinis scenarijus aprašo sėkmingą užduoties pateikimą, kai darbas įkeliamas ir sistema patvirtina veiksmą. Alternatyvus scenarijus apibrėžia situaciją, kai užduotis nepateikiama laiku arba neįkeliamas, ir sistema apie tai informuoja naudotoją.

Tokiu būdu panaudojimo atvejo specifikacija leidžia detaliai apibrėžti užduočių pateikimo funkcijos veikimą bei užtikrina jos aiškumą, nuoseklumą ir galimybę ją testuoti. Šis panaudojimo atvejis taip pat tiesiogiai siejasi su kibernetinio saugumo įgūdžių ugdymu, nes praktinių užduočių pateikimas ir vertinimas leidžia formuoti realius naudotojų gebėjimus, o ne vien teorines žinias.

Veiklos diagrama. Yra UML modelio tipas, skirtas vaizduoti veiksmų seką sistemoje ir sprendimo taškus, kurie lemia tolesnę proceso eigą. Ji leidžia aiškiai matyti tiek pagrindinį scenarijų, tiek galimas alternatyvias veiksmų kryptis.

Pateiktoje veiklos diagramoje (žr. 10 pav.) vaizduojamas panaudojimo atvejis „Pateikti užduotį“, remiantis 1 lentelėje pateikta specifikacija. Procesas prasideda studento prisijungimu prie sistemos ir perėjimu į pasirinktą kursą. Tuomet studentas pasirenka veiklą „Užduotis“, o sistema patikrina, ar yra įkeltas failas arba įvestas tekstas.

Jeigu užduotis pateikta, studentas ją patvirtina ir procesas baigiamas sėkmingai. Jeigu užduotis nepateikta, sistema pateikia pranešimą apie klaidą arba vėlavimą, ir procesas nutraukiamas. Tokiu būdu diagrama aiškiai atskleidžia tiek pagrindinę, tiek alternatyvią proceso eigą.



10 pav. Pagrindinio ir alterantvyaus scenarijaus veiklos diagrama

Tokia proceso struktūra leidžia užtikrinti nuoseklų mokymosi veiklų vykdymą ir aiškiai apibrėžia naudotojo sąveiką su sistema, kas yra svarbu siekiant mažinti naudotojų klaidų tikimybę kibernetinio saugumo kontekste.

4.3. Skyriaus išvados

1. Atlikta analizė parodė, kad efektyvi kibernetinio saugumo mokymams skirta virtualioji mokymosi aplinka turi atitikti tiek funkcinius, tiek nefunkcinius reikalavimus. Funkciniai reikalavimai užtikrina mokymosi proceso organizavimą – nuo mokomosios medžiagos pateikimo iki žinių vertinimo ir grįžtamojo ryšio teikimo, o nefunkciniai reikalavimai lemia sistemos patikimumą, saugumą, prieinamumą ir naudojimo patogumą.
2. Nustatyta, kad virtualioji mokymosi aplinka turi būti lanksti ir pritaikoma skirtingų naudotojų grupių – administratorių, dėstytojų ir studentų – poreikiams. Taip pat išanalizavus sistemos posistemius nustatyta, kad turinio pateikimo, testavimo ir vertinimo, komunikacijos bei valdymo funkcijos yra esminės siekiant užtikrinti kokybišką, struktūruotą ir į vartotoją orientuotą mokymosi procesą.
3. Atliktas panaudojimo atvejų modeliavimas parodė, kad UML modeliai leidžia aiškiai ir struktūruotai apibrėžti sistemos funkcionalumą, naudotojų sąveiką bei praktinį funkcinių reikalavimų realizavimą. Detalesnis modeliavimas, naudojant specifikacijas ir veiklos diagramas, padeda tiksliau apibrėžti sistemos procesus bei užtikrinti jų nuoseklumą ir pritaikomumą realiems mokymosi scenarijams.
4. Apibendrinant galima teigti, kad tokios virtualiosios mokymosi aplinkos kaip „Moodle“ atitinka pagrindinius iškeltus reikalavimus ir gali būti sėkmingai taikomos KAS personalo kibernetinio saugumo įgūdžių ugdymui, o panaudojimo atvejų modeliavimas sudaro pagrindą efektyviam sistemos projektavimui bei žmogiškojo faktoriaus keliamų rizikų mažinimui.

5. Kibernetinio saugumo ugdymo poreikio pagrindimas remiantis KAS duomenų analize

Skirtingai nei ankstesniuose skyriuose nagrinėta nacionalinio lygmens kibernetinio saugumo statistika, šiame skyriuje analizuojami konkretūs KAS duomenys. Ši analizė leidžia įvertinti realias kibernetines grėsmes organizacijos viduje ir pagrįsti kibernetinio saugumo įgūdžių ugdymo poreikį.

Šiuolaikinėje karinėje struktūroje darbas neįsivaizduojamas be informacinių technologijų, nes kasdienės tarnybinės užduotys ir administraciniai procesai vykdomi naudojant įvairias informacines sistemas. Remiantis moksliniais tyrimais ir praktine patirtimi, dažniausiai silpniausia kibernetinio saugumo grandis yra naudotojas.

Darbuotojų kibernetinio saugumo lygis organizacijoje nėra vienodas, nes ne visi turi pakankamus įgūdžius dirbti su informacinėmis technologijomis. Todėl svarbu analizuoti realius incidentus ir saugumo duomenis, kurie leidžia identifikuoti dažniausiai pasitaikančias klaidas ir žinių spragas.

Nuotolinio mokymosi aplinka suteikia galimybę ne tik perteikti teorines žinias, bet ir stebėti besimokančiųjų pažangą, analizuoti jų daromas klaidas bei pritaikyti mokymo turinį pagal realius poreikius. Tai leidžia efektyviau planuoti kibernetinio saugumo ugdymo procesą ir didinti organizacijos atsparumą grėsmėms.

Ši analizė yra svarbi ne tik esamos situacijos įvertinimui, bet ir tolimesniam sprendimų pagrindimui, nes leidžia nustatyti, kokio pobūdžio kibernetinio saugumo įgūdžiai yra svarbiausi KAS personalui. Gauti rezultatai sudaro pagrindą kurti tikslingas, realiomis grėsmėmis paremtas mokymo priemones.

5.1. Tyrimo metodas ir duomenų šaltiniai

Šiame darbe pasirinkta kibernetinės gynybos įvykių suvestinių analizė kaip pagrindinis poreikių nustatymo metodas [14]. Analizuojami KAS kibernetinio saugumo ir elektroninio pašto apsaugos duomenys, kuriuose pateikiama informacija apie registruotus incidentus ir saugumo įvykius. Tyrimo metu surinkti kibernetinės valdybos incidentų ir el. pašto apsaugos duomenys yra prieinami tik organizacijos atsakingiems specialistams, todėl tikslūs kiekybiniai rodikliai viešai nėra pateikiami. Siekiant užtikrinti informacijos konfidencialumą bei kartu išlaikyti tyrimo analizės objektyvumą, duomenys darbe pateikiami procentinėmis išraiškomis. Toks duomenų pateikimo būdas leidžia atlikti patikimą statistinę analizę, įvertinti pagrindines grėsmių tendencijas bei nustatyti sritis, kuriose išlieka didžiausi kibernetinio saugumo pavojai.

Taikomas kiekybinis tyrimo metodas, leidžiantis analizuoti statistinius duomenis ir nustatyti bendras kibernetinių grėsmių tendencijas visos organizacijos mastu. Šis metodas suteikia galimybę objektyviai įvertinti kibernetinio saugumo situaciją ir pagrįsti ugdymo poreikį. Ataskaitų analizė leidžia identifikuoti dažniausiai pasitaikančius incidentų tipus ir rizikos sritis, kurios dažnai yra susijusios su naudotojų žinių trūkumu. Vien tik techninių saugumo priemonių nepakanka, todėl būtina sisteminga mokymosi parama ir personalo kompetencijų ugdymas.

Tyrimo ribotumai ir duomenų patikimumas. Atliekant tyrimą svarbu įvertinti jo ribotumus. Analizuojami duomenys yra apibendrinti visos KAS mastu, todėl neleidžia detaliam išskirti atskirų padalinių, informacinių sistemų ar pareigybių specifinių problemų. Dėl šios priežasties gauti rezultatai atspindi bendras kibernetinių grėsmių tendencijas organizacijoje, tačiau neleidžia tiksliai identifikuoti individualių naudotojų elgsenos ar konkrečių incidentų atsiradimo aplinkybių.

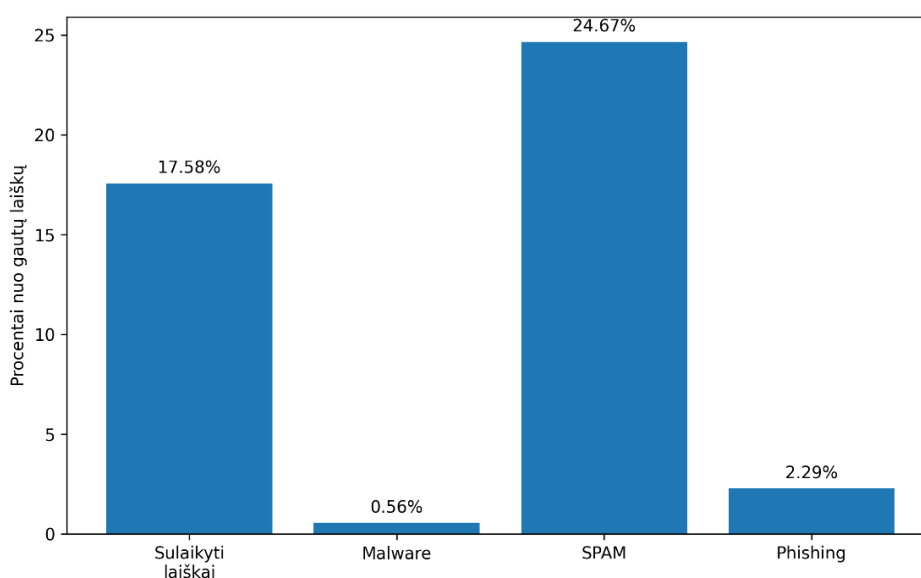
Tyrimo ribotumą taip pat lemia informacijos konfidencialumo reikalavimai. Dalis tiriamų duomenų yra riboto naudojimo, todėl darbe nepateikiami tikslūs kiekybiniai rodikliai, konkretūs techniniai parametrai ar organizacijos naudojamų apsaugos priemonių detalės. Siekiant išlaikyti tyrimo objektyvumą ir kartu užtikrinti duomenų apsaugą, statistiniai duomenys pateikiami procentinėmis išraiškomis bei apibendrinta forma.

Kitas ribotumas susijęs su incidentų samprata. Fiksuojami saugumo įvykiai nebūtinai reiškia realius saugumo pažeidimus ar sėkmingas kibernetines atakas, kadangi didelė jų dalis yra automatiškai aptinkama ir blokuojama naudojamomis saugumo priemonėmis. Todėl registruotų įvykių skaičius daugiau parodo bendrą grėsmių aktyvumą ir organizacijos susidūrimą su potencialiomis rizikomis, o ne vien tik realiai įvykusius saugumo pažeidimus.

Nepaisant išvardytų ribotumų, tyrime naudoti duomenys laikytini patikimais, nes jie gaunami iš oficialių KAS kibernetinio saugumo stebėsenos ir incidentų registravimo šaltinių, kuriuose taikomi vieningi duomenų rinkimo, apdorojimo ir analizės principai. Tai leidžia objektyviai vertinti kibernetinių grėsmių pobūdį, jų pasiskirstymą bei tendencijas, taip pat pagrįsti poreikį stiprinti personalo kibernetinio saugumo kompetencijas nuotolinio mokymosi priemonėmis.

5.2. Elektroninio pašto apsaugos duomenų analizė

Apibendrinus KAS elektroninio pašto apsaugos duomenis nustatyta, kad per analizuojamą laikotarpį buvo gautas bendras elektroninių laiškų kiekis, kuris šiame darbe laikomas 100 %. Analizė rodo, kad reikšminga dalis laiškų buvo susijusi su potencialiomis kibernetinėmis grėsmėmis. Automatinės saugumo priemonės sulaikė didelį kiekį įtartinų laiškų, tarp jų – kenkimo programinės įrangos (angl. malware), nepageidaujamų laiškų (angl. spam) ir apgaulingų laiškų (angl. phishing) atvejus (žr. 11 pav.). Tai rodo, kad KAS personalas nuolat susiduria su įvairiomis kibernetinėmis grėsmėmis, nukreiptomis tiek į naudotojus, tiek į informacines sistemas.



11 pav. El. pašto apsaugos statistika

Atlikus detalesnę duomenų analizę matyti, kad sulaikytų laiškų kiekis sudaro reikšmingą viso gaunamų laiškų srauto dalį. Tai patvirtina, kad kibernetinės grėsmės yra nuolatinė organizacijos

veiklos dalis, o personalas reguliariai susiduria su potencialiai pavojinga informacija. Taip pat nustatyta, kad didžiausią dalį sudaro „spam“ tipo bei kiti sulaikyti laišakai, tiesiogiai orientuoti į naudotoją. Tai reiškia, kad net ir efektyviai veikiant techninėms apsaugos priemonėms, galutinis saugumo užtikrinimas dažnai priklauso nuo naudotojo veiksmų, budrumo ir gebėjimo atpažinti grėsmes.

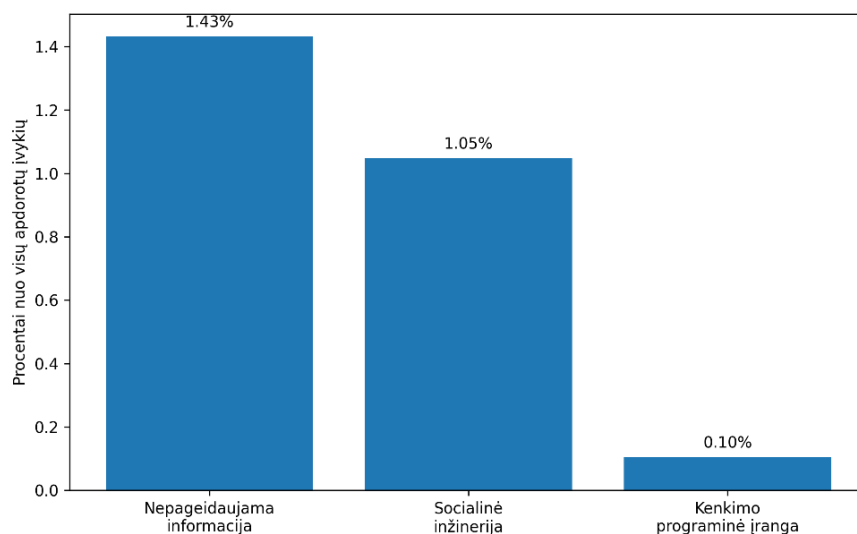
Gauti rezultatai patvirtina, kad vien techninių apsaugos priemonių nepakanka, todėl būtina stiprinti naudotojų kibernetinio saugumo kompetencijas bei ugdyti gebėjimą atpažinti socialinės inžinerijos ir kitų kibernetinių atakų požymius.

5.3. Kibernetinių incidentų analizė

Analizuojant kibernetinių incidentų statistiką nustatyta, kad per nagrinėjamą laikotarpį buvo apdorotas bendras saugumo įvykių skaičius, kuris šiame darbe laikomas 100 %. Analizuoti saugumo įvykiai apima atvejus, kurie buvo identifikuoti kaip potencialiai keliantys grėsmę informacinių sistemų saugumui arba nukrypstantys nuo įprasto naudotojų ir sistemų veikimo modelio.

Incidentai suskirstyti į tris pagrindines kategorijas:

- nepageidaujamų laiškų, klaidinančios ar žalingos informacijos platinimas;
- socialinės inžinerijos atakos, siekiant išvilioti prisijungimo duomenis;
- kenkimo programinė įranga, aptinkama ir blokuojama saugumo priemonėmis.



12 pav. Kibernetinių incidentų statistika

Diagrama rodo (žr. 12 pav.), kad didžioji dalis incidentų yra susiję su nepageidaujama informacija ir socialinės inžinerijos atakomis. Tai patvirtina, kad pagrindiniu kibernetinių grėsmių taikiniu išlieka žmogus – informacinių sistemų naudotojas. Nors kenkimo programinės įrangos atvejų skaičius yra mažesnis, tai nebūtinai reiškia mažesnę grėsmę, nes tokio pobūdžio atakos dažnai yra sudėtingesnės, sunkiau aptinkamos ir gali sukelti didesnę žalą.

Dominuojantis socialinės inžinerijos atakų pobūdis rodo aiškią tendenciją – kibernetiniai veikėjai vis dažniau siekia paveikti žmogų, o ne tiesiogiai atakuoti technologines sistemas. Tai leidžia daryti išvadą, kad efektyvus kibernetinio saugumo užtikrinimas vis labiau priklauso nuo naudotojų gebėjimo atpažinti grėsmes bei tinkamai reaguoti į galimus incidentus.

Gauti rezultatai pagrindžia poreikį stiprinti personalo kibernetinio saugumo kompetencijas bei taikyti nuotolinio mokymosi sprendimus, orientuotus į praktinių įgūdžių ugdymą ir socialinės inžinerijos grėsmių atpažinimą

5.4. Kibernetinio saugumo įgūdžių ugdymo poreikių identifikavimas

Apibendrinus elektroninio pašto apsaugos ir incidentų analizės rezultatus, galima identifikuoti pagrindines kibernetinio saugumo ugdymo poreikio kryptis.

Didelė apgaulingų ir socialinės inžinerijos pobūdžio laiškų dalis rodo, kad naudotojai nuolat susiduria su bandymais paveikti jų sprendimus ir išvilioti jautrią informaciją. Tai rodo būtinybę stiprinti darbuotojų gebėjimus atpažinti kibernetines grėsmes.

Ypač svarbu ugdyti praktinius įgūdžius:

- atpažinti phishing tipo laiškus;
- vertinti įtartinus nuorodas;
- reaguoti į galimus kibernetinius incidentus;
- laikytis saugaus elgesio principų informacinėje aplinkoje.

Nustatyta, kad net ir esant pažangioms techninėms apsaugos priemonėms, žmogiškasis faktorius išlieka viena pagrindinių rizikos priežasčių. Todėl kibernetinio saugumo ugdymas turi būti orientuotas ne tik į teorines žinias, bet ir į praktinių įgūdžių formavimą.

Atsižvelgiant į nustatytus poreikius, galima teigti, kad efektyvus kibernetinio saugumo ugdymas turi būti orientuotas į praktinių situacijų analizę, interaktyvų mokymąsi ir nuolatinį grįžtamąjį ryšį.

Tokie reikalavimai sudaro prielaidas kurti specializuotą virtualiąją mokymosi aplinką, kuri būtų pritaikyta realioms KAS grėsmėms ir leistų efektyviau ugdyti personalo kibernetinio saugumo įgūdžius.

5.5. Skyriaus išvados

1. Apibendrinus KAS kibernetinio saugumo duomenų analizę nustatyta, kad organizacijos personalas nuolat susiduria su įvairiomis kibernetinėmis grėsmėmis, ypač susijusiomis su socialine inžinerija ir apgaulingais elektroniniais laiškais. Didelis automatiškai sulaikomų laiškų kiekis rodo grėsmių intensyvumą, tačiau tuo pačiu pabrėžia ir žmogiškojo faktoriaus svarbą.
2. Atlikta analizė parodė, kad pagrindinės kibernetinio saugumo problemos yra susijusios su naudotojų žinių ir praktinių įgūdžių trūkumu. Tai pagrindžia būtinybę sistemingai ugdyti personalo kibernetinio saugumo kompetencijas.
3. Galima teigti, kad NM, paremtas realių incidentų analize ir praktinių įgūdžių ugdymu, yra efektyvi priemonė didinti organizacijos atsparumą kibernetinėms grėsmėms. Be to, atlikta analizė parodė, kad esamos universalios mokymosi platformos ne visuomet leidžia pilnai atlikti specifinius organizacijos poreikius, todėl tikslinga kurti specializuotus sprendimus, orientuotus į realių kibernetinių grėsmių analizę ir praktinių įgūdžių ugdymą.

6. Nuotolinio kibernetinio saugumo įgūdžių ugdymo paramos modelis

Kibernetinis saugumas KAS negali būti užtikrinamas vien tik techninėmis saugumo priemonėmis, todėl svarbus vaidmuo tenka ir personalo mokymui bei supažindinimui su kibernetinio saugumo ir kibernetinės higienos principais. Efektyvi mokymosi parama apima instruktorių, ryšių ir informacinių sistemų specialistų, saugumo įgaliotinio bei dalinio vadovybės teikiamą palaikymą kibernetinio saugumo ugdymo procese.

Nuotolinis kibernetinio saugumo ugdymas reikalauja ne tik tinkamo mokymosi turinio, bet ir aiškiai apibrėžto paramos modelio, kuris apimtų dalyvių vaidmenis, bendradarbiavimo principus, techninį palaikymą, grįžtamąjį ryšį ir mokymosi proceso stebėseną. Toks modelis leidžia užtikrinti nuoseklų, į besimokantįjį orientuotą ir realiomis grėsmėmis pagrįstą ugdymo procesą.

Atliktoje KAS duomenų analizėje nustatyta, kad pagrindinės kibernetinio saugumo problemos yra susijusios su žmogiškuoju faktoriumi, praktinių įgūdžių trūkumu ir nepakankamu mokymosi nuoseklumu. Todėl paramos modelis turi būti orientuotas ne tik į turinio pateikimą, bet ir į nuolatinį besimokančiojo palaikymą, pažangos stebėseną bei praktinių gebėjimų stiprinimą.

6.1. Nuotolinio mokymosi dalyvių vaidmenys, atsakomybės ir bendradarbiavimas

Aiškiai apibrėžti nuotolinio mokymosi dalyvių vaidmenys ir jų tarpusavio sąveika yra būtina veiksmingos mokymosi aplinkos sąlyga. Kiekvienas mokymosi proceso dalyvis atlieka svarbų vaidmenį užtikrinant mokymosi proceso tęstinumą, kokybę ir praktinį įgytų žinių pritaikymą tarnybinėje veikloje.

Besimokantysis KAS personalas yra pagrindinis mokymosi proceso dalyvis, atsakingas už aktyvų dalyvavimą nuotolinio mokymosi veiklose, mokymosi medžiagos įsisavinimą, savarankišką žinių gilinimą ir savo mokymosi pažangos stebėjimą. Besimokantieji turi laikytis kibernetinės higienos principų, taikyti įgytas žinias kasdienėje tarnybinėje veikloje ir laiku reaguoti į galimas kibernetines grėsmes informacinėje aplinkoje.

Instruktorius vaidmenį nuotolinio kibernetinio saugumo ugdymo procese gali atlikti RIS specialistai bei saugumo įgaliotinis, turintys reikiamą kompetenciją ir praktinę patirtį. Šie asmenys yra atsakingi už mokymosi turinio rengimą, veiklų planavimą, mokymosi proceso moderavimą ir nuolatinio grįžtamojo ryšio teikimą. Remdamiesi besimokančiųjų rezultatais, testų duomenimis bei kibernetinių incidentų ir elektroninio pašto apsaugos statistika, jie gali identifikuoti problemines sritis ir atitinkamai koreguoti mokymo turinį, akcentuodami aktualiausias kibernetines rizikas, tokias kaip socialinės inžinerijos atakos, apgaulingi elektroniniai laišakai ar kenkimo programinė įranga.

Svarbią paramą teikia ir RIS specialistai bei saugumo įgaliotinis, kurie yra atsakingi už techninių mokymosi priemonių veikimą, nuotolinio mokymosi aplinkos prieinamumą ir saugumą. Jie užtikrina, kad nuotolinio mokymosi platformos veiktų stabiliai, o saugumo sprendimai būtų tinkamai konfigūruoti ir nuolat atnaujinami.

Dalinio vadovybė atlieka svarbų organizacinį ir motyvacinį vaidmenį. Ji sudaro sąlygas personalui dalyvauti nuotoliniame mokyme, nustato mokymosi prioritetus, atsakomybes ir reikalavimus, skiria mokymuisi reikalingą laiką bei užtikrina mokymosi integravimą į kasdienę tarnybinę veiklą. Vadovybės palaikymas yra esminis veiksnys formuojant kibernetinio saugumo kultūrą padalinyje ir skatinant personalo įsitraukimą į ugdymo procesą.

Nuotolinio mokymosi dalyvių bendradarbiavimas grindžiamas aiškiais komunikacijos kanalais ir veiksmingais grįžtamojo ryšio mechanizmais. Mokymosi procese naudojamos nuotolinio mokymosi platformos, elektroninis paštas, vaizdo konferencijos ir diskusijų forumai, kurie leidžia operatyviai spręsti iškilusias problemas, dalytis patirtimi ir užtikrinti nuoseklų bei efektyvų kibernetinio saugumo ugdymo procesą.

Toks vaidmenų ir atsakomybių paskirstymas leidžia užtikrinti, kad kibernetinio saugumo ugdymo procesas būtų ne tik techniškai įgyvendinamas, bet ir organizaciškai palaikomas. Tai ypač svarbu KAS, kur mokymosi efektyvumas priklauso nuo aiškios atsakomybių struktūros ir koordinuoto skirtingų dalyvių bendradarbiavimo.

6.2. Kibernetinio saugumo įgūdžių ugdymo paramos teikimo planas

Remiantis atlikta KAS kibernetinio saugumo ataskaitų analize bei apibrėžtais nuotolinio mokymosi dalyvių vaidmenimis ir atsakomybėmis, sudaromas kibernetinio saugumo ugdymo nuotoliniu būdu paramos teikimo planas. Šio plano tikslas – užtikrinti nuoseklų, duomenimis pagrįstą ir į besimokantįjį orientuotą kibernetinio saugumo ugdymą, mažinant žmogiškojo faktoriaus keliamas kibernetines rizikas. Paramos teikimo planas apima tiek technologinius, tiek organizacinius aspektus.

Paramos teikimo planas apima kelias tarpusavyje susijusias paramos sritis: mokymosi turinio paramą, techninę paramą, konsultacinę paramą, vertinimo ir grįžtamojo ryšio paramą bei mokymosi stebėseną ir tobulinimą.

Mokymosi turinio parama apima nuotolinio mokymosi medžiagos rengimą ir atnaujinimą, orientuotą į realias KAS fiksuojamas kibernetines grėsmes. Mokymosi turinys formuojamas remiantis incidentų statistika ir apima tokias temas kaip socialinė inžinerija, apgaulingi elektroniniai laišakai, kenkimo programinė įranga, saugus darbas su informacinėmis sistemomis ir kibernetinė higiena. Medžiaga gali būti pateikiama įvairiais formatais: tekstinėmis instrukcijomis, vaizdo medžiaga, praktiniais pavyzdžiais ir testais.

Techninė parama užtikrina stabilų ir saugų nuotolinio mokymosi aplinkos veikimą. RIS specialistai bei saugumo įgaliotinis yra atsakingi už nuotolinio mokymosi platformų prieinamumą, naudotojų autentifikavimą, duomenų saugumą ir techninių trikdžių šalinimą.

Konsultacinė parama apima nuolatinį bendravimą tarp besimokančiųjų ir instruktorių. Besimokantieji turi galimybę gauti konsultacijas nuotoliniu būdu, užduoti klausimus, aptarti kylančias problemas ir gauti metodinę pagalbą.

Vertinimo ir grįžtamojo ryšio parama grindžiama nuolatiniu besimokančiųjų žinių tikrinimu ir mokymosi rezultatų analize. Vertinimui gali būti naudojami teoriniai testai, praktinės užduotys ir mokymosi pažangos stebėseną. Instruktoriai, remdamiesi rezultatais, teikia individualų ir grupinį grįžtamąjį ryšį.

Mokymosi stebėseną ir tobulinimą vykdomi analizuojant mokymosi aplinkos duomenis, tokius kaip besimokančiųjų aktyvumas, mokymuisi skirtas laikas, testų rezultatai ir pasikartojančios klaidos. Ši informacija leidžia instruktoriams įvertinti mokymosi poveikį, koreguoti turinį ir planuoti tolesnes ugdymo priemones.

Apibendrinant galima teigti, kad parengtas kibernetinio saugumo ugdymo nuotoliniu būdu paramos teikimo planas sudaro vientisą sistemą, kuri apjungia mokymosi turinį, technologinius sprendimus, konsultacijas, vertinimą ir stebėseną. Tokia sistema leidžia kryptingai ugdyti KAS personalo kibernetinį raštingumą ir prisideda prie bendro kibernetinio saugumo lygio didinimo.

Parengtas paramos teikimo planas tiesiogiai siejasi su 5 skyriuje nustatytais poreikiais. Kadangi didžiausios grėsmės yra susijusios su socialine inžinerija, apgaulingais laiškais ir naudotojų elgsena, paramos priemonės turi būti orientuotos į praktinių situacijų analizę, greitą grįžtamąjį ryšį ir nuolatinį mokymosi turinio atnaujinimą pagal realias grėsmes.

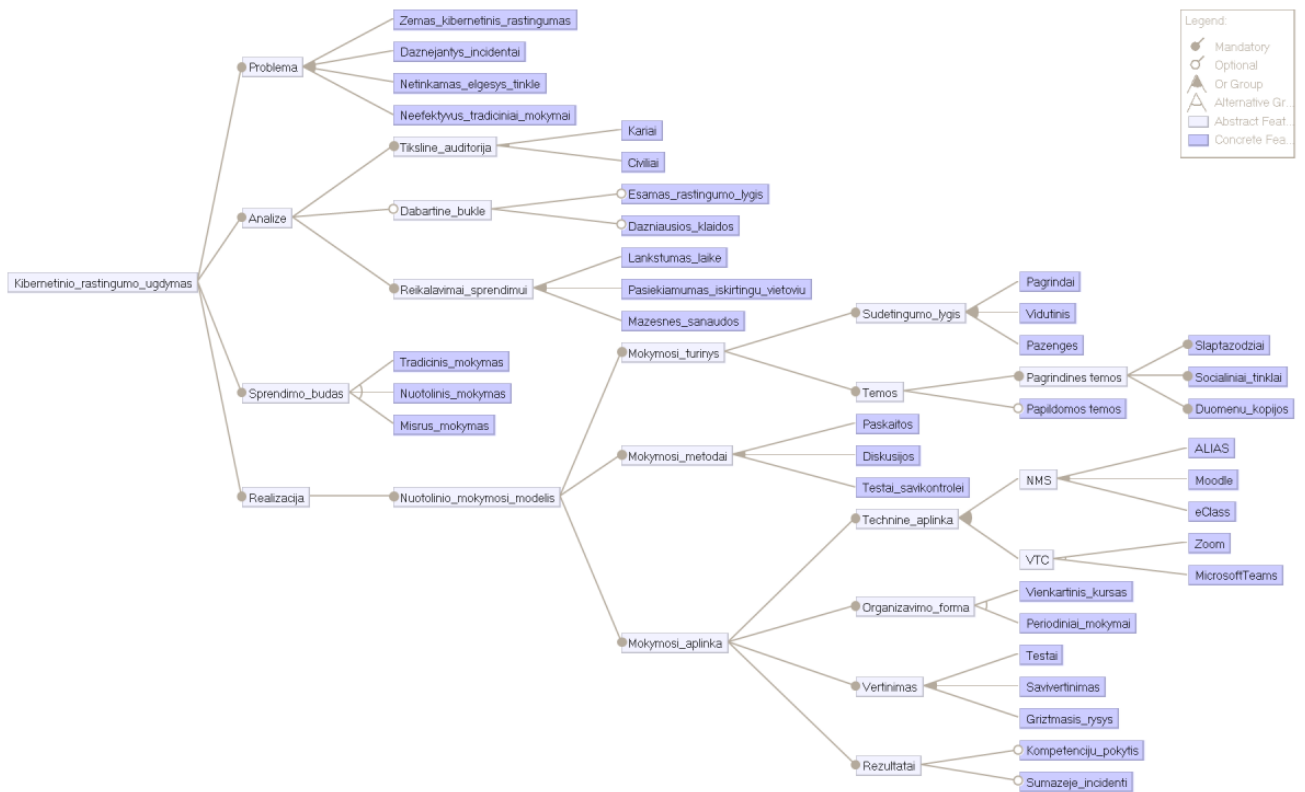
3 lentelė. Kibernetinio saugumo ugdymo nuotoliniu būdu paramos teikimo planas

Paramos sritis	Paramos priemonės	Atsakingi dalyviai	Nauda / tikslas
Mokymosi turinio parama	Nuotolinio mokymosi medžiaga (instrukcijos, vaizdo medžiaga, praktiniai pavyzdžiai), teoriniai testai, atnaujinamas turinys pagal incidentų statistiką	Instruktorius, RIS specialistai, saugumo įgaliotinis	Užtikrinti aktualų, duomenimis pagrįstą kibernetinio saugumo ugdymą
Techninė parama	Nuotolinio mokymosi platformos palaikymas, naudotojų autentifikavimas, techninių trikdžių šalinimas, saugumo sprendimų priežiūra	RIS specialistai	Užtikrinti stabilų, saugų ir patikimą mokymosi aplinkos veikimą
Konsultacinė parama	Nuotolinės konsultacijos, klausimų–atsakymų sesijos, metodinė pagalba, bendravimas el. paštu ar platformoje	Instruktorius, RIS specialistai, saugumo įgaliotinis	Padėti besimokantiems spręsti problemas ir geriau įsisavinti mokymosi turinį
Vertinimo ir grįžtamojo ryšio parama	Teoriniai testai, praktinės užduotys, individualus ir grupinis grįžtamasis ryšys	Instruktorius	Įvertinti žinių lygį, identifikuoti klaidas ir skatinti tobulėjimą
Mokymosi stebėseną ir tobulinimas	Mokymosi aktyvumo stebėjimas, testų rezultatų analizė, pasikartojančių klaidų identifikavimas	Instruktorius, RIS specialistai	Tobulinti mokymo turinį ir didinti kibernetinio saugumo efektyvumą
Organizacinė parama	Mokymuisi skirto laiko suteikimas, kibernetinio saugumo kultūros skatinimas	Dalinio vadovybė	Didinti personalo motyvaciją ir įsitraukimą į mokymosi procesą

6.3. Kibernetinio saugumo įgūdžių ugdymo požymių diagrama

Kibernetinio saugumo ugdymo požymių diagrama skirta struktūruotai aprašyti personalo kibernetinio saugumo ugdymo sistemą ir jos sudedamąsias dalis. Ši diagrama leidžia identifikuoti pagrindinius proceso elementus, jų hierarchinę struktūrą bei tarpusavio ryšius, taip sudarant prielaidas nuosekliam ugdymo modelio projektavimui.

Požymių diagramos šakninis elementas yra „Kibernetinio saugumo ugdymas“, kuris išskaidomas į keturias pagrindines požymių grupes: problemą, analizę, sprendimo būdą ir realizaciją (žr. 13 pav.).



13 pav. Kibernetinio saugumo ugdymo požymių diagrama

Problemos šakoje identifikuojami esminiai veiksniai, lemiantys kibernetinio saugumo trūkumus. Čia išskiriami tokie požymiai kaip žemas kibernetinio saugumo lygis, dažnėjančios incidentai, netinkamas elgesys tinkle ir neefektyvūs tradiciniai mokymai. Taip pat apibrėžiama tikslinė auditorija, kurią sudaro kariai ir civiliai darbuotojai.

Analizės dalyje vertinama dabartinė situacija ir identifikuojamos spragos. Čia nagrinėjamas esamas raštingumo lygis, daromos saugumo klaidos, incidentų pobūdis bei rizikų suvokimas. Taip pat apibrėžiami reikalavimai sprendimui, kurie tampa atskaitos tašku mokymo modelio kūrimui.

Sprendimo būdo šakoje pateikiamos galimos mokymo alternatyvos: tradicinis mokymas, NM, mišrus mokymas bei nuotolinio mokymosi modelis. Iš jų išskiriamas nuotoliniu ir mišriu mokymu grįstas sprendimas kaip labiausiai tinkamas adaptaciniam ir personalizuotam kibernetinio saugumo ugdymui.

Realizacijos dalis apima praktinį sprendimo įgyvendinimą. Čia detalizuojamas mokymo turinys, mokymo metodai, mokymo aplinka, organizavimo forma ir vertinimas. Mokymo turinys gali būti skirstomas pagal sudėtingumo lygius – pradinį, vidutinį ir pažengusį – apimant tokias temas kaip slaptažodžiai, socialinė inžinerija, duomenų kopijos ir dirbtinio intelekto grėsmės. Mokymo metodai apima paskaitas, diskusijas, testus ir savikontrolę. Mokymo aplinka realizuojama naudojant skaitmenines platformas, tokias kaip „Moodle“, „Open eClass“, „Zoom“ ar „Microsoft Teams“.

Požymių diagrama leidžia pažvelgti į kibernetinio saugumo ugdymo procesą kaip į tarpusavyje susijusių elementų sistemą. Ji suteikia aiškią struktūrą, kuri gali būti naudojama tiek kuriant ugdymo modelį, tiek jį analizuojant ar tobulinant. Taip pat leidžia ne tik struktūruoti ugdymo modelį, bet ir

parodyti, kad kibernetinio saugumo ugdymas turi būti suprantamas kaip kompleksinė sistema, kurioje problemos, jų analizė, sprendimo pasirinkimas ir realizacija yra tarpusavyje susiję elementai.

6.4. Kibernetinio saugumo ugdymo kontekstinis grafas

Požymių diagramos elementai gali būti transformuojami į kontekstinio grafo sąlyginius mazgus (C), apibrėžiančius besimokančiojo būklę, bei veiksmų mazgus (A), nurodančius taikomas ugdymo ar korekcines priemones. Tokiu būdu požymių diagrama atsako į klausimą, kas sudaro sistemą, o kontekstinis grafas – kaip sistema veikia skirtingomis sąlygomis.

Kontekstinis grafas leidžia vizualiai pavaizduoti personalo kibernetinio saugumo ugdymo procesą, parodant, kaip mokymosi eiga keičiasi priklausomai nuo besimokančiojo žinių lygio, daromų klaidų ir testų rezultatų. Grafas leidžia aiškiai matyti, kokie veiksmai atliekami esant skirtingoms sąlygoms ir kokių kelių pasiekiamas pagrindinis tikslas – sumažinti kibernetinių incidentų riziką ir užtikrinti saugų personalo elgesį informacinėse sistemose.

Lentelėje pateikiami kontekstiniai sąlygų mazgai (C1–C6), kurie apibrėžia sprendimo logiką. Šios sąlygos nusako, kokiais atvejais mokymosi procesas tęsiamas, kada būtina taikyti papildomas priemones ir kaip nustatoma besimokančiojo pasirengimo bei saugaus elgesio būklė (žr. lentelę 5).

4 lentelė. Kontekstinių sąlygų mazgai (C1–C6)

Elementas	Reikšmė
C1	Ar besimokantysis turi pakankamą kibernetinio saugumo lygį?
C2	Ar besimokantysis daro kritines saugumo klaidas?
C3	Ar besimokantysis supranta galimas rizikas organizacijai?
C4	Ar besimokantysis geba taikyti saugaus elgesio principus praktikoje?
C5	Ar besimokantysis išlaikė savikontrolės testą?
C6	Ar sumažėjo incidentų rizika ir pasiektas tikslas?

Lentelėje taip pat pateikiami veiksmų mazgai (A1–A7), kurie nurodo, kokie konkretūs mokymo ar korekcijos veiksmai atliekami esant atitinkamoms sąlygoms kontekstiniame grafe. Šie veiksmai sudaro nuoseklų personalo kibernetinio saugumo ugdymo procesą (žr. lentelę 6).

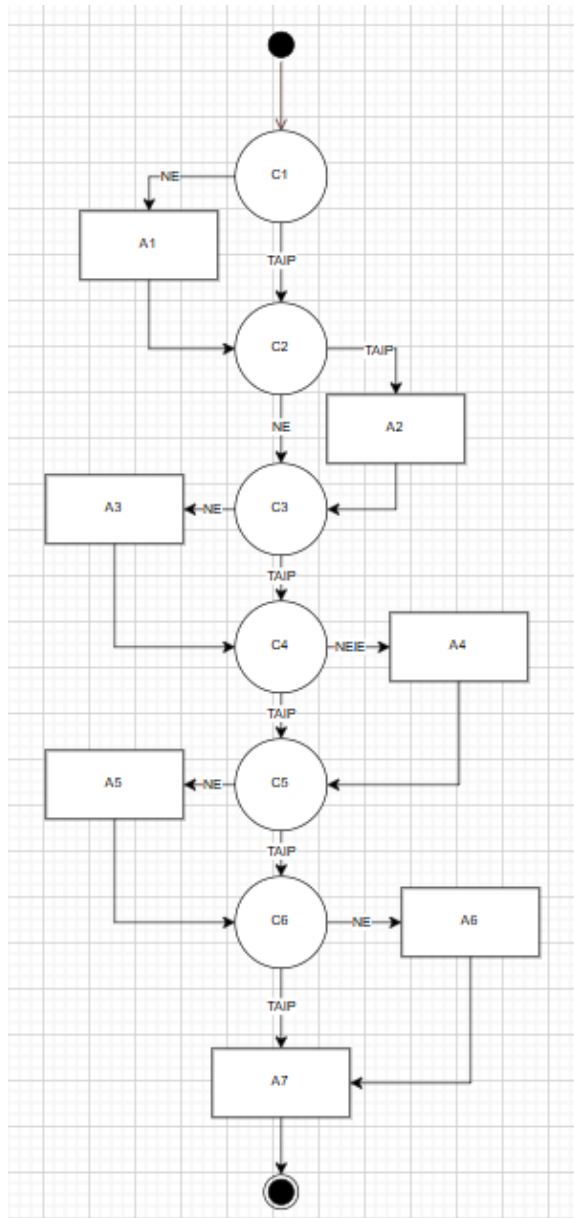
5 lentelė. Veiksmų mazgai (A1–A7)

Elementas	Reikšmė
A1	Suteikti pradinį kibernetinio saugumo mokymą
A2	Pateikti personalizuotas mokomąsias priemones pagal klaidas
A3	Pateikti edukacinius rizikų scenarijus
A4	Suteikti praktines kibernetinio saugumo užduotis
A5	Leisti atlikti savikontrolės testą nuotolinėje aplinkoje
A6	Suteikti grįžtamąjį ryšį ir korekcijas pagal testo rezultatus
A7	Patvirtinti, kad tikslas pasiektas ir incidentų rizika sumažinta

Paveiksle pavaizduotas kontekstinis grafas, vaizduojantis personalo kibernetinio saugumo ugdymo proceso eigą. Grafas parodo, kaip mokymosi kelias kinta priklausomai nuo besimokančiojo žinių

lygio, klaidų, rizikų supratimo ir testų rezultatų, ir kaip pasiekiamas galutinis mokymo tikslas (žr. 14 pav.).

Kontekstinis grafas suteikia galimybę modeliuoti ne vien teorinį mokymosi procesą, bet ir praktinį sprendimų priėmimą, priklausantį nuo besimokančiojo pasirengimo lygio. Tai leidžia kurti adaptyvų ugdymo modelį, kuriame mokymosi eiga gali būti pritaikoma pagal realius naudotojo rezultatus ir daromas klaidas.



14 pav. KAS personalo kibernetinio saugumo ugdymo kontekstinis grafas

6.5. Skyriaus išvados

1. Apibendrinant galima teigti, kad nuotolinio kibernetinio saugumo ugdymo paramos modelis turi būti grindžiamas aiškiai apibrėžtais dalyvių vaidmenimis, nuosekliu bendradarbiavimu ir sisteminga parama besimokantiejiems. Efektyvus instruktorių, RIS specialistų, saugumo įgaliotinio bei dalinio vadovybės bendradarbiavimas sudaro prielaidas sėkmingam mokymosi procesui.

2. Parengtas paramos teikimo planas leidžia struktūruotai apibrėžti pagrindines paramos sritis – mokymosi turinį, techninį palaikymą, konsultacijas, vertinimą ir stebėseną. Tokia sistema prisideda prie kryptingo personalo kibernetinio saugumo kompetencijų ugdymo.
3. Požymių diagrama ir kontekstinis grafas leidžia modeliuoti kibernetinio saugumo ugdymo procesą kaip vientisą sistemą, kurioje aiškiai matyti pagrindiniai proceso elementai, jų ryšiai ir sprendimų logika. Tai sudaro prielaidas nuosekliam ir duomenimis pagrįstam nuotolinio kibernetinio saugumo ugdymo organizavimui. Toks modelis taip pat sudaro metodinį pagrindą specializuotos virtualiosios mokymosi aplinkos kūrimui, orientuotam į KAS personalo kibernetinio saugumo įgūdžių ugdymą.

7. Virtualios mokymosi aplinkos realizacija

Kuriama VMA skirta kibernetinio saugumo įgūdžių ugdymui. Sistema suteikia galimybę mokytis per struktūruotus mokymosi modulius, apimančius tokias temas kaip slaptažodžių saugumas, sukčiavimo (angl. phishing) atpažinimas, asmens duomenų apsauga ir saugus elgesys internete.

Sistema leidžia vartotojams:

- mokytis savarankiškai pasirinktu tempu;
- dalyvauti interaktyviose užduotyse ir testuose;
- įsivertinti savo žinių lygį;
- tobulinti praktinius kibernetinio saugumo įgūdžius.

Tokiu būdu VMA prisideda prie vartotojų sąmoningumo didinimo ir saugesnio elgesio skaitmeninėje erdvėje formavimo.

Kuriant sistemą taikomas iteratyvus ir lankstus programinės įrangos kūrimo metodas, grindžiamas nuolatiniu funkcionalumo tobulinimu, testavimu ir pritaikymu pagal naudotojų poreikius. Šio metodo esmė:

- sistemos funkcionalumas kuriamas etapais;
- sprendimai priimami remiantis praktiniu sistemos veikimu;
- didelis dėmesys skiriamas naudotojo sąsajos paprastumui ir aiškumui;
- sistema nuolat tobulinama atsižvelgiant į grįžtamąjį ryšį.

Toks kūrimo principas leidžia sukurti lanksčią ir praktiškai pritaikomą virtualią mokymosi aplinką.

7.1. Sprendimo pagrindimas ir santykis su esamomis sistemomis

Nors šiuolaikinėje praktikoje plačiai naudojamos virtualios mokymosi aplinkos, tokios kaip „Moodle“ ar „Open eClass“, šiame darbe buvo pasirinkta kurti atskirą prototipinę sistemą.

Toks sprendimas priimtas siekiant sukurti specializuotą aplinką, orientuotą būtent į KAS personalo kibernetinio saugumo įgūdžių ugdymą.

Esamos mokymosi platformos yra universalios ir pritaikytos įvairioms mokymo sritims, tačiau jos nėra orientuotos į specifinius kibernetinio saugumo scenarijus, aktualius KAS. Tokie scenarijai kaip socialinės inžinerijos atakos, sukčiavimo (angl. phishing) atvejai ar saugaus elgesio informacinėse sistemose praktika reikalauja tikslinio turinio ir interaktyvių sprendimų, kurie gali būti efektyviau įgyvendinami specializuotoje aplinkoje.

Sukurtas sprendimas šiame darbe vertintinas kaip minimalus veikiantis produktas (toliau - MVP), skirtas įvertinti, kaip specializuota VMA gali prisidėti prie kibernetinio saugumo įgūdžių stiprinimo. Šis prototipas leidžia testuoti pasirinktus mokymo metodus, vertinti naudotojų įsitraukimą bei analizuoti mokymosi proceso efektyvumą.

Taip pat pažymėtina, kad kuriama sistema nėra skirta pakeisti esamas mokymosi platformas, o gali būti integruojama arba naudojama kaip papildomas įrankis šalia jau veikiančių sprendimų, tokių kaip „Moodle“. Tokiu būdu sudaromos prielaidos plėtoti kompleksinį ir efektyvų kibernetinio saugumo įgūdžių ugdymo modelį.

7.2. Sukurto produkto aprašas

Sukurta kibernetinio saugumo įgūdžių ugdymo platforma yra skirta vartotojų švietimui apie saugų elgesį skaitmeninėje erdvėje. Platformos tikslas – padėti vartotojams atpažinti kibernetines grėsmes ir ugdyti praktinius įgūdžius, reikalingus asmeninių duomenų bei skaitmeninės tapatybės apsaugai.

Sistema orientuota į savarankišką mokymąsi, todėl vartotojai gali mokytis jiems patogiu metu ir tempu. Pagrindiniame platformos puslapyje pateikiama informacija apie mokymosi tikslus, naudą bei pateikiama aiški navigacija, leidžianti lengvai pasiekti mokymosi turinį.

Platformoje pateikiami struktūruoti mokymosi kursai, suskirstyti pagal temas, tokias kaip:

- slaptažodžių saugumas;
- duomenų apsauga;
- socialinė inžinerija;
- saugus elgesys internete.

Kiekvienas kursas sudarytas iš pamokų, kuriose pateikiama:

- teorinė medžiaga;
- praktiniai pavyzdžiai;
- rekomenduojami veiksmai.

Po kiekvienos pamokos vartotojai gali atlikti testus bei praktines užduotis. Testai leidžia įsivertinti įgytas žinias, o rezultatai pateikiami iš karto, skatinant refleksiją ir mokymosi tęstinumą. Sistema taip pat suteikia galimybę stebėti mokymosi pažangą – vartotojai gali matyti atliktas pamokas, testų rezultatus ir savo tobulėjimą laikui bėgant.

Administravimo funkcijos leidžia:

- kurti ir valdyti kursus;
- stebėti vartotojų aktyvumą;
- analizuoti mokymosi rezultatus.

Apibendrinant galima teigti, kad sukurta sistema sudaro sąlygas sistemingai ugdyti kibernetinio saugumo įgūdžius ir taikyti juos praktikoje. Šis produktas atitinka ankstesniuose skyriuose identifiкуotus poreikius, nes orientuojasi ne tik į teorinių žinių perteikimą, bet ir į praktinių įgūdžių formavimą, pažangos stebėseną bei aktyvų vartotojo įsitraukimą.

7.3. Programinės įrangos priemonės sistemos realizacijai

Kuriant virtualiąją mokymosi aplinką, būtina paruošti tinkamą programinę aplinką ir pasirinkti atitinkamas technologijas, kurios užtikrintų sistemos kūrimą, testavimą ir diegimą.

Šiam projektui buvo naudojamos šios pagrindinės programinės priemonės (žr. 14 pav.):

- Cursor – programavimo aplinka, skirta efektyviam kodo rašymui ir redagavimui [15];
- Node.js – serverinės dalies vykdymo aplinka [16];
- GitHub ir GitHub Desktop – versijų kontrolės sistema ir projekto valdymo priemonė [17];
- Supabase – duomenų bazės ir autentifikacijos sprendimas [18];
- Vercel – sistemos talpinimo ir diegimo platforma [19].

Šių technologijų derinys leidžia užtikrinti modernios, greitos ir lengvai plečiamos virtualios mokymosi aplinkos sukūrimą. Pasirinktas technologijų rinkinys atitinka kuriamos sistemos poreikius, nes leidžia realizuoti tiek vartotojų autentifikaciją, tiek mokymosi turinio valdymą, pažangos stebėseną ir viešą sistemos publikavimą. Be to, šios technologijos užtikrina sprendimo lankstumą ir plėtros galimybes ateityje. Detalios sistemos diegimo instrukcijos pateikiamos (1 priede).



15 pav. Pagrindinės programinės įrangos

7.4. Sistemos realizavimo eiga

Prieš pradėdant programavimo darbus buvo parengtas produkto reikalavimų dokumentas (toliau - PRD), leidęs aiškiai apibrėžti sistemos tikslus, vartotojų roles, pagrindinį funkcionalumą ir MVP apimtį. PRD rengimui buvo pasitelkti dirbtinio intelekto įrankis „Claude AI“ [20], kuris padėjo struktūruoti pirminius reikalavimus bei suformuoti MVP funkcionalumą „User Stories“ formatu.

Parengus PRD dokumentą, buvo sukurta projekto kūrimo aplinka, apimanti versijų valdymo, programavimo, duomenų bazės ir diegimo priemones. Projekto realizavimo metu buvo:

- parengta programinė aplinka;
- sukonfigūruota versijų kontrolė;
- sukurta duomenų bazės ir autentifikacijos infrastruktūra;
- parengta projekto architektūra;
- pradėtas funkcinių komponentų įgyvendinimas.

Šiame etape naudotos technologijos leido užtikrinti nuoseklų ir valdomą sistemos kūrimo procesą bei sudarė sąlygas tolesniam funkcionalumo plėtimui. Sistemos realizavimo eiga rodo, kad kuriamas sprendimas nebuvo formuojamas atsitiktinai, bet buvo grindžiamas aiškiai apibrėžtais reikalavimais ir nuosekliu kūrimo procesu. Tai sustiprina darbo praktinę vertę ir pagrindžia kuriamos sistemos aktualumą. Detalesnės dirbtinio intelekto užklausos ir gauti atsakymai pateikiami (žr. 2 priedą).

Parengus produkto reikalavimų dokumentą, buvo pradėtas virtualiosios mokymosi aplinkos kūrimo procesas. Kūrimas buvo vykdomas naudojant internetinių aplikacijų kūrimo technologijas ir komponentinę architektūrą.

Pirmiausia buvo sukurta projekto struktūra ir apibrėžti pagrindiniai sistemos komponentai bei duomenų modeliai. Vėliau buvo įgyvendintos pagrindinės sistemos funkcijos:

- vartotojų autentifikacija ir registracija;
- mokymosi modulių peržiūra;
- testavimo ir užduočių atlikimo sistema;
- mokymosi progreso stebėseną;
- administravimo funkcijos.

Kūrimo metu buvo nuolat atliekamas funkcionalumo testavimas, vertinamas naudotojo sąsajos patogumas ir atliekami patobulinimai pagal gautą grįžtamąjį ryšį. Sistema buvo diegiama naudojant „Cursor“ platformą, kuri leidžia automatiškai atnaujinti aplikaciją po kiekvieno kodo pakeitimo. Svarbiausi sistemos realizacijos fragmentai pateikiami (žr. 1, 3 priedus).

7.5. Platformos taikymo ir poveikio vartotojų žinioms tyrimas

Atliekant baigiamojo projekto tyrimą buvo siekiama įvertinti sukurtos kibernetinio saugumo mokymosi platformos efektyvumą. Tyrimas buvo vykdomas taikant eksperimentinį metodą, pagrįstą vartotojų sąveika su sukurta sistema.

Tyrimo metu nustatyta, kad platformoje (<https://bagiamasisprojektas.vercel.app/>) apsilankė daugiau nei 220 vartotojų, tačiau tyrimą iki galo atliko 52 respondentai, kurie savanoriškai pilnai išbandė platformą. Tyrimo dalyviai buvo skirtingo amžiaus ir patirties, dauguma jų jau turėjo ankstesnės patirties naudojantis nuotolinio mokymosi sistemomis.

Tyrimo metu respondentai:

- susipažino su platformoje pateikta teorine medžiaga;
- atliko žinių patikrinimo testus;
- sprendė baigiamąjį testą;
- užpildė apklausą apie platformos naudojimo patirtį (žr. 5 priedą).

Tokiu būdu buvo surinkti tiek kiekybiniai duomenys (testų rezultatai ir vertinimai), tiek kokybiniai duomenys (respondentų atsiliepimai).

7.6. Tyrimo rezultatai

Tyrimo rezultatai parodė, kad didžioji dalis respondentų 76,9 % jau buvo anksčiau dalyvavę nuotoliniuose mokymuose, todėl galėjo objektyviai įvertinti platformos funkcionalumą.

Vertinant pradinės kibernetinio saugumo žinias nustatyta, kad 44,2 % respondentų savo žinias vertino kaip geras, 36,5 % – kaip vidutines. Tai rodo, kad platforma buvo testuojama ne tik pradedančiuju, bet ir jau turinčių pagrindinių žinių vartotojų.

Platformos naudojimo paprastumas buvo įvertintas labai aukštai – net 46,2 % respondentų skyrė maksimalų (10) balą. Taip pat nustatyta, kad 94,2 % respondentų platformos struktūrą vertino kaip aiškia ir suprantama. Platformos dizainas taip pat sulaukė teigiamo įvertinimo – dauguma respondentų skyrė 8–10 balų, o 40,4 % – maksimalų įvertinimą.

Vertinant mokymosi medžiagą nustatyta, kad 88,5 % respondentų ją laikė aiškia ir naudinga. Tai rodo, kad pateiktas turinys yra tinkamai parengtas ir suprantamas vartotojams. Testų kokybės vertinimas parodė, kad 94,2 % respondentų klausimus laikė aiškiais. Tačiau dalis respondentų nurodė, kad testų sudėtingumas galėtų būti didesnis.

Svarbiausias tyrimo rezultatas – platformos poveikis vartotojų žinioms. Net 80,8 % respondentų nurodė, kad platforma padėjo pagerinti jų kibernetinio saugumo žinias, o dar 17,3 % – kad pagerino iš dalies. Be to, net 96 % respondentų rekomenduoju platformą kitiems, o 94,2 % teigė, kad naudotųsi tokia sistema ateityje.

Kokybinė rezultatų analizė. Analizuojant respondentų pateiktus atvirus atsakymus nustatyta, kad labiausiai vertinami platformos aspektai yra:

- paprastas ir aiškus naudojimas;
- neperkrautas ir patrauklus dizainas;
- lengva navigacija;
- aiškiai pateikta informacija;
- galimybė patikrinti savo žinias.

Tačiau respondentai taip pat pateikė ir pasiūlymų platformos tobulinimui. Dažniausiai minimi aspektai:

- poreikis didinti testų sudėtingumą,
- klausimų įvairovės trūkumas,
- praktinių situacijų (pvz., phishing pavyzdžių) trūkumas,
- nenoras registruotis pateikiant asmeninius duomenis,
- techniniai nesklandumai (testų atsistatymas perkrovus puslapį).

Taip pat buvo siūloma išplėsti platformos turinį, įtraukiant daugiau mokymosi medžiagos ir temų.

7.7. Skyriaus išvados

1. Apibendrinant galima teigti, kad šiame skyriuje aprašyta virtualiosios mokymosi aplinkos realizacija pagrindžia sukurtos sistemos tinkamumą KAS personalo kibernetinio saugumo įgūdžių ugdymui. Pasirinktos technologijos ir taikytas iteratyvus kūrimo metodas leido sukurti lanksčią, lengvai plečiamą ir praktikoje pritaikomą sistemą. Dirbtinio intelekto panaudojimas projektavimo etape padėjo efektyviau apibrėžti sistemos reikalavimus ir sumažinti kūrimo sudėtingumą.
2. Sukurta sistema atitinka ankstesniuose skyriuose iškeltus reikalavimus, leidžia organizuoti nuotolinį mokymąsi, vertinti žinias ir stebėti mokymosi pažangą, todėl gali būti sėkmingai taikoma kibernetinio saugumo ugdymo procese.
3. Atlikus tyrimą nustatyta, kad sukurta kibernetinio saugumo mokymosi platforma yra tinkama įvairaus pasirengimo vartotojams, kadangi dauguma jų pasižymėjo vidutiniu arba geru pradinio žinių lygiu. Platforma pasižymi aukštu naudojimo paprastumu, aiškia struktūra ir logišku informacijos pateikimu, o jos dizainas yra patrauklus ir neperkrautas. Tai leidžia vartotojams lengvai orientuotis sistemoje ir efektyviai naudotis pateiktu mokymosi turiniu.
4. Tyrimo rezultatai parodė, kad platformoje pateikta mokymosi medžiaga yra suprantama ir naudinga, o testų klausimai – aiškūs. Tačiau nustatyta, kad testų sudėtingumas kai kuriais atvejais yra nepakankamas, o praktinių užduočių trūkumas riboja galimybę taikyti žinias realiose situacijose. Dėl to rekomenduojama didinti klausimų įvairovę, sudėtingumą bei įtraukti daugiau situacinių užduočių. Taip pat nustatyta, kad platforma daro reikšmingą teigiamą poveikį vartotojų žinioms ir pasižymi labai aukštu pasitenkinimo lygiu – dauguma vartotojų ją rekomenduoju kitiems ir naudotųsi ateityje. Vis dėlto vartotojų pasitikėjimą mažina būtinybė registruotis pateikiant asmeninius duomenis, o tam tikri techniniai trūkumai daro įtaką naudojimo patirčiai, todėl jų sprendimas yra svarbus tolimesniam sistemos tobulinimui.

Išvados

1. Atlikus krašto apsaugos sistemos kibernetinių incidentų ir duomenų saugumo pažeidimų ataskaitų analizę nustatyta, kad didžiausią riziką saugumui kelia socialinės inžinerijos atakos, o žmogiškoji klaida išlieka dominuojančia pažeidimų priežastimi, kasmet lemdama nuo 52 % iki 72 % visų incidentų. Šie dėsningumai įrodo, kad net ir pačios pažangiausios technologinės bei automatinės filtravimo priemonės nėra pajėgios visiškai neutralizuoti grėsmių, jei informacinių sistemų naudotojai nesugeba atpažinti apgaulingo ir manipuliacinio pobūdžio turinio.
2. Ištyrus krašto apsaugos sistemos personalo kibernetinio saugumo įgūdžius išryškėjo kritinė spraga tarp teorinių žinių ir praktinių saugumo principų taikymo: didelė dalis personalo nenaudoja skirtingų slaptažodžių, o dalis personalo ignoroja dviejų veiksnių autentifikacijos (2FA) apsaugą. Kartu identifikuota, kad aukštą rizikos lygį lemia ne tik bazinės kibernetinės higienos trūkumas, bet ir tai, jog net pusė darbuotojų susiduria su mokymosi motyvacijos stoka dėl neįtraukiančių ir vien į teoriją orientuotų tradicinių mokymo formatų. Tai patvirtina būtinybę pereiti prie interaktyvaus, į elgsenos formavimą orientuoto nuotolinio ugdymo.
3. Lyginamoji universalių virtualiųjų mokymosi aplinkų, tokių kaip „Moodle“ ir „Open eClass“, analizė atskleidė esminę technologinę ir metodinę spragą. Nors šios sistemos pasižymi plačiu funkcionalumu, jos nėra pritaikytos specifiniams krašto apsaugos sistemos kibernetinio saugumo scenarijams, nes stokojama įrankių, leidžiančių simuliuoti tikslines atakas bei analizuoti ir individualizuoti naudotojų elgseną. Tai pagrindžia specializuoto, į konkrečius organizacijos poreikius orientuoto ir lanksčiai plečiamo mokymosi sprendimo sukūrimo būtinybę.
4. Remiantis reikalavimų specifikacija bei UML modeliavimu, suprojektuotas nuotolinio kibernetinio saugumo ugdymo paramos modelis, apjungiantis instruktorių, RIS specialistų, saugumo įgaliotinio bei dalinio vadovybės bendradarbiavimą. Panaudojant požymių diagramą ir kontekstinius grafus, suformuota vientisa mokymosi sistema, kurioje mokymosi eiga, korekciniai veiksmai ir grįžtamasis ryšys lanksčiai kinta priklausomai nuo besimokančiojo žinių lygio, daromų klaidų ir rizikų supratimo.
5. Realizavus virtualios mokymosi aplinkos sprendimą, pritaikant „React“, „Node.js“ bei „Supabase“ technologijas, eksperimentinis vartotojų testavimas įrodė į praktiką bei savikontrolę orientuoto mokymo efektyvumą. Gauti tyrimo rezultatai parodė, kad net 80,8 % testuotojų platformos pagalba pagerino savo kibernetinio saugumo žinias, o tai patvirtina, jog interaktyvi ir grįžtamąjį ryšį teikianti sistema sėkmingai atliepia poreikį didinti personalo atsparumą ir mažina žmogiškojo faktoriaus nulemtų kibernetinių incidentų riziką.

Literatūros sąrašas

1. KRAŠTO APSAUGOS MINISTERIJA. Lietuvos nacionalinio saugumo strategija. Vilnius: Krašto apsaugos ministerija, 2022.
2. ENISA. 2013 metų grėsmių analizė [interaktyvus]. 2013 [žiūrėta 2025-10-15]. Prieiga per internetą: https://www.enisa.europa.eu/sites/default/files/all_files/ENISAAnnualreport2013.pdf
3. CERT-LT. Kibernetinio saugumo incidentų ataskaita . Vilnius: NKSC, 2023
4. KRAŠTO APSAUGOS MINISTERIJA. Krašto apsaugos ministerijos ataskaita. Vilnius: Krašto apsaugos ministerija, 2022.
5. NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS. Nacionalinė kibernetinio saugumo ataskaita [interaktyvus]. 2023 [žiūrėta 2025-10-15]. Prieiga per internetą: <https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2023.pdf>
6. BEURAN, R., TANG, D., HASEGAWA, S., TAN, Z. ir TAN, Y. Supporting cybersecurity education and training via LMS integration: CyLMS. Springer, 2019.
7. KATSANTONIS, M. N., MANIKAS, A. ir MAVRIDIS, I. Cyber range design framework for cyber security education and training. International Journal of Information Security, 2023.
8. SUDNIUTĖ, G. Švietimo bendruomenės kibernetinio saugumo kompetencijų tobulinimas. Kaunas: Kauno technologijos universitetas, 2024.
9. NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS. NKSC kibernetinių mokymų platforma [interaktyvus]. NKSC, 2023 [žiūrėta 2025-11-12]. Prieiga per internetą: <https://mokymai.nksc.lt/>
10. NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS. Nacionalinio kibernetinio saugumo būklės ataskaita, 2020 m. [interaktyvus]. Vilnius: Krašto apsaugos ministerija, 2020 [žiūrėta 2025-11-14]. Prieiga per internetą: https://www.nksc.lt/doc/nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2020.pdf
11. NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS. Nacionalinio kibernetinio saugumo būklės ataskaita, 2021 m. [interaktyvus]. Vilnius: Krašto apsaugos ministerija, 2021 [žiūrėta 2025-11-14]. Prieiga per internetą: <https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2021.pdf>
12. NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS. Nacionalinio kibernetinio saugumo būklės ataskaita, 2022 m. [interaktyvus]. Vilnius: Krašto apsaugos ministerija, 2022 [žiūrėta 2025-11-14]. Prieiga per internetą: <https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2022.pdf>
13. NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS. Nacionalinio kibernetinio saugumo būklės ataskaita, 2024 m. [interaktyvus]. Vilnius: Krašto apsaugos ministerija, 2024 [žiūrėta 2025-11-14]. Prieiga per internetą: <https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2024.pdf>
14. LIETUVOS KARIUOMENĖ KIBERNETINĖS GYNYBOS VALDYBA. Įvykių suvestinės. Vilnius: Lietuvos kariuomenė Kibernetinės gynybos valdyba, 2025.
15. ANYSPHERE, INC. Cursor: The best way to code with AI [interaktyvus]. 2026 [žiūrėta 2026-04-01]. Prieiga per internetą: <https://www.cursor.com/>
16. OPENJS FOUNDATION. Node.js — Run JavaScript Everywhere [interaktyvus]. [žiūrėta 2026-04-01]. Prieiga per internetą: <https://nodejs.org/>

17. GITHUB, INC. GitHub · Change is constant. GitHub keeps you ahead. [interaktyvus]. 2026 [žiūrėta 2026-04-01]. Prieiga per internetą: <https://github.com/>
18. SUPABASE INC. Supabase | The Postgres Development Platform. [interaktyvus]. [žiūrėta 2026-04-01]. Prieiga per internetą: <https://supabase.com/>
19. VERCEL. Vercel: Build and deploy the best web experiences with the AI Cloud [interaktyvus]. [žiūrėta 2026-04-01]. Prieiga per internetą: <https://vercel.com/>
20. ANTHROPIC. Claude [interaktyvus]. [žiūrėta 2026-04-05]. Prieiga per internetą: <https://claude.ai/>

Priedai

1 priedas. Sistemų diegimo instrukcijos

GitHub paskyros sukūrimas

Pirmasis žingsnis kuriant sistemą – susikurti paskyrą GitHub platformoje, kuri naudojama projekto kodo saugojimui ir versijų valdymui.

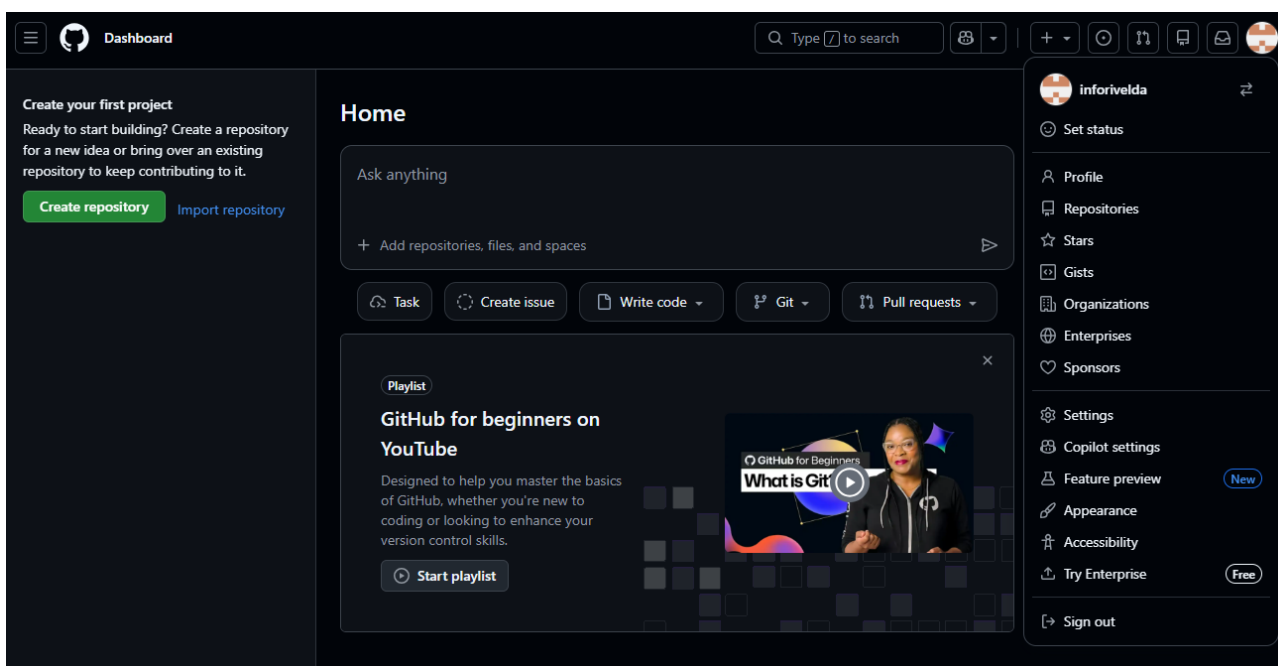
GitHub bus naudojamas:

- projekto kodo saugojimui (versijų valdymui);
- komandinio darbo organizavimui;
- integracijai su kitomis paslaugomis (Supabase, Vercel).

Veiksmai:

- Apsilankyti svetainėje <https://github.com>;
- Užsiregistruoti naudojant el. Paštą.

Ši paskyra vėliau bus naudojama prisijungiant prie kitų sistemų, todėl rekomenduojama naudoti tą patį el. paštą.



16 pav. Prisijungimas „GitHub“ sukurtas

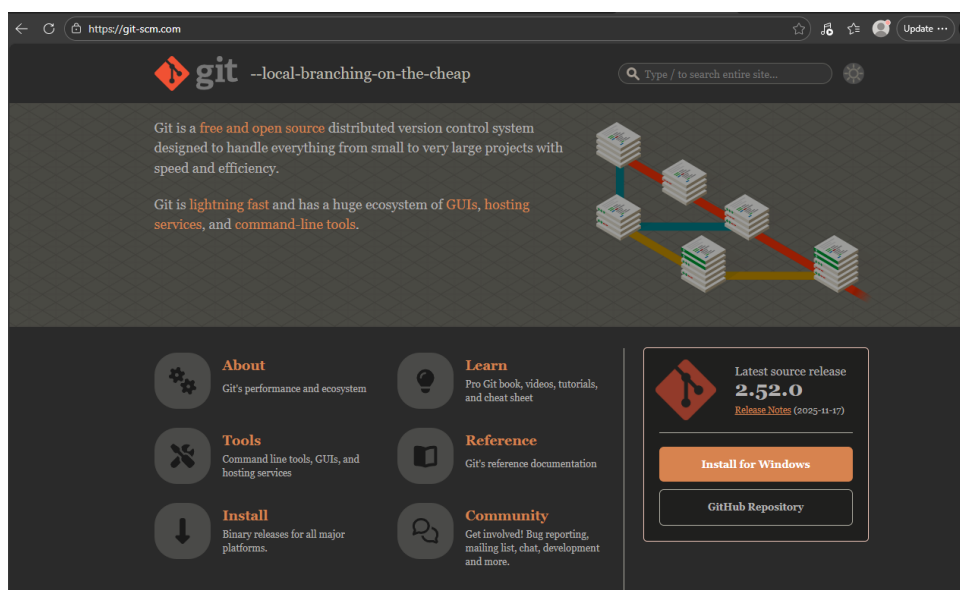
Git įdiegimas

Git yra versijų valdymo sistema, leidžianti sekti projekto pakeitimus.

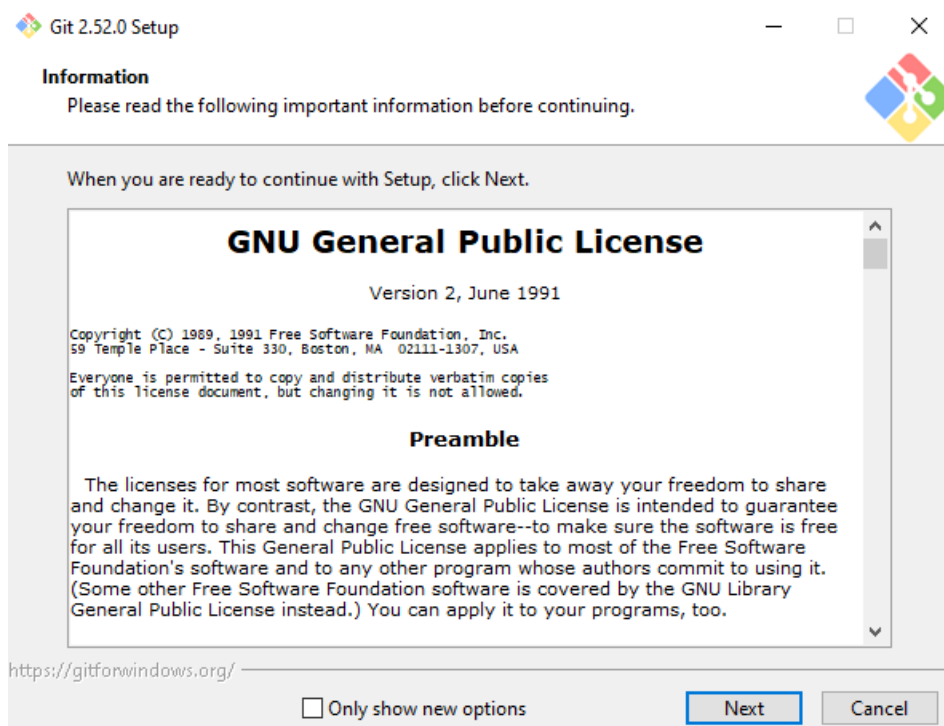
Veiksmai:

- Apsilankyti <https://git-scm.com>;
- Atsisiųsti diegimo failą pagal naudojamą operacinę sistemą;
- Įdiegti paliekant numatytuosius nustatymus.

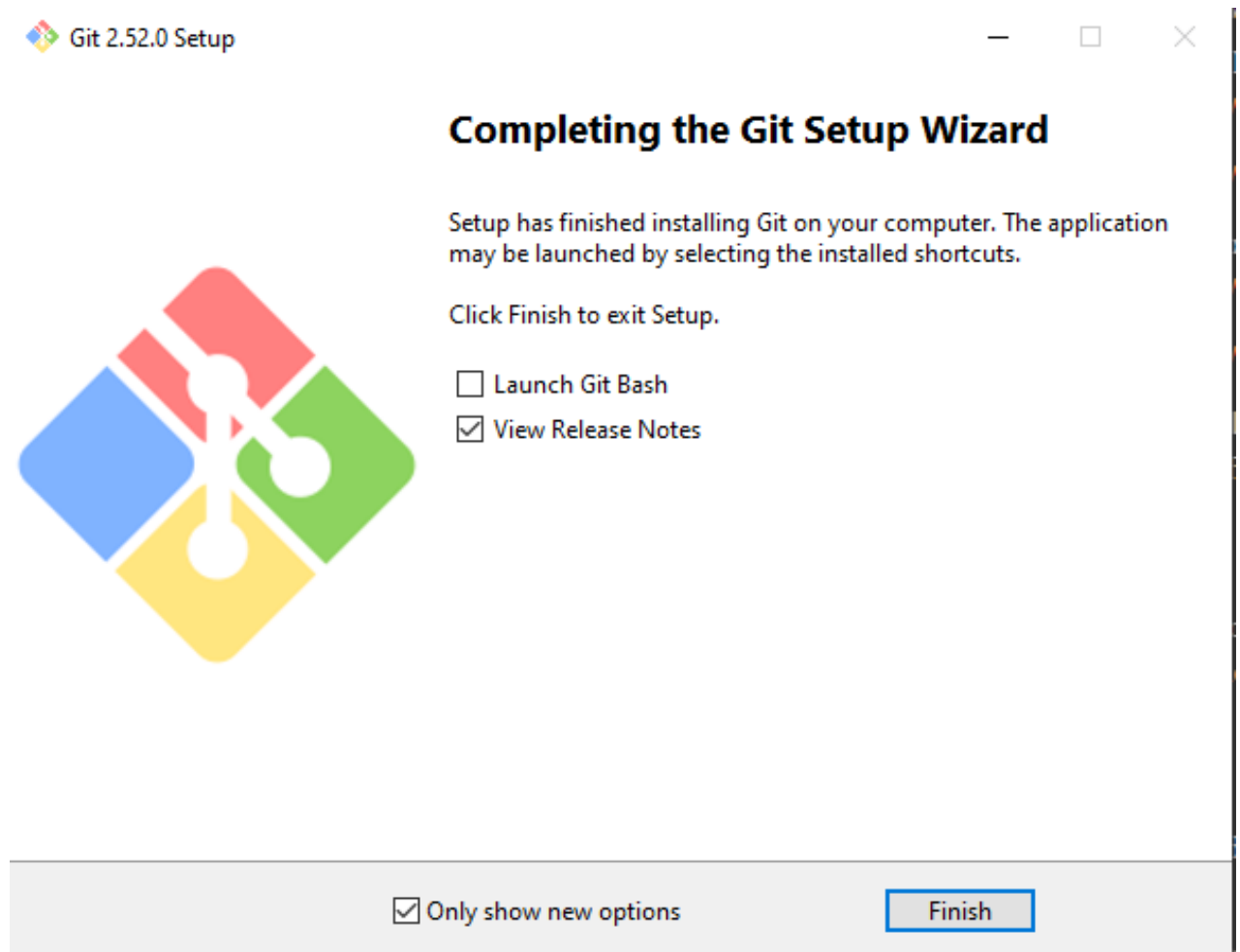
Git leis lokaliai dirbti su projektu ir sinchronizuoti kodą su GitHub saugykla.



17 pav. „Git“ atsisiuntimas



18 pav. „Git“ įdiegimas



19 pav. „Git“ įdiegimas baigtas

Node.js įdiegimas

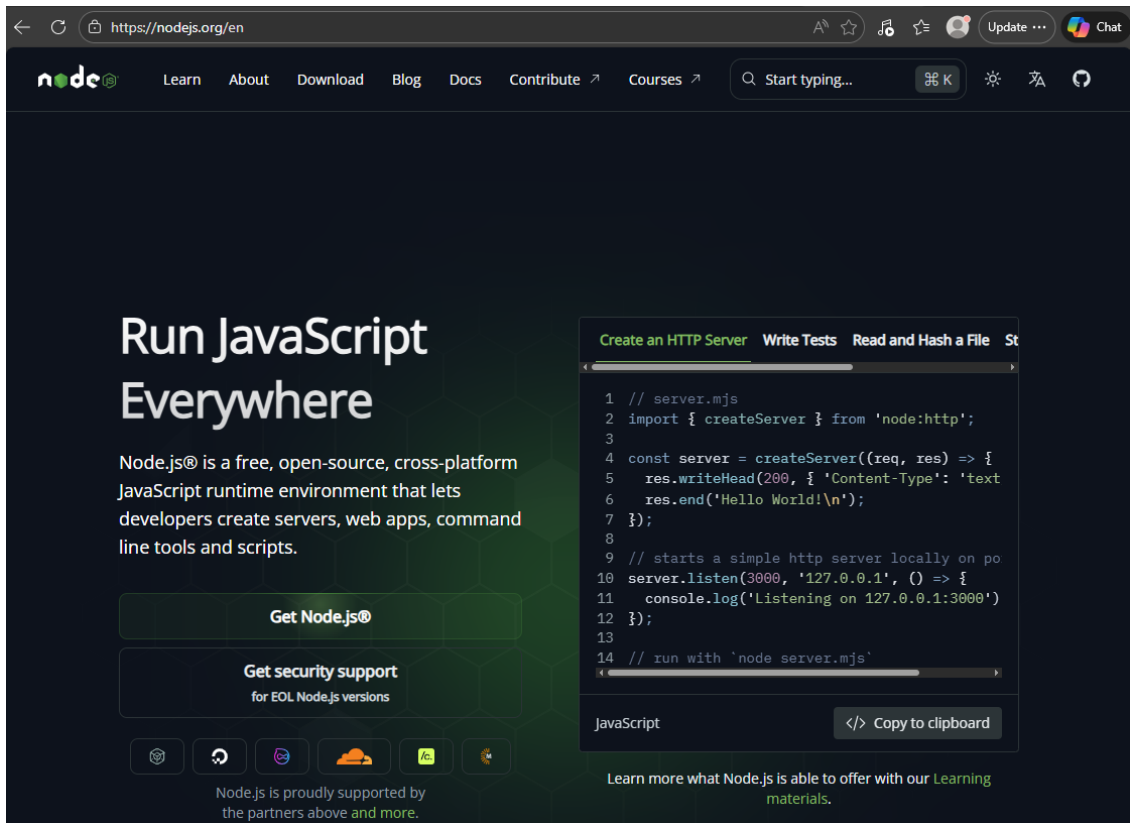
Node.js naudojamas React aplikacijos paleidimui ir paketų valdymui.

Veiksmai:

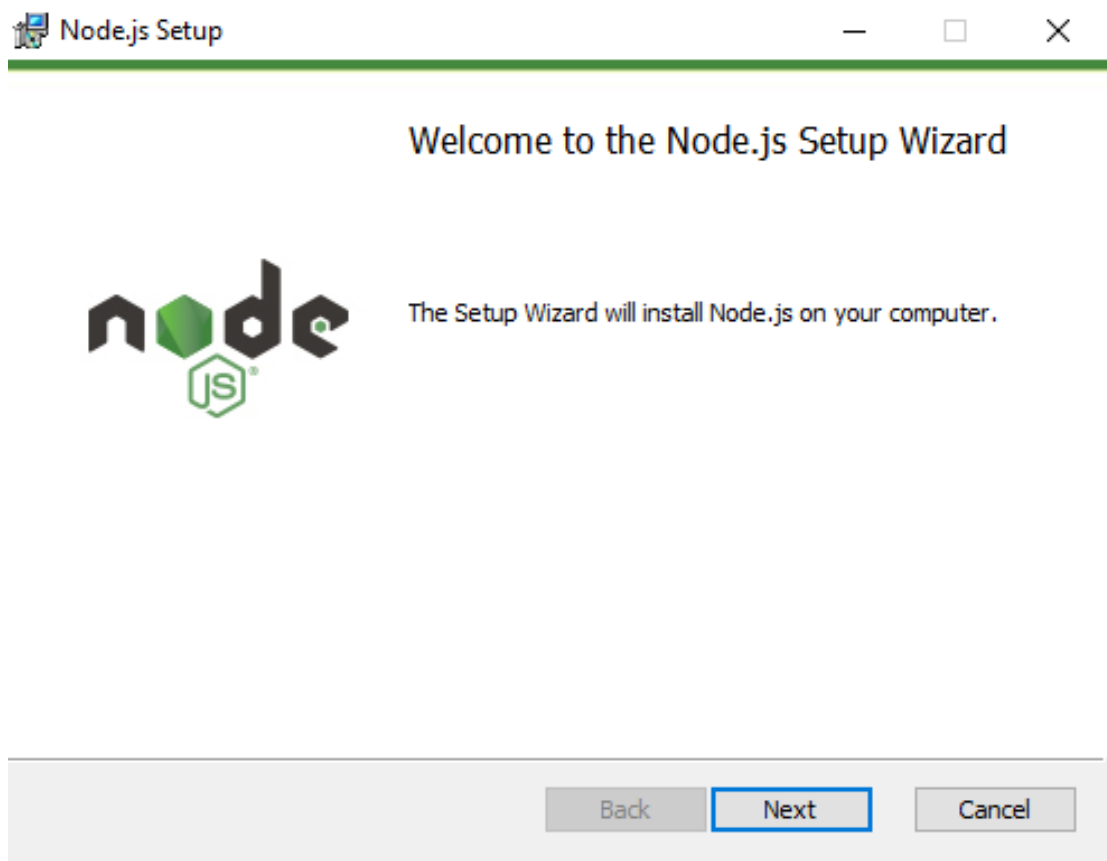
- Apsilankyti <https://nodejs.org>;
- Atsisiųsti LTS (Long Term Support) versiją;
- Įdiegti sistemą.

Node.js reikalingas:

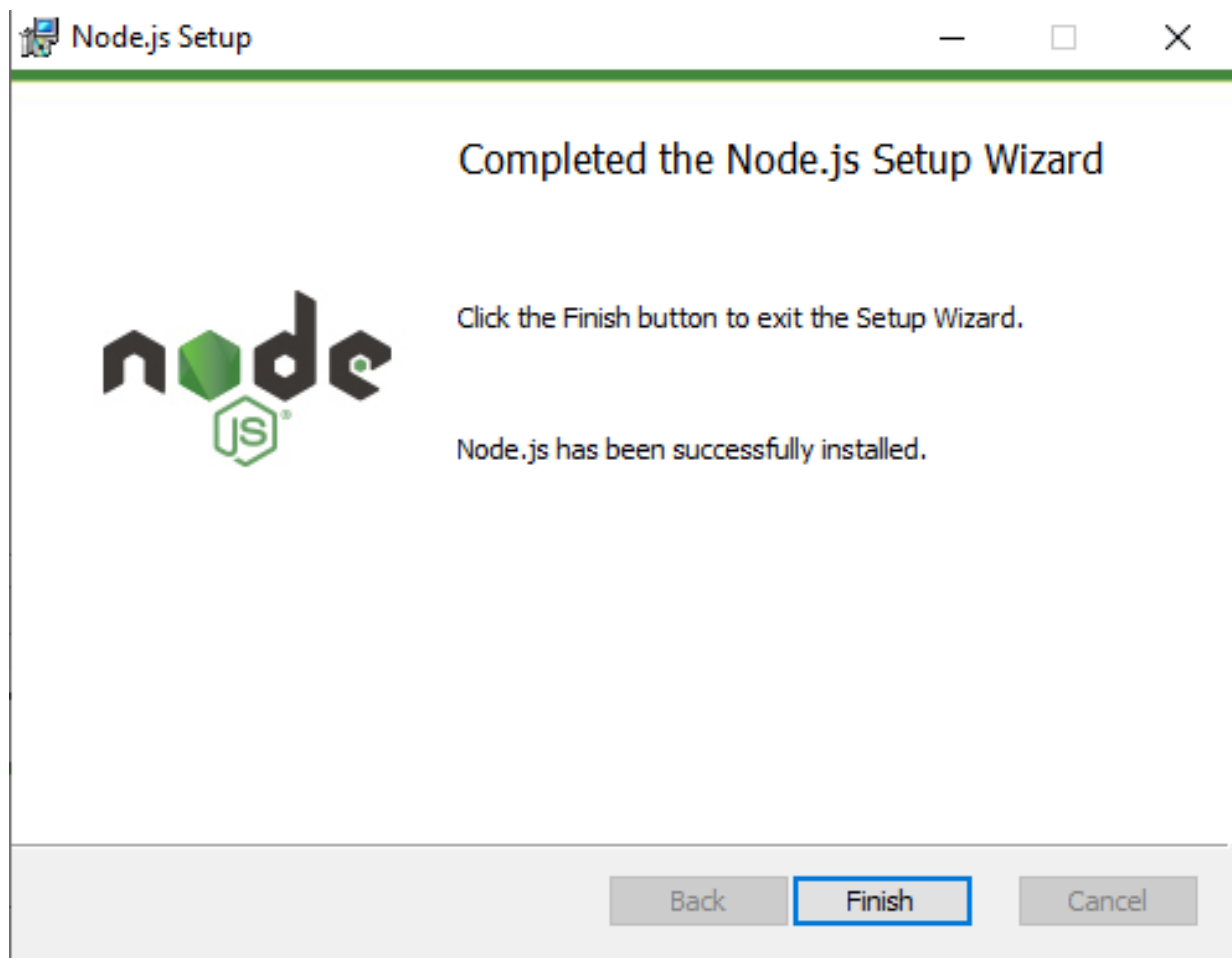
- paketų valdymui (npm);
- projekto paleidimui lokaliai;
- kūrimo serveriui.



20 pav. „Node.js“ atsiuntimas



21 pav. „Node.js“ įdiegimas



22 pav. „Node.js“ įdiegimas baigtas

Supabase konfigūravimas

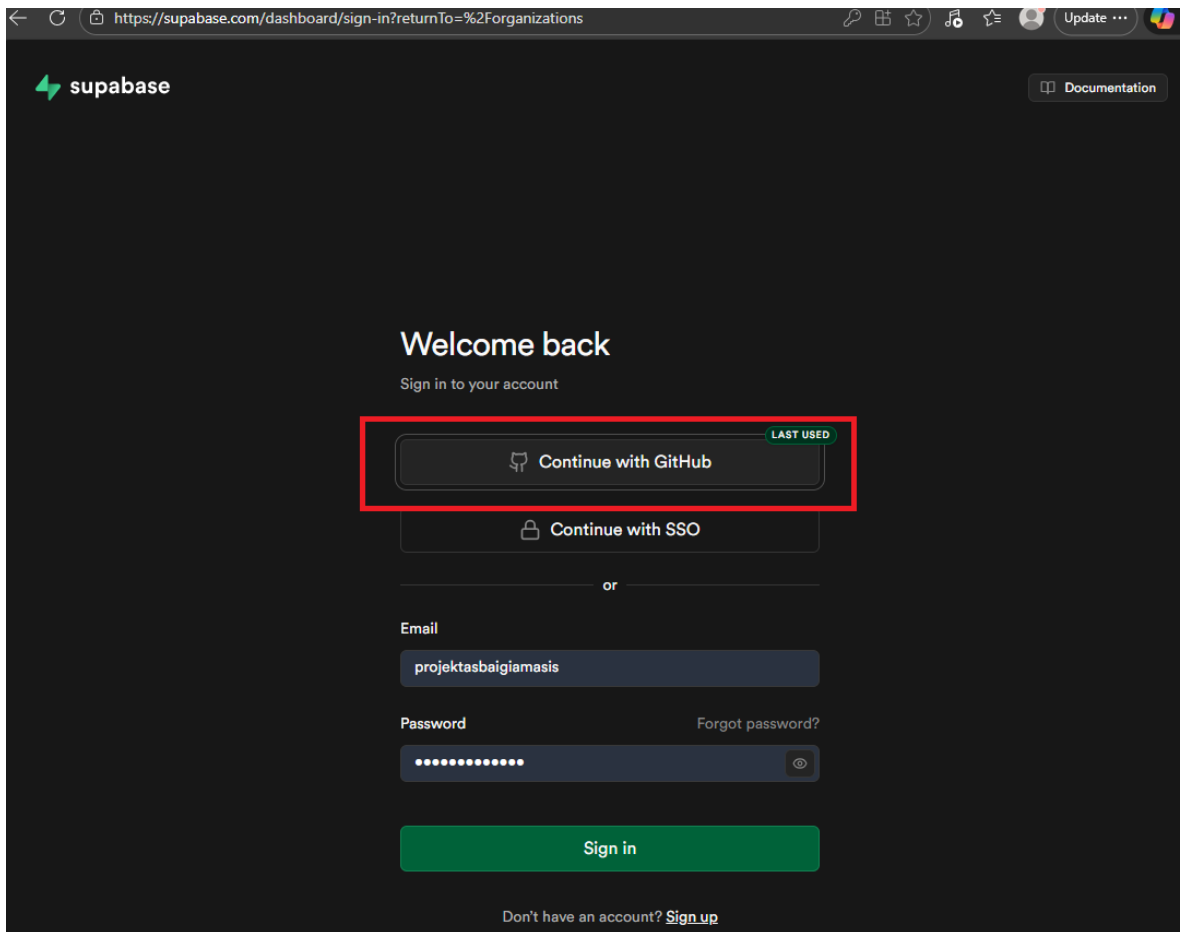
Toliau kuriama duomenų bazės ir autentifikacijos infrastruktūra naudojant Supabase.

Veiksmai:

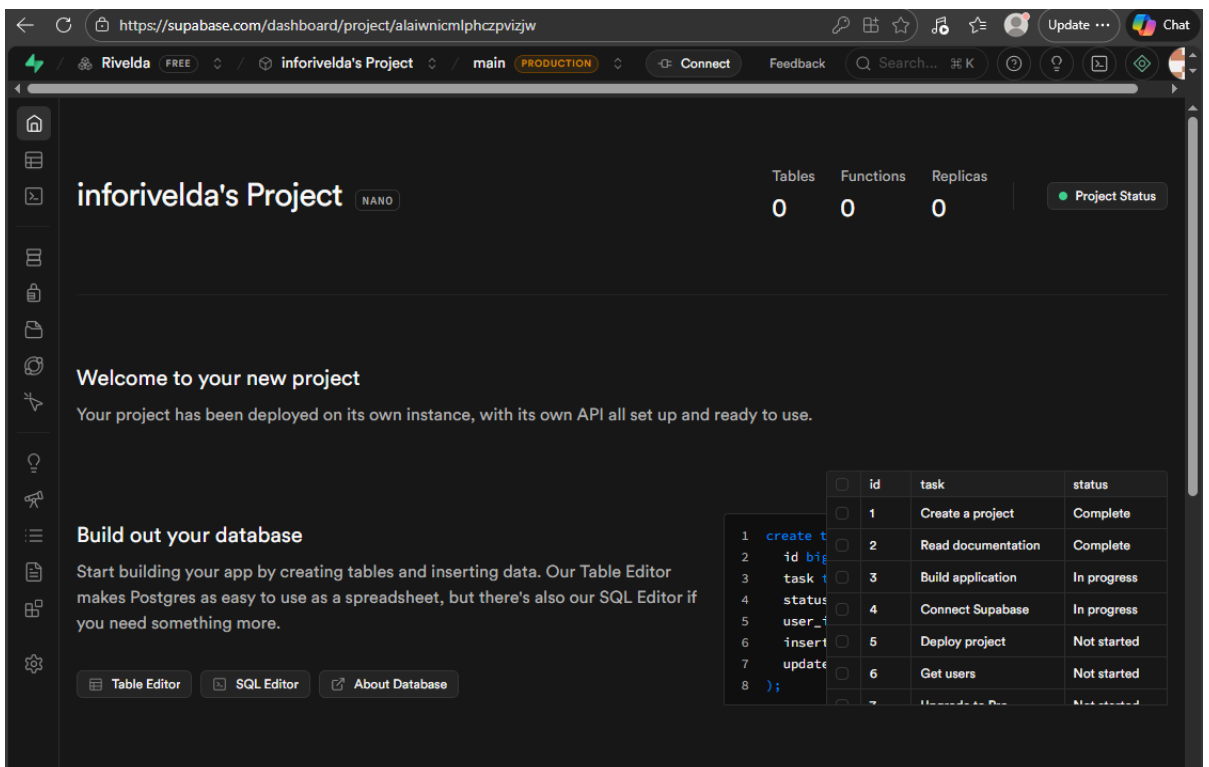
- Apsilankyti <https://supabase.com>;
- Pasirinkti Sign in with GitHub;
- Prisijungti naudojant jau sukurtą GitHub paskyrą;
- Nemokamame plane galima susikurti iki 2 projektų.

Supabase naudojamas:

- vartotojų autentifikacijai;
- duomenų bazei (kursai, pamokos, testai);
- vartotojų progresui saugoti.



23 pav. Prisijungimas prie „Supabase“



24 pav. Prisijunta prie „Supabase“

Vercel platformos naudojimas

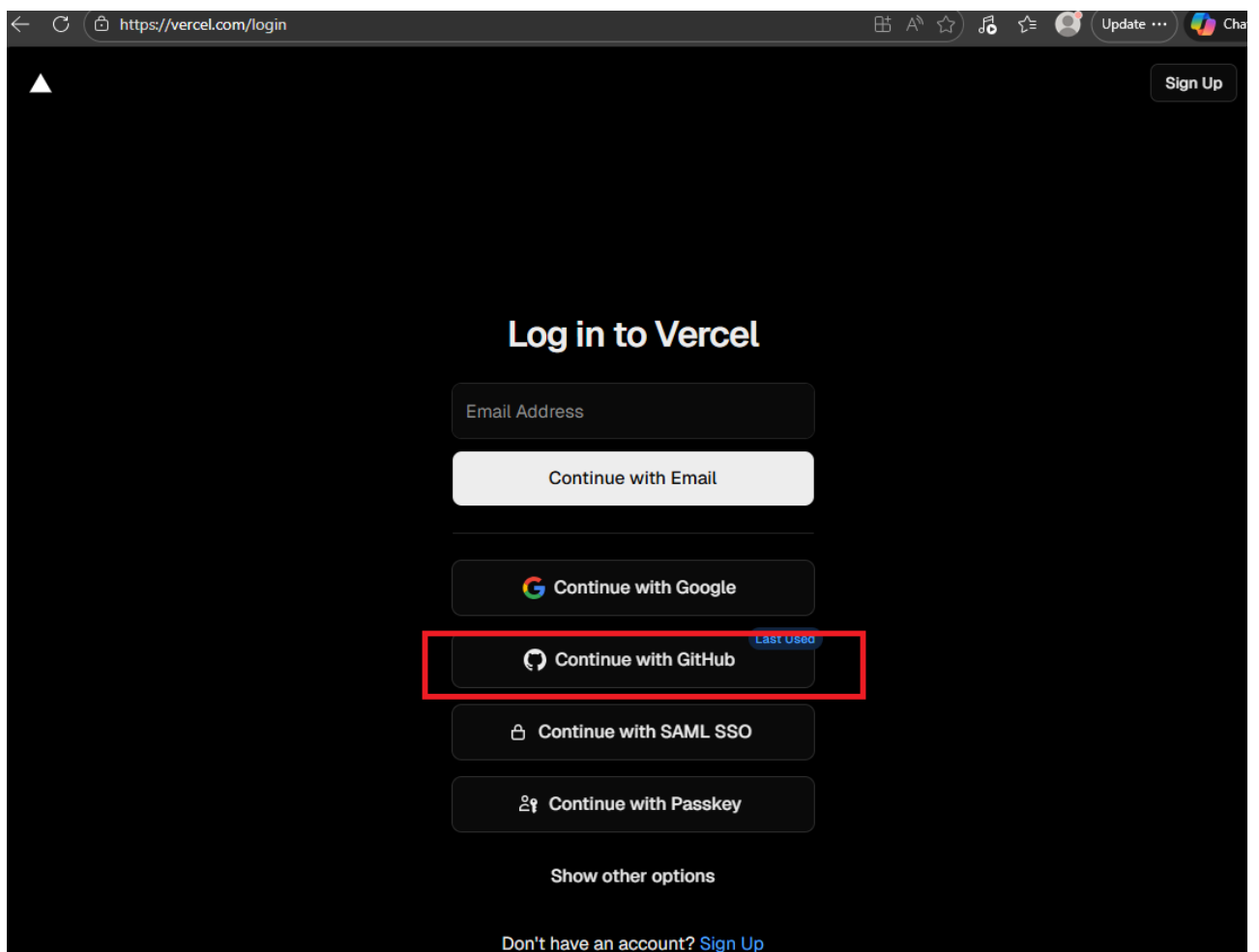
Projekto talpinimui (hostingui) naudojama Vercel platforma.

Veiksmai:

- Apsilankyti <https://vercel.com>;
- Prisijungti naudojant GitHub paskyrą;
- Leisti Vercel pasiekti GitHub repozitorijas.

Vercel automatiškai:

- diegia React aplikaciją;
- atnaujina ją po kiekvieno kodo pakeitimo;
- suteikia viešą URL.



25 pav. Prisijunta prie „Vercel“

Programavimo aplinkos parengimas

Efektyviam darbui pasirenkamas dirbtinio intelekto palaikomas kodo redaktorius (šiam projekte naudojamas Cursor).

Galimi variantai:

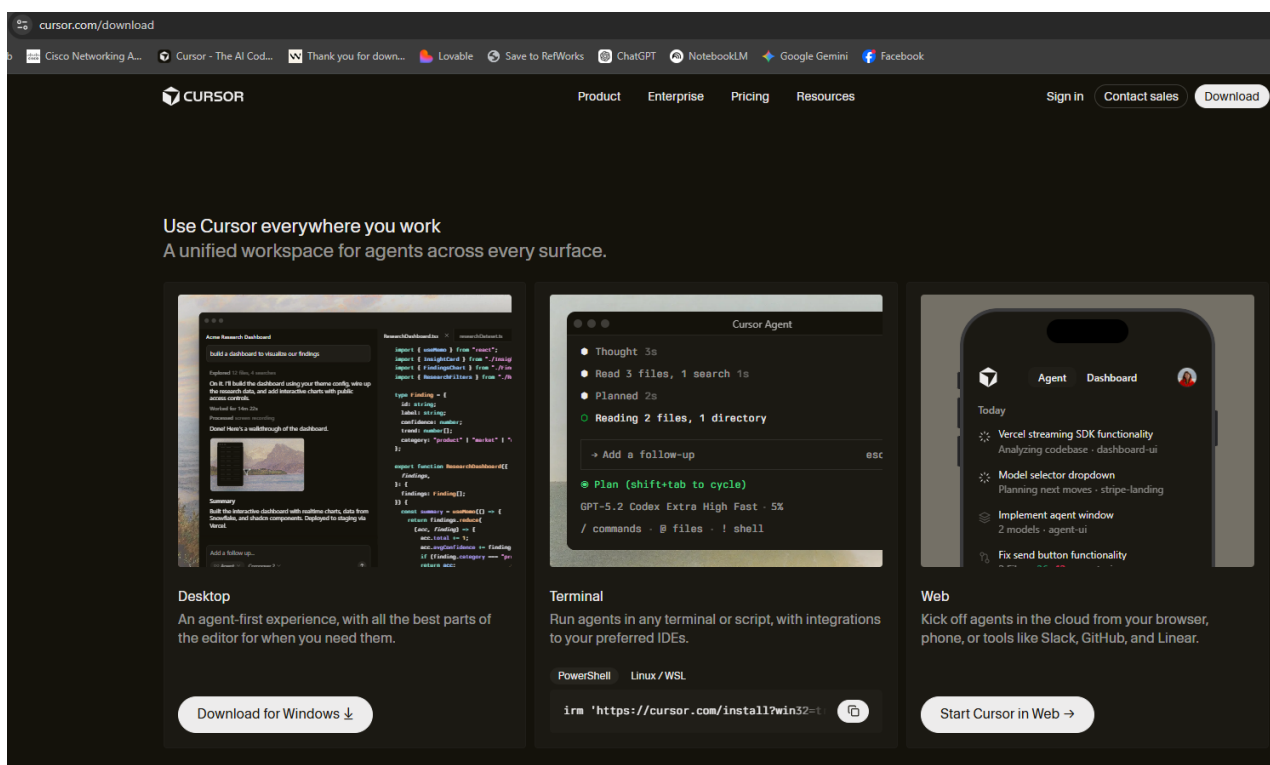
- Cursor AI;
- Windsurf.

Veiksmai:

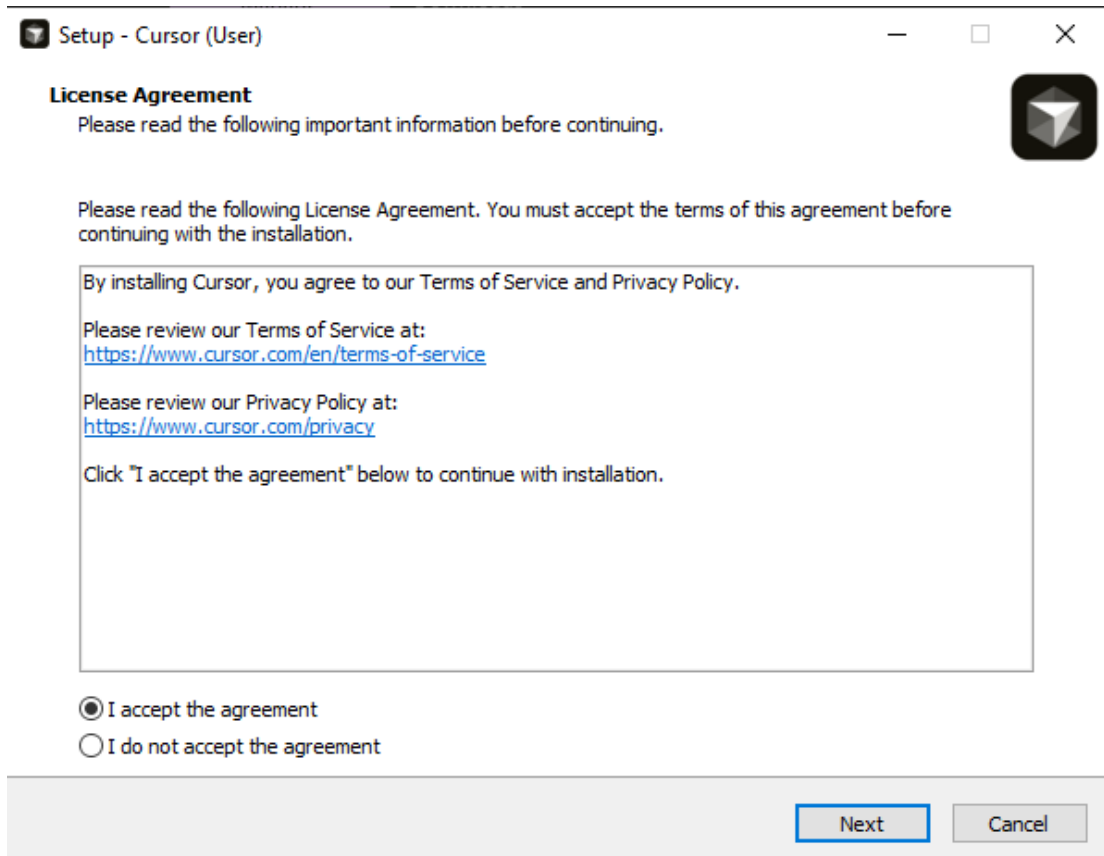
- Apsilankyti <https://www.cursor.com>;
- Atsisiųsti ir įsidiegti programą.

Šis redaktorius padeda:

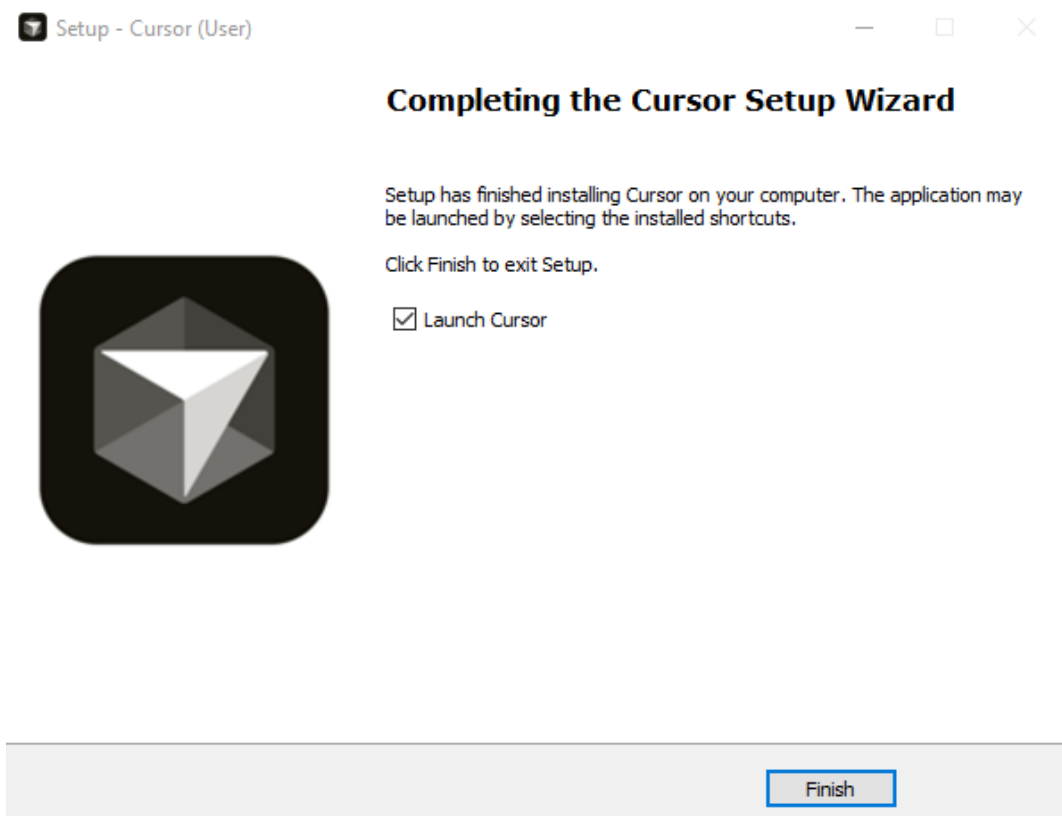
- Greičiau rašyti React kodą;
- Suprasti klaidas;
- Generuoti komponentus.



26 pav. „Cursor“ programos parsisiuntimas



27 pav. „Cursor“ įdiegimas



28 pav. „Cursor“ įdiegtas

2 priedas. DI įrankių naudojimas

Rengiant baigiamąjį magistro projektą buvo naudojami dirbtinio intelekto įrankiai, skirti teksto redagavimui, programinės įrangos kūrimo pagalbai. DI priemonės buvo naudojamos kaip pagalbiniai įrankiai, nepažeidžiant akademinio sąžiningumo principų.

DI įrankis	Panudojimo sritis	Pritaikymas projekte
Claude AI	PRD generavimas	Naudotas produkto reikalavimų dokumento struktūros ir funkcinių reikalavimų generavimui
Gemini	Vertimai	Atskirų sąsajos elementų ir terminų vertimas į anglų arba lietuvių kalbą
Cursor	Programinės įrangos kūrimas	Konsultacijos kuriant virtualiąją mokymosi aplinką: React, Supabase, autentifikacijos, duomenų bazės ir vartotojo sąsajos realizacijos klausimais
ChatGPT	Teksto redagavimas	Naudotas gramatinių, stilistinių ir struktūrinių teksto klaidų taisymui lietuvių kalba.

6 lentelė. Užklausa Claude AI:

Tu esi patyręs React programuotojas, specializuojantis modernių React aplikacijų kūrime.

Aš noriu sukurti kibernetinio saugumo ugdymo nuotoliniu būdu platformos (LMS) MVP. Svetainė skirta darbuotojų švietimui apie saugų elgesį internete, įskaitant el. pašto sukčiavimo (phishing) ir socialinės inžinerijos atakų atpažinimą, pasitelkiant interaktyvias pamokas, testus ir praktines užduotis.

Mano technologijų rinkinys: React, TypeScript, Vite, Supabase, Tailwind CSS, shadcn/ui komponentai. Projektas bus talpinamas Vercel platformoje.

Prašau parengti PRD pagal mano reikalavimus ir pateikti šio projekto MVP funkcionalumą „User Stories“ formatu.

Projektas turi turėti šias dalis:

- Bendrosios funkcijos
- Autentifikacija ir registracija (prisijungimas su „Google“ arba el. paštu)
- Mokymosi modulių peržiūra
- Forumas (kurti temas ir rašyti pranešimus gali tik prisijungę vartotojai)
- Žinučių funkcija (tik registruoti vartotojai gali siųsti privačias žinutes kitiems vartotojams)
- Testai ir praktinės užduotys
- Mokymosi progreso stebėjimas (vartotojai mato tik savo progresą, administratorius – visų vartotojų)
- Kursų kūrimas ir valdymas (prieinama tik administratoriams)
- Administratoriaus funkcijos
- Sertifikato išdavimas sėkmingai baigus galutinį kursą (tik prisijungusiems vartotojams)

Papildomas reikalavimas: sistema privalo turėti administratoriaus panelę (turinio valdymo modulį), kurioje prisijungęs administratorius galėtų patogiai kurti ir redaguoti kursus, pamokas, testus bei kitą turinį.

Užduok man klausimus, susijusius su šiuo kontekstu. Kiekvienam klausimui pateik sunumeruotus galimus atsakymų variantus su trumpomis rekomendacijomis. Gavęs mano atsakymus, pateik keletą PRD įgyvendinimo (implementacijos) variantų, iš kurių galėsiu pasirinkti tinkamiausią.

7 lentelė. Gautas Claude AI atsakymas:

Klausimai dėl kibernetinio saugumo LMS MVP

Sveiki! Puikus projektas. Norint parengti tikslų PRD, turiu kelias svarbias detales išsiaiškinti:

1. Turinio struktūra ir organizacija

Kaip bus organizuotas mokymosi turinys?

Paprastas hierarchinis - Kursas → Pamokos → Turinys (paprasčiausias, greičiausiai realizuojamas MVP)

Su moduliais - Kursas → Moduliai → Pamokos → Turinys (lanksčiau grupuoti turinį)

Su sekų valdymu - Kursas → Pamokos su priklausomybėmis (reikia baigti A prieš pradėdant B)

Laisvas pasirinkimas - Vartotojas gali laisvai naršyti bet kokia tvarka

Rekomenduoju: (1) MVP etape, nes paprasčiausias įgyvendinti, o vėliau galima išplėsti

2. Testų ir užduočių tipai

Kokių tipų vertinimo užduotis planuojate?

Tik vieno pasirinkimo testai - Paprasčiausia realizuoti, automatinis vertinimas

Kelio pasirinkimo testai - Vienas teisingas iš kelių, automatinis vertinimas

Kelių teisingų atsakymų testai - Sudėtingiau vertinti, bet lankstesni

Praktiniai scenarijai - Vartotojas sprendžia situacijas (pvz., atpažinti phishing el. laišką), interaktyvus

Mišrus variantas - Skirtingose pamokose skirtingi tipai

Rekomenduoju: (2) MVP etape + (4) nes tai atitinka kibernetinio saugumo specifiką

3. Sertifikato reikalavimai

Kokie kriterijai sertifikatui gauti?

Tik galutinio testo išlaikymas - 80%+ teisingų atsakymų paskutiniame teste

Visų pamokų užbaigimas - Reikia peržiūrėti visas pamokas + išlaikyti testus

Bendras balų slenkstis - Surinkti X balų per visą kursą

Laiko reikalavimas - Užbaigti per tam tikrą laiką + išlaikyti testus

Rekomenduoju: (2) nes užtikrina, kad vartotojas tikrai pereina visą medžiagą

4. Forum funkcionalumas

Kokio lygio forumo funkcijas reikia MVP etape?

Bazinė - Kurti temas, rašyti komentarus, matyti sąrašą

Su kategorijomis - Temos sugrupuotos pagal kursus/modulius

Su moderavimu - Administratorius gali šalinti/redaguoti įrašus

Su reakcijomis - Like/helpful funkcionalumas, geriausių atsakymų žymėjimas

Rekomenduoju: (2) + (3) MVP etape, kad forumai būtų organizuoti ir saugūs

5. Privačių žinučių sistema

Kokio tipo žinučių sistema?

Paprasta vienas-vienam - Tiesioginės žinutės tarp dviejų vartotojų

Su pokalbių istorija - Išsaugomi pokalbiai, galima grįžti

Real-time su pranešimais - WebSocket/realtime atnaujinimai

Tik administratorius → vartotojas - Palaikymo tikslais (paprasčiausias)

Rekomenduoju: (2) MVP etape (be real-time), naudojant Supabase Realtime vėliau galima išplėsti

6. Mokymosi progreso detalizacija

Ką tiksliai rodo progreso sekimas?

Bazinis - Užbaigtų pamokų %, užbaigti testai

Detalus - Pamokų %, testų balai, sugaištas laikas

Su analytics - Silpnos vietos, pakartotinai žiūrėtos pamokos, progreso istorija

Su lyginamąja statistika - Vartotojo progresą palyginti su vidurkiu

Rekomenduoju: (2) MVP etape - pakankamai informatyvus, nesudėtingas realizuoti

7. Turinio tipai pamokose

Kokio formato bus pamokų turinys?

Tik tekstas ir paveikslėliai - Paprasčiausias variantas

Tekstas + įterpti video (YouTube/Vimeo) - Įprastas LMS būdas

Interaktyvus turinys - Quiz'ai pamokų viduje, interaktyvūs scenarijai

Mišrus - Skirtingose pamokose skirtingi formatai

Rekomenduoju: (4) bet MVP pradžiai (2), nes video efektyvus mokymuisi

8. Administratoriaus turinio valdymas

Kokio tipo redaktorius turinio kūrimui?

Paprastos formos - Textarea su Markdown palaikymu

WYSIWYG redaktorius - Rich text editor (Tiptap/Quill)

Blokų redaktorius - Kaip Notion, komponuojami turinio blokai

JSON schema forma - Techningesnis, bet lankstesnis

Rekomenduoju: (2) MVP etape - intuityvus administratoriams, nereikia mokytis Markdown

9. Vartotojų rolės

Kokias vartotojų roles numatote sistemoje?

Tik 2 rolės - Vartotojas ir Administratorius (paprasčiausias)

3 rolės - Vartotojas, Moderatorius (forumo), Administratorius

4+ rolės - + Instruktorius (kuria kursus), Organizacijos vadovas (mato savo komandos progresą)

Dinaminės teisės - Lanksčiai priskiriamos teisės per admin panelę

Rekomenduoju: (1) MVP etape, vėliau galima išplėsti iki (3)

10. Supabase architektūra

Kaip planuojate naudoti Supabase funkcionalumą?

Tik Auth + Database - Baziniai poreikiai

+ Storage - Paveikslėlių, video failų, sertifikatų saugojimas

+ Realtime - Live updates forumuose, žinutėse

+ Edge Functions - Serverless funkcijos sertifikatų generavimui, email pranešimams

Rekomenduoju: (2) MVP etape + (4) sertifikatams, (3) pridėti vėlesnėse versijose

Prašau atsakyti į kiekvieną klausimą pasirinkdami skaičių (pvz., "1: 1, 2: 2, 3: 2..." arba išsamiau aprašydami savo pageidavimus).

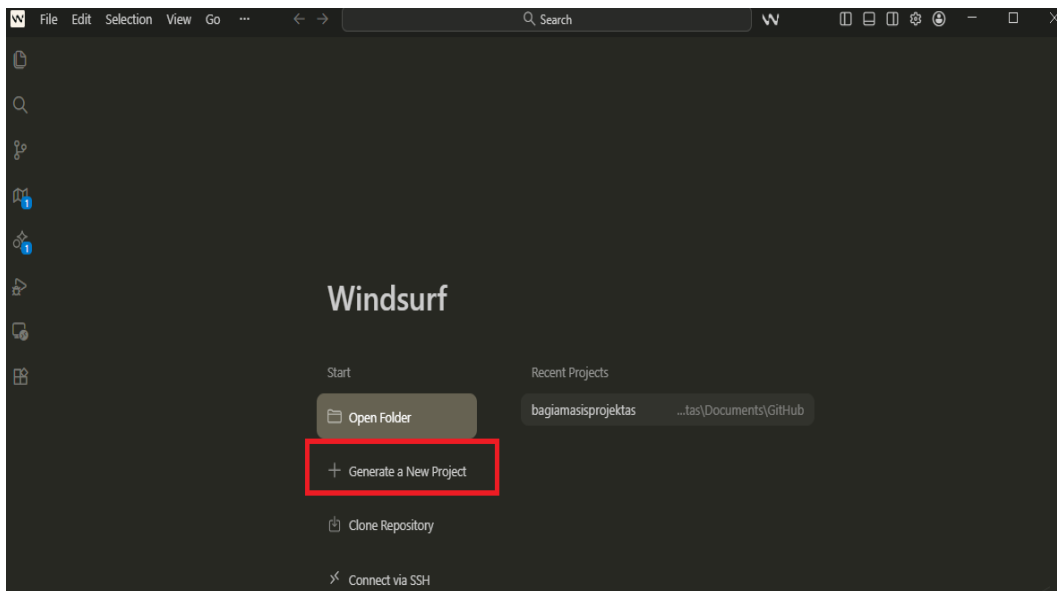
Gavęs jūsų atsakymus, parengsiu kelis skirtingus PRD įgyvendinimo variantus su aiškiais rekomendacijomis MVP etapui!

8 lentelė. Pateiktas atsakymas Claude AI:

1: 1, 2: 2, 3: 1 70%, 4: 1 2 3 4, 5: 1 2, 6: 2, 7: 1 4, 8: 2, 9: 1, 10: 1 2 3 4

3 priedas. Sistemos realizacijos fragmentai

Parengus PRD dokumentą mokymosi valdymo sistemai, pereinama prie projekto kūrimo etapo. Šiame etape atidaroma „Cursor“ kūrimo aplinka ir sukuriamas naujas projektas.



29 pav. Sukuriame naują projektą.

```
1 # PRD - Mokymosi Valdymo Sistema (LMS)
11 ## 2. FUNKCINIAI REIKALAVIMAI
13 ### 2.1 Vartotojų Rolės
15 #### 2.1.1 Administratorius
20
21 #### 2.1.2 Dėstytojas
22 - Kurso turinio kūrimas
23 - Testų sudarymas
24 - Studentų pažangos stebėjimas
25 - Atsiliepimų suteikimas
26
27 #### 2.1.3 Studentas
28 - Kursų peržiūra
29 - Užduočių atlikimas
30 - Testų laikymas
31 - Pažangos stebėjimas
32
33 ## 3. SISTEMOS FUNKCIONALUMAS
34
35 ### 3.1 Vartotojo Valdymas
36 - Registracija ir prisijungimas
37 - Profilio valdymas
38 - Slaptažodžio atkūrimas
39 - El. pašto patvirtinimas
40
41 ### 3.2 Kursų Valdymas
42 - Kurso kūrimas ir redagavimas
43 - Pamokų struktūros kūrimas
44 - Medžiagos įkėlimas
45 - Prieigos teisių valdymas
46
47 ### 3.3 Testavimo Sistemos Reikalavimai
48 - Testų kūrimas
49 - Automatinis vertinimas
50 - Išsamūs rezultatų ataskaitos
51 - Testų laikymo stebėjimas
52
53 ## 4. TECHNINĖ ARCHITEKTŪRA
54
55 ### 4.1 Technologijų Rinkinys
56
57 **Frontend:**
58 - React 18+ su TypeScript
```

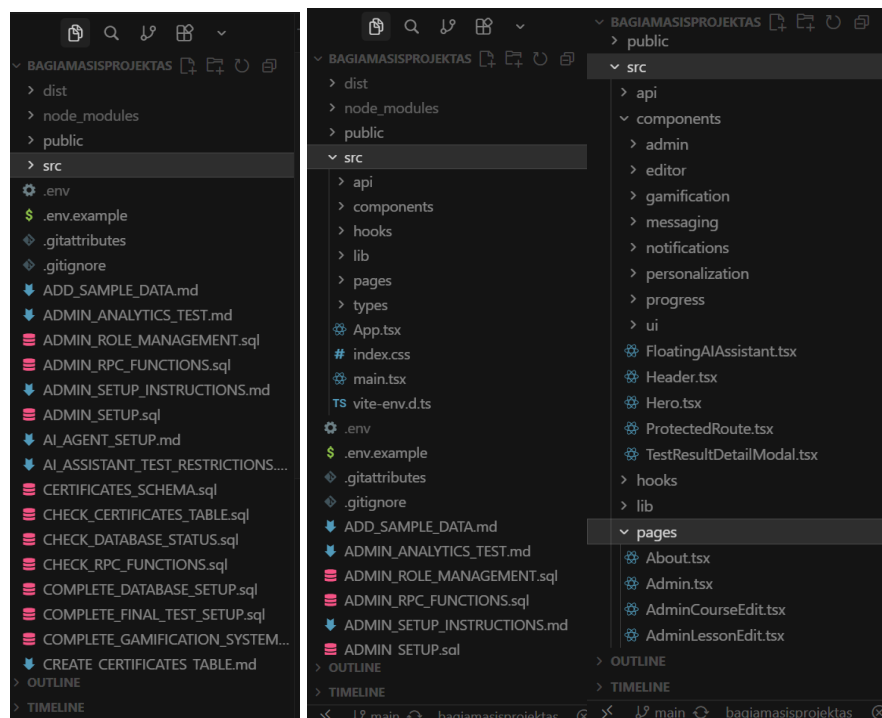
30 pav. PRD įkėlimas į „Cursor“

```

1 # Mokymosi valdymo sistemos (LMS) užduočių sąrašas
70 ## Užduočių sąrašas
75
76 ### 1.0 Vartotojų autentifikavimas ir autorizavimas
77
78 - [x] 1.1 Vartotojo registracijos ir prisijungimo sistemos sukūrimas
79 - [x] Sukurti registracijos formą su privalomais laukais
80 - [x] Įdiegti el. pašto patvirtinimo srautą
81 - [x] Sukurti prisijungimo formą su "prisiminti mane" funkcija
82 - [x] Įdiegti Google prisijungimą
83
84 - [x] 1.2 Rolės pagrįstos prieigos valdymas
85 - [x] Apibrėžti vartotojų roles (administratorius, dėstytojas, studentas)
86 - [x] Sukurti apsaugos taisykles kiekvienai rolei
87 - [x] Įdiegti maršrutų apsaugą pagal roles
88
89 - [ ] 1.3 Slaptažodžio atkūrimo funkcionalumas
90 - [x] Sukurti slaptažodžio atkūrimo formą
91 - [x] Įdiegti saugų atkūrimo nuorodų siuntimą el. paštu
92 - [x] Sukurti slaptažodžio atnaujinimo formą
93
94 - [x] 1.4 El. pašto patvirtinimas
95 - [x] Sukurti el. laiškų šablonus
96 - [x] Įdiegti patvirtinimo nuorodų generavimą
97 - [x] Sukurti patvirtinimo būsenos valdymą
98
99 [Visos likusios užduotys bus pateiktos toliau...]
100
101 ### 2.0 Kursų valdymo sistema
102 - [x] 2.1 Kurso kūrimo ir redagavimo sąsajos kūrimas
103 - [x] 2.2 Pamokų struktūros kūrimo įrankis
104 - [x] 2.3 Medžiagos įkėlimo funkcionalumas
105 - [x] 2.4 Kursų užsirašymo sistema
106
107 ### 3.0 Testavimo ir vertinimo modulis
108 - [x] 3.1 Testų kūrimo sąsaja
109 - [x] 3.2 Automatinis testų vertinimas
110 - [x] 3.3 Rezultatų analizės ir ataskaitų sistema
111 - [x] 3.4 Testų stebėjimo ir saugumo funkcijos
112
113 ### 4.0 Vartotojo skydelis ir pažangos stebėjimas
114 - [x] 4.1 Studento pažangos stebėjimas
115 - [x] 4.2 Dėstytojo mokinių stebėsenos įrankis

```

31 pav. Užduočių ir subužduočių planas

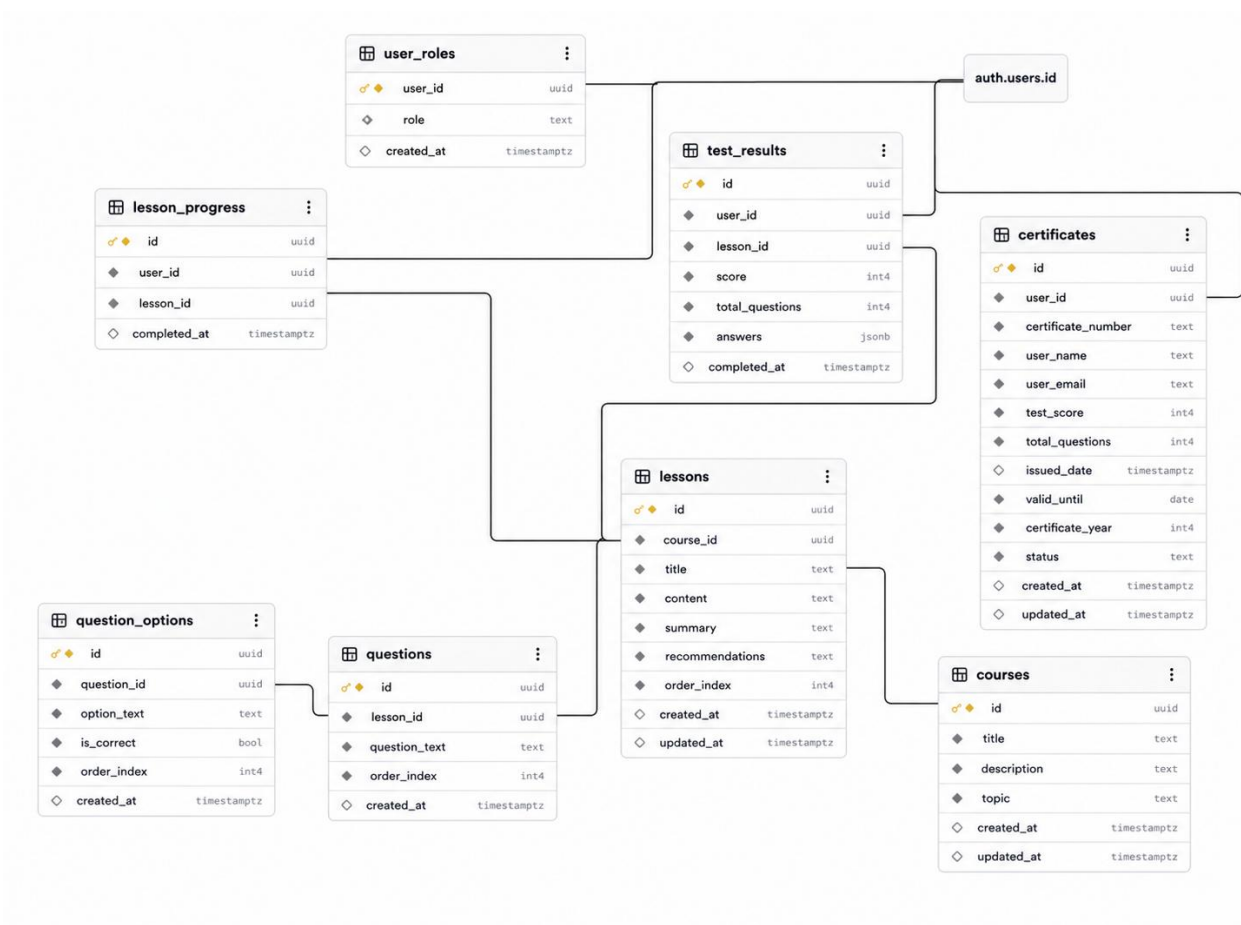


32 pav. Projekto failų struktūra integruotoje programavimo aplinkoje

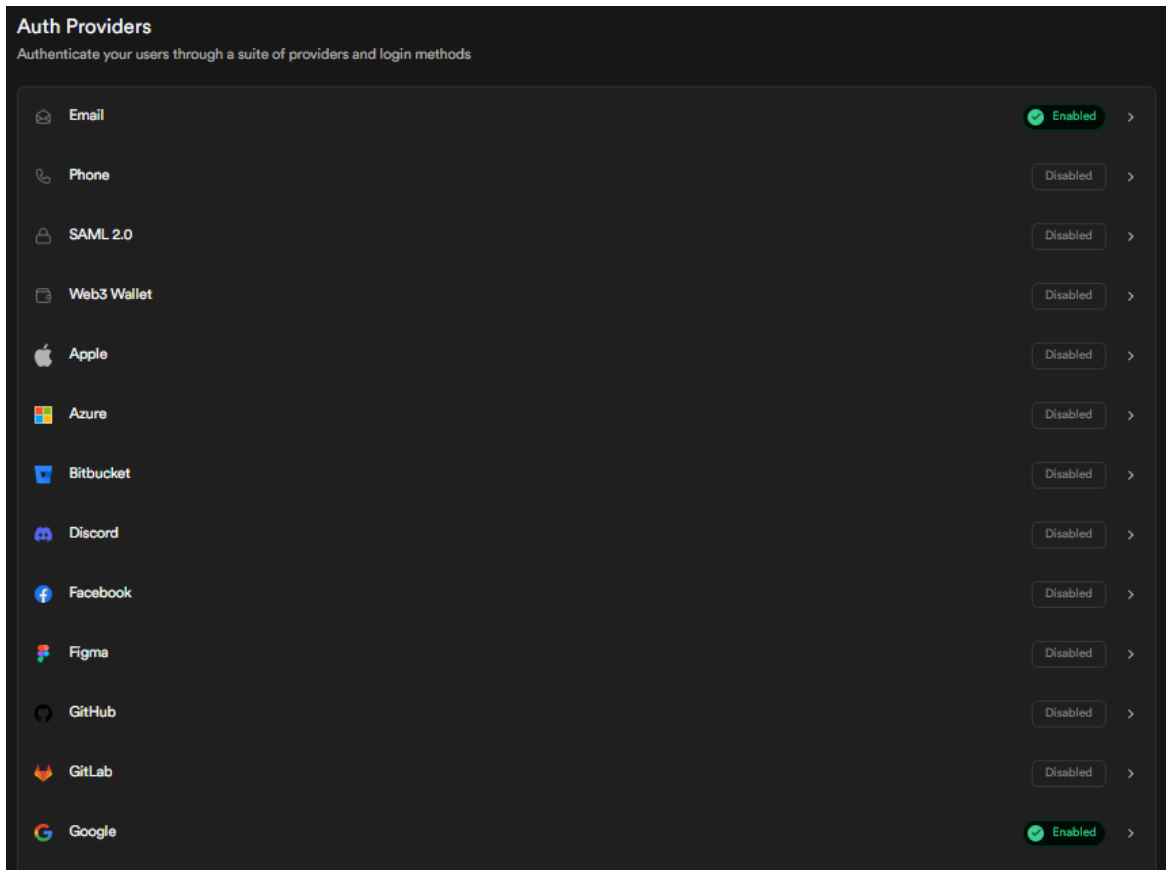
NAME	COLUMNS	ROWS (ESTIMATED)	SIZE (ESTIMATED)	REALTIME
certificates	13	5	112 kB	× Disabled
courses	6	4	32 kB	× Disabled
it_knowledge_base	14	2	128 kB	× Disabled
it_knowledge_categories	7	12	48 kB	× Disabled
learning_sessions	17	25	128 kB	× Disabled
lesson_progress	4	15	40 kB	× Disabled
lessons	9	12	16 MB	× Disabled
messages	13	7	96 kB	× Disabled
notifications	10	0	32 kB	× Disabled
profiles	6	1	48 kB	× Disabled
question_options	6	462	256 kB	× Disabled
questions	5	114	832 kB	× Disabled
test_results	7	25	160 kB	× Disabled
user_preferences	7	0	16 kB	× Disabled
user_roles	3	1	32 kB	× Disabled
user_stats	13	0	16 kB	× Disabled
visitors	13	53	80 kB	× Disabled

77 tables

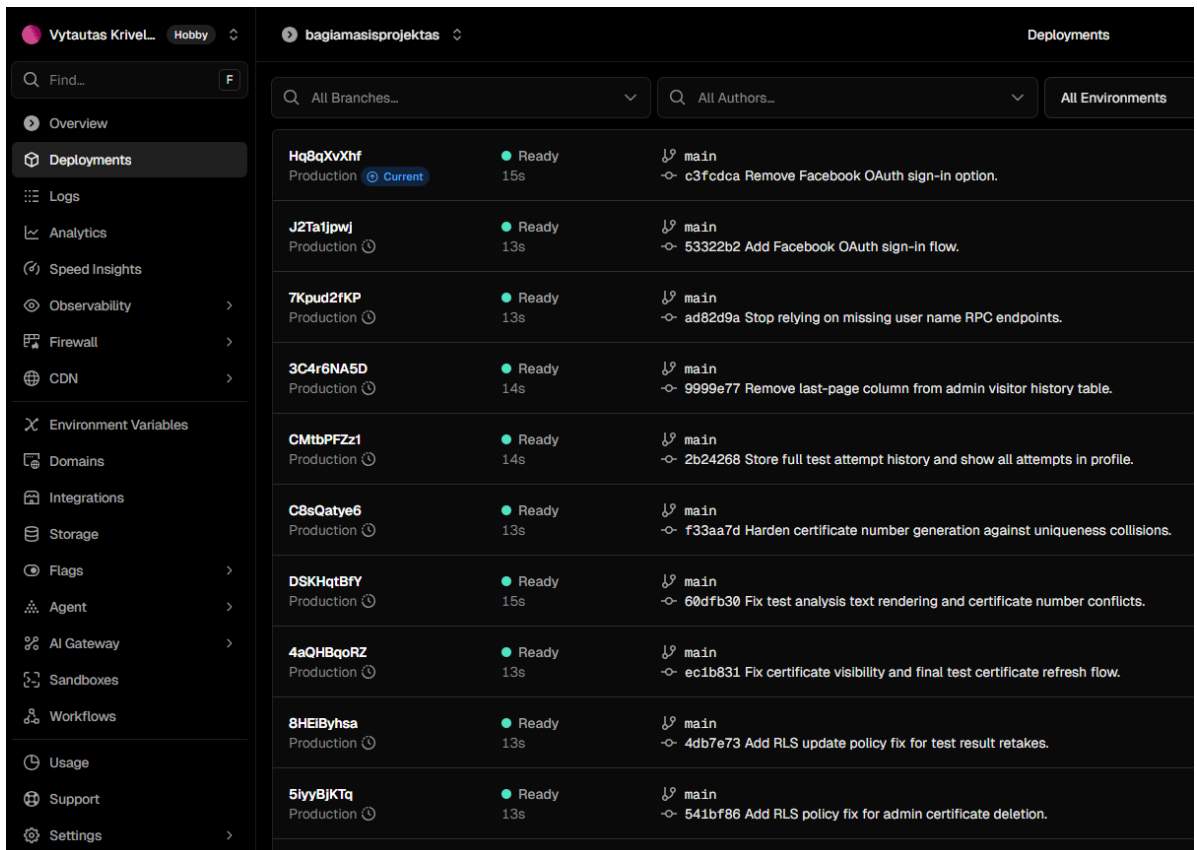
33 pav. Duomenų bazės lentelių sąrašas „Supabase“ aplinkoje




34 pav. Kursų duomenų bazės lentelių ir jų tarpusavio ryšių diagrama



35 pav. „Supabase“ įgalintos prisijungimo funkcijos




36 pav. Sistemos publikavimo ir versijavimo procesas


Kibernetinio saugumo įgūdžių mokymas
 Prisijunkite arba užsiregistruokite, kad galėtumėte mokytis

El. paštas

Slaptažodis [Pamiršote slaptažodį?](#)

ARBA



37 pav. Prisijungimo langas su el. paštu arba „google“

[Pagrindinis](#) [Kursai](#) [Forumai](#) [Apie mus](#)

[Žinutės](#) [Profilis](#) [Atsijungti](#)

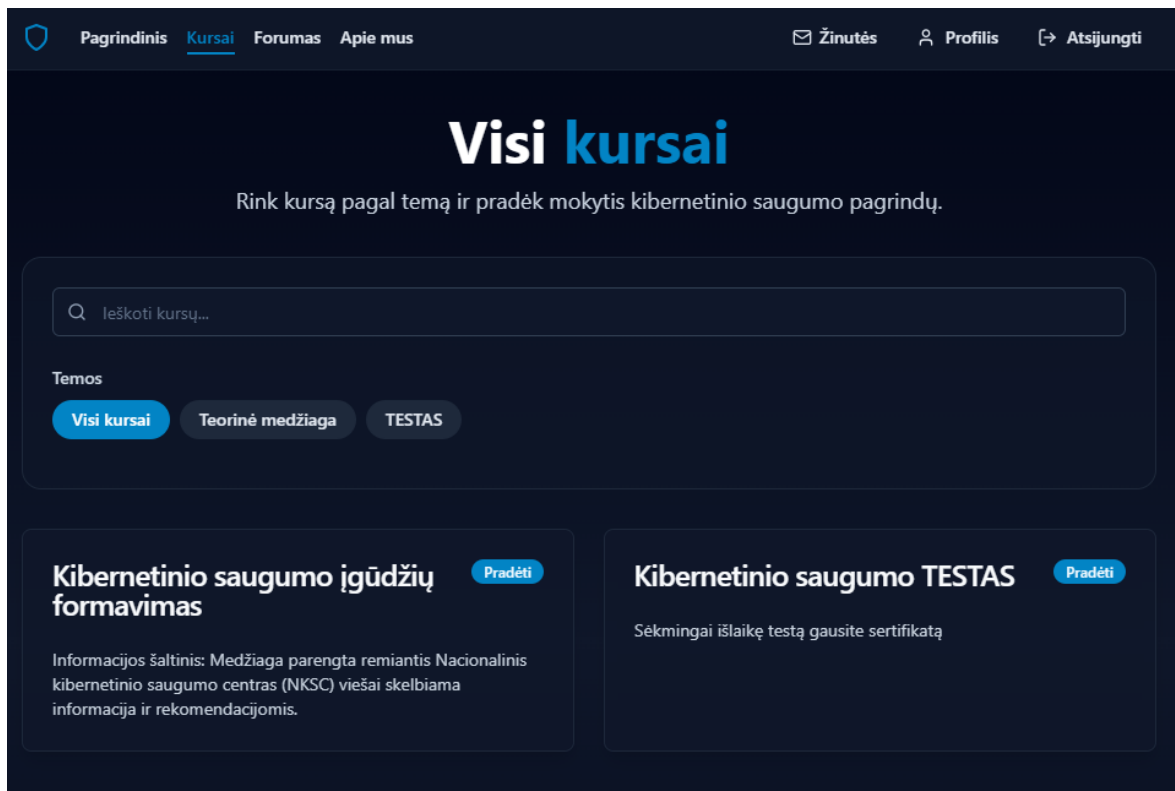
☆ Nemokama mokymosi platforma

Tapk saugesniu internete jau šiandien

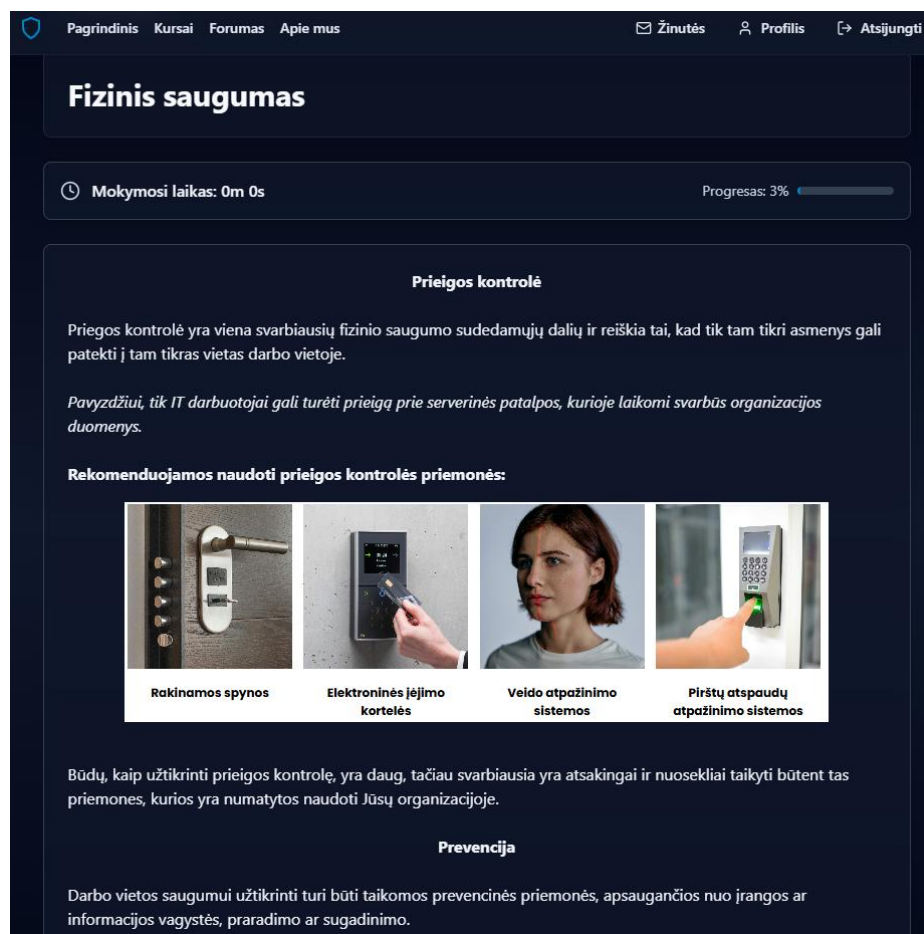
Interaktyvūs kursai, praktinės užduotys ir testai padės išmokti atpažinti grėsmes ir apsaugoti savo duomenis nuo kibernetinių atakų.

<p style="font-size: small;">DABAR (JŪSŲ LAIKAS)</p> <p>2026 m. balandžio 28 d., antradienis</p> <p style="font-size: large; font-weight: bold;">16:00:51</p>	<p style="font-size: small;">UNIKALŪS LANKYTOJAI</p> <p style="font-size: large; font-weight: bold;">53</p>
---	---

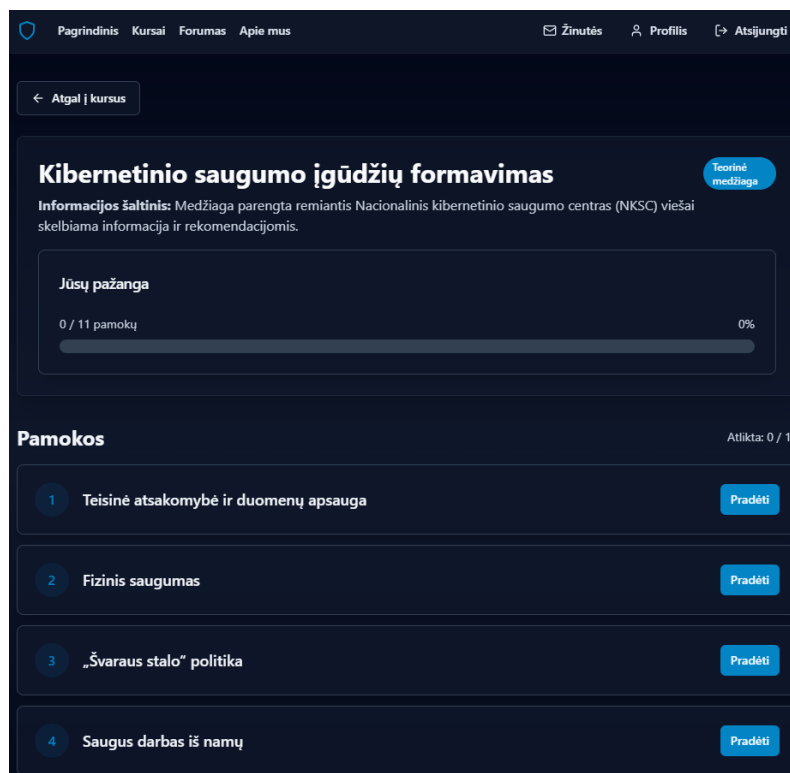
38 pav. Pagrindinio puslapio vaizdas prisijungus vartotojui



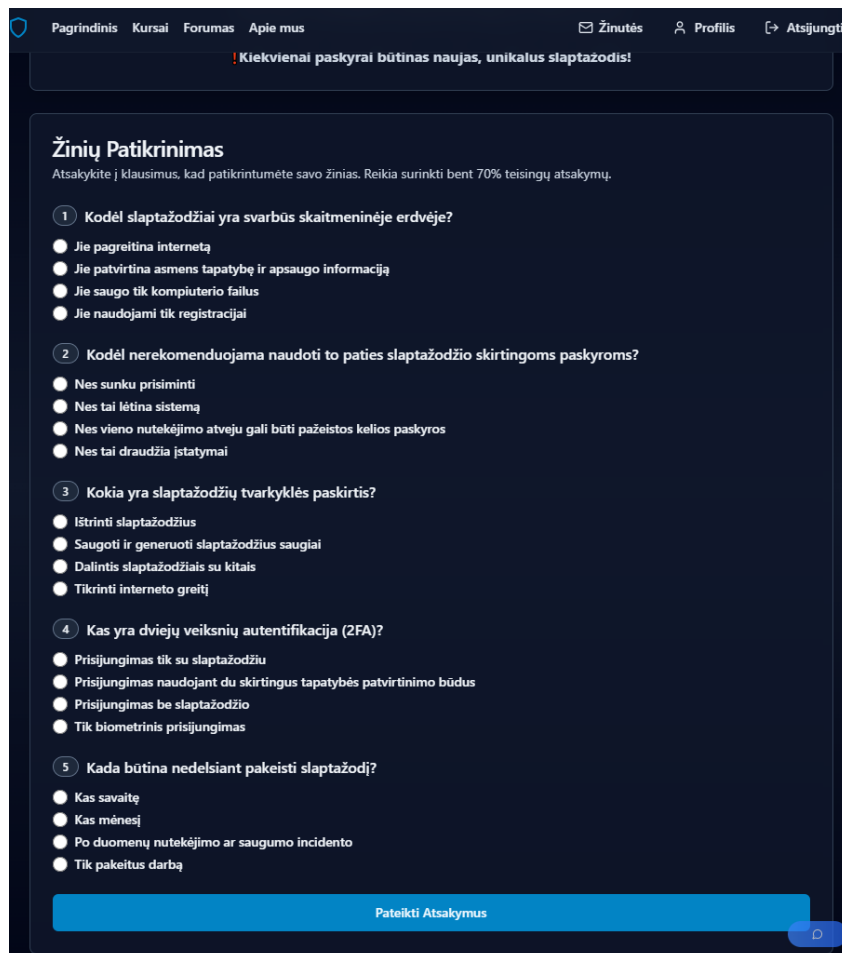
39 pav. Mokymosi platformos kursų peržiūros ir pasirinkimo puslapis



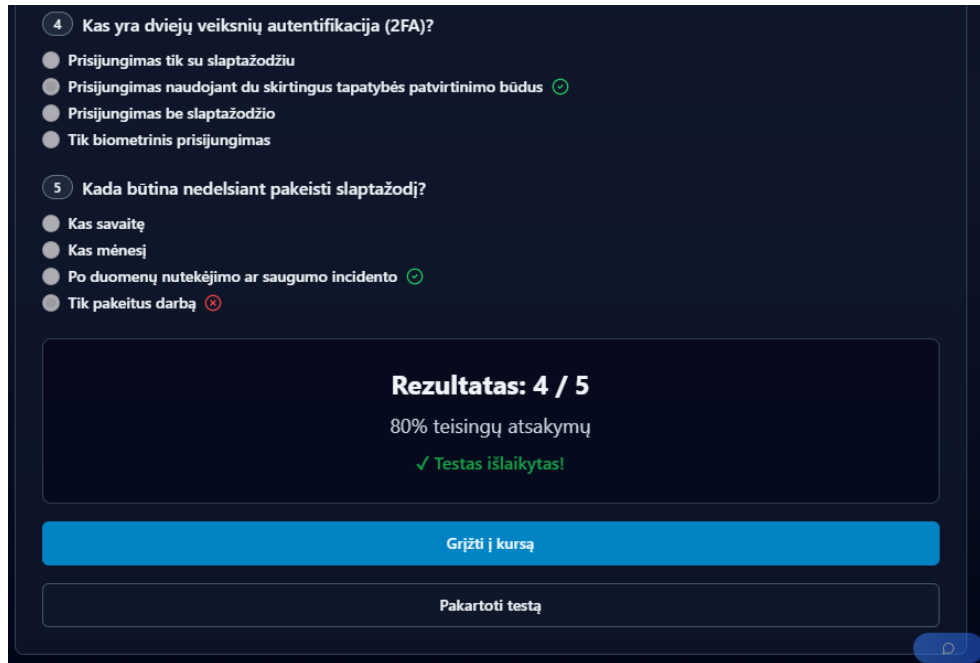
40 pav. Pamokos mokomosios medžiagos pateikimo puslapis



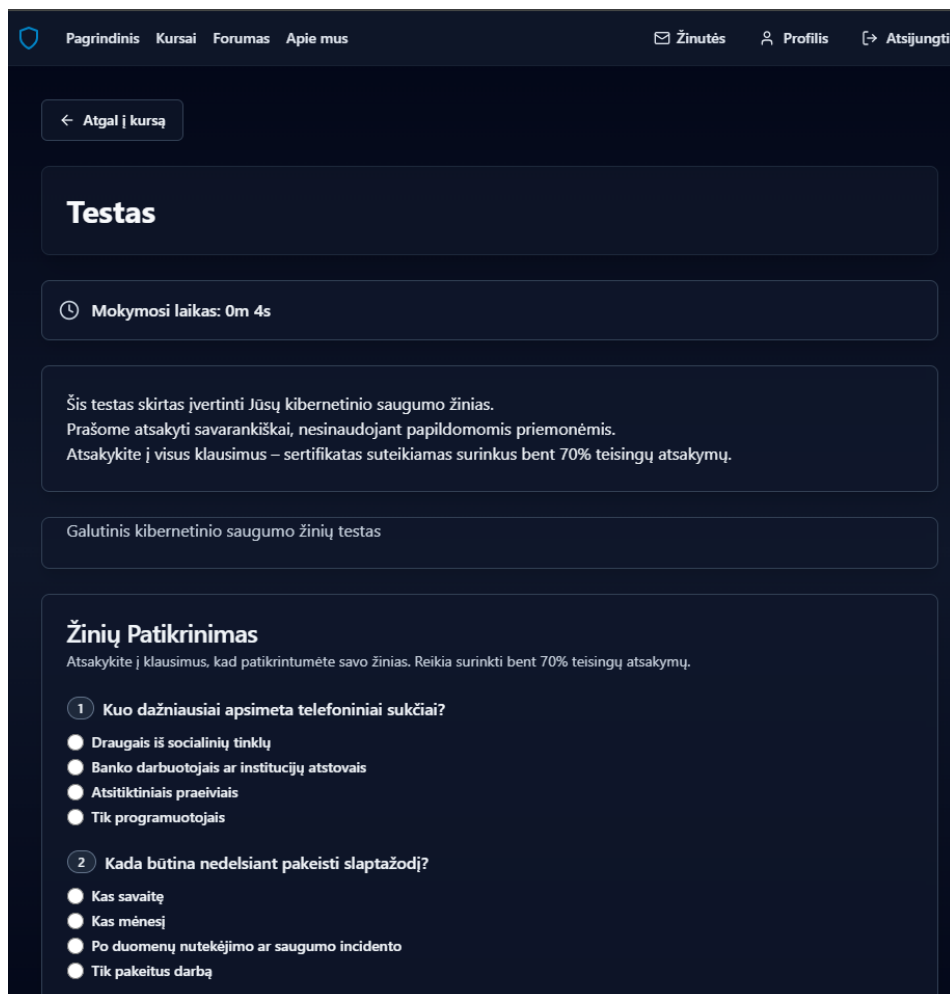
41 pav. Kurso peržiūros puslapis su pamokų sąrašu



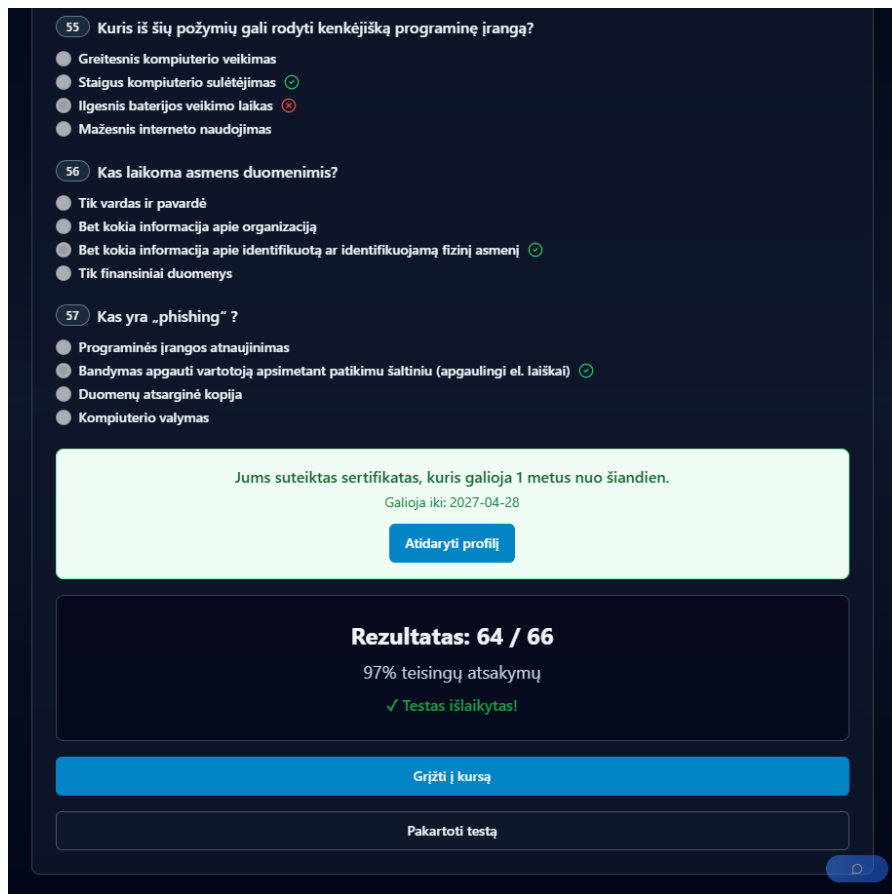
42 pav. Pamokos žinių patikrinimo (testo) puslapis



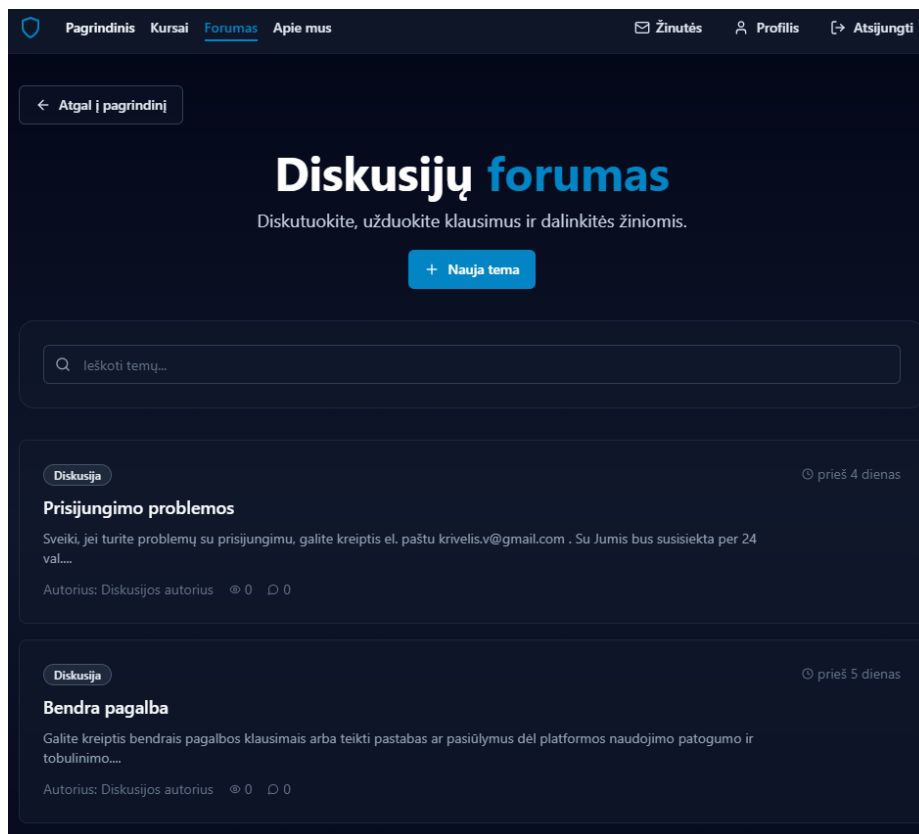
43 pav. Žinių patikrinimo (testo) rezultatų puslapis



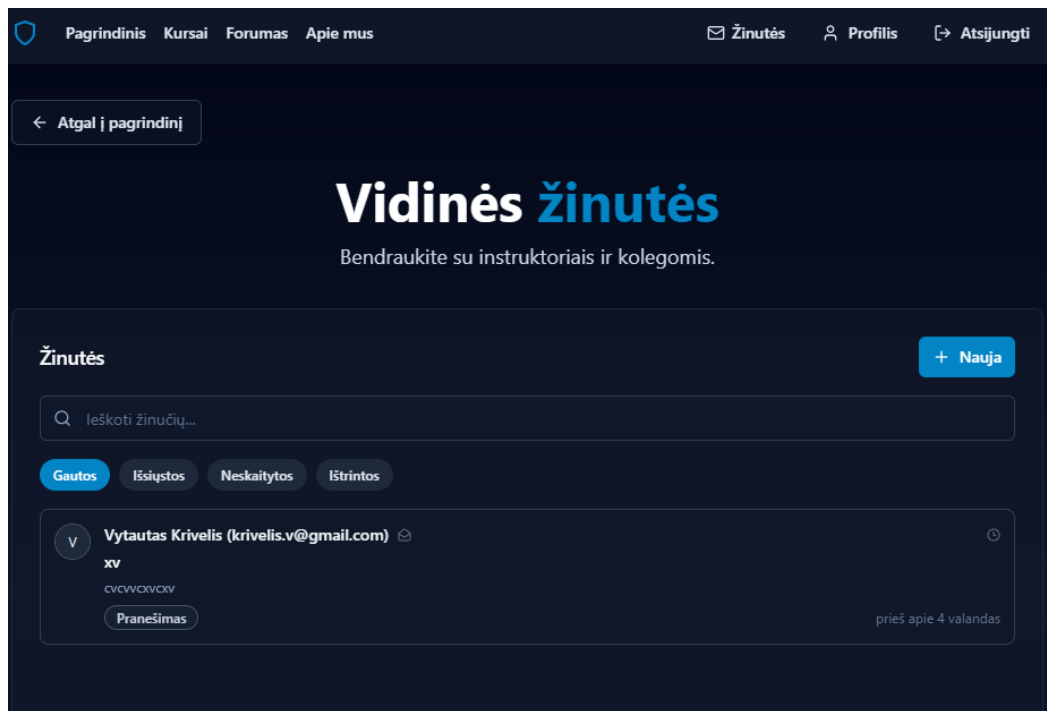
44 pav. Galutinio kibernetinio saugumo žinių patikrinimo testo puslapis



45 pav. Galutinio žinių patikrinimo testo rezultatai ir sertifikato suteikimas



46 pav. Diskusijų forumo puslapis mokymosi platformoje



47 pav. Vidinių žinučių (pranešimų) sistemos puslapis



48 pav. Vartotojo profilio puslapis su mokymosi pažanga ir sertifikatais

Mano sertifikatai

Sertifikato Nr.	Kas laikė sertifikatą?	Rezultatas	Išdavimo data	Galioja iki	Statusas
KS-2026-MOHCYVMM-866615	Vytautas	63 / 66 (95%)	2026-04-27	2027-04-27	Galiojantis Peržiūrėti

Testų istorija

Kursas	Pamoka	Rezultatas	Data	Klaidos
Kibernetinio saugumo TESTAS	Testas	64 / 66	2026-04-28 16:22	Analizė
Kibernetinio saugumo įgūdžių formavimas	Saugūs slaptažodžiai	4 / 5	2026-04-28 16:12	Analizė
Kibernetinio saugumo įgūdžių formavimas	Saugūs slaptažodžiai	5 / 5	2026-04-28 16:12	Analizė
Kibernetinio saugumo TESTAS	Testas	63 / 66	2026-04-27 18:34	Analizė

49 pav. Vartotojo testų istorijos ir sertifikatų peržiūros puslapis

Pagrindinis Kursai Forumas Apie mus
Žinutės Profilis Atsijungti

✔ Galiojantis

Sertifikato Nr. KS-2026-MOHCYVMM-866615

Patvirtinama, kad

Vytautas

info.rivelda@gmail.com

sėkmingai išlaikė kibernetinio saugumo mokymą

Testo rezultatai

63/66

Teisingi atsakymai

95%

Galutinis rezultatas

📅 Išdavimo data

2026-04-27

📅 Galioja iki

2027-04-27

📄 Tikrinimo kodas

Skenuokite tikrinimui

Šis sertifikatas patvirtina, kad darbuotojas turi pakankamas žinias kibernetinio saugumo srityje ir gali saugiai dirbti su organizacijos informacinėmis sistemomis.

Sertifikatas galioja 12 mėnesių nuo išdavimo dienos

Po galiojimo pabaigos reikės perlaikyti galutinį testą

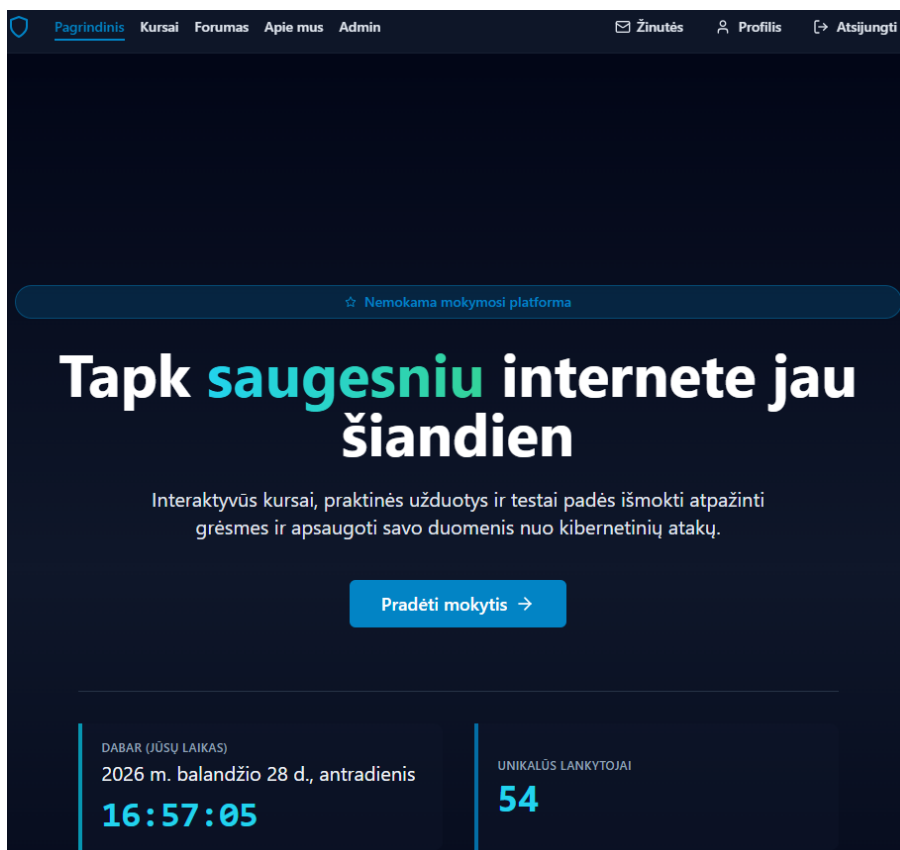
⬇️ Atsisiųsti sertifikatą

Grįžti į profilį

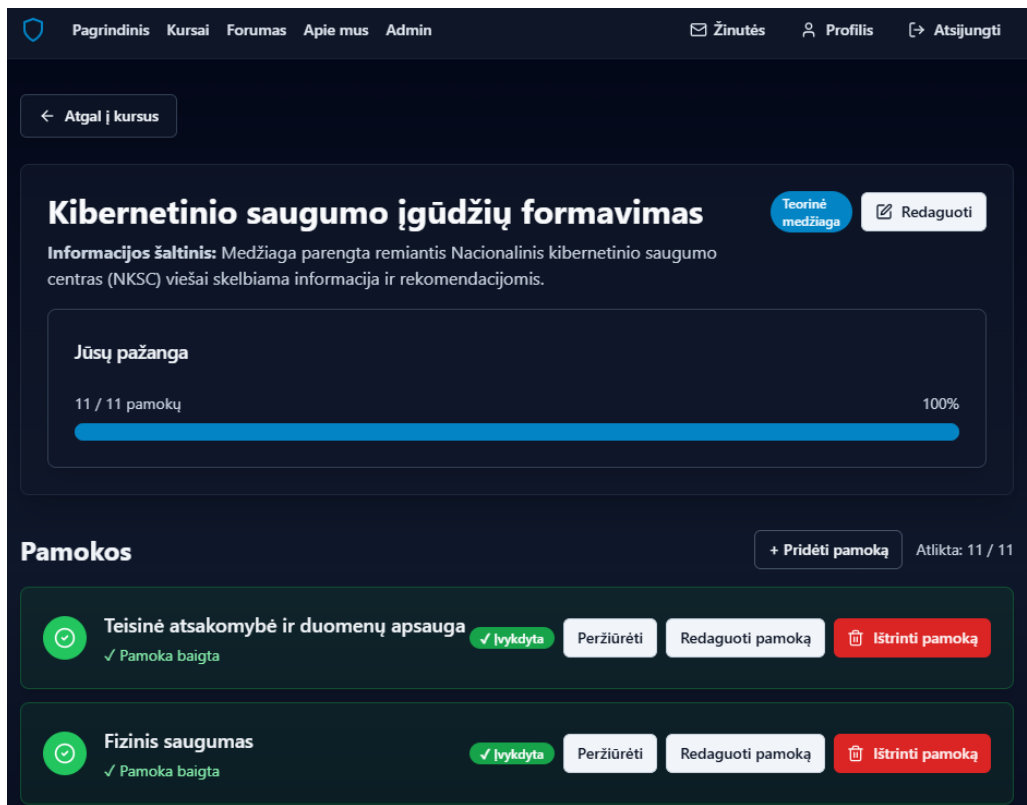
50 pav. Automatiškai sugeneruoto mokymų sertifikato su rezultatais ir galiojimo informacija vaizdas



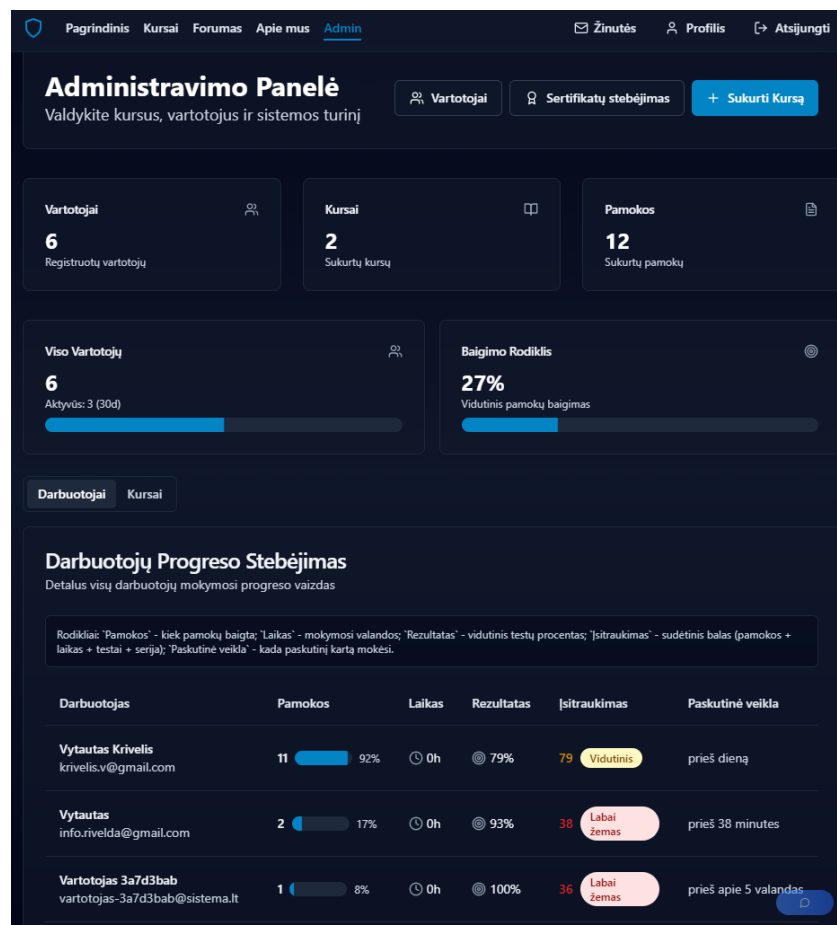
51 pav. Atsisiųsto kibernetinio saugumo mokymų sertifikato vaizdas



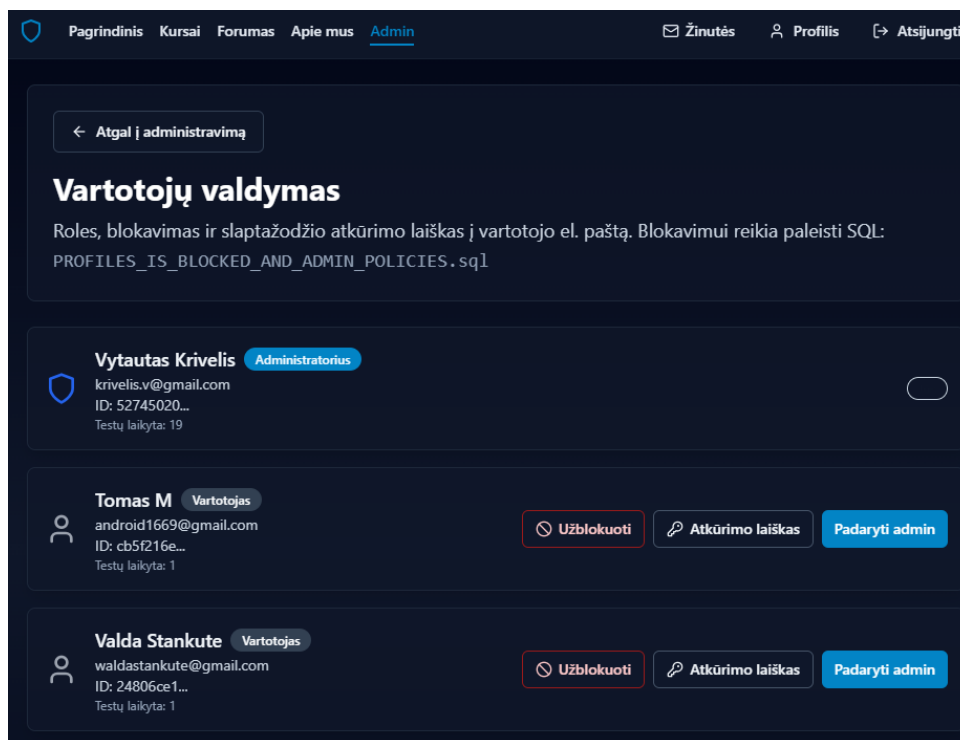
52 pav. Administratoriaus pagrindinis puslapis prisijungus prie sistemos



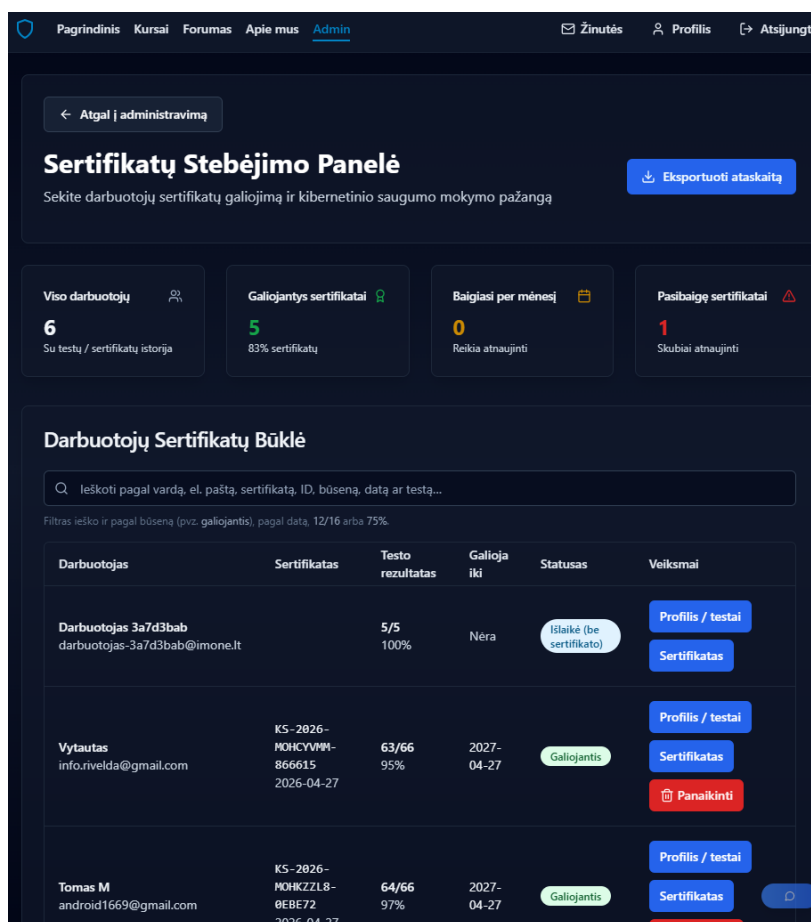
53 pav. Administratoriaus kurso valdymo puslapis su pamokų redagavimo funkcijomis



54 pav. Administratoriaus valdymo panelė mokymosi platformoje



55 pav. Vartotojų valdymo puslapis administratoriaus aplinkoje



56 pav. Sertifikatų stebėjimo ir valdymo panelė administratoriaus aplinkoje

Vartotojo veikla
Testų istorija, kursų pažanga ir sertifikatai (admin peržiūra).

Vartotojo informacija
 Vardas: Vytautas Krivėlis
 El. paštas: krivev.v@gmail.com
 Vartotojo ID: 52745808-3438-43f6-8ea8-bdaa3f97cfc

Testų suvestinė
 Iš viso bandymų: 19
 Su rezultatu ≥ 70%: 14
 Vidutinis %: 79%
 Pirmas bandymas: 2026-04-23 09:54
 Paskutinis bandymas: 2026-04-27 20:35
 Būtį vieną pamokait atlikti daugiau nei vienas bandymas (4 pam.) — matomas pastanga / pakartojimų požymis.

Kursų pažanga

Kibernetinio saugumo įgūdžių formavimas 16/18
91% baigta

Kibernetinio saugumo TESTAS 1/1
100% baigta

Sertifikatai

Sertifikato Nr.	Rezultatas	Išduota	Galioja iki	Peržiūrėti
KS-2026-0002	60 / 60 (100%)	2026-04-27	2027-04-23	Peržiūrėti

Testų istorija

Kursas	Pamoka	Rezultatas	Data	Klaidos
Kibernetinio saugumo įgūdžių formavimas	Keršijūka programinė įranga	4/5	2026-04-27 20:35	Analizė
Kibernetinio saugumo įgūdžių formavimas	Saugūs slaptažodžiai	5/5	2026-04-27 20:34	Analizė
Kibernetinio saugumo įgūdžių formavimas	Socialinė inžinerija (QR kodai)	3/3	2026-04-27 20:31	Analizė

57 pav. Administratoriaus vartotojo veiklos ir mokymosi pažangos stebėsenos puslapis

Testo atsakymai X

Kibernetinio saugumo įgūdžių formavimas · Saugūs slaptažodžiai
2026-04-28 16:12 · 4 / 5 · neteisingų: 1

#5 **Neteisingai**
Kada būtina nedelsiant pakeisti slaptažodį?
 Pasirinktas atsakymas: Tik pakeitus darbą
 Teisingas variantas: Po duomenų nutekėjimo ar saugumo incidento

#1 **Teisingai**
Kodėl slaptažodžiai yra svarbūs skaitmeninėje erdvėje?
 Pasirinktas atsakymas: Jie patvirtina asmens tapatybę ir apsaugo informaciją

#2 **Teisingai**
Kodėl nerekomenduojama naudoti to paties slaptažodžio skirtingoms paskyroms?
 Pasirinktas atsakymas: Nes vieno nutekėjimo atveju gali būti pažeistos kelios paskyros

#3 **Teisingai**
Kokia yra slaptažodžių tvarkyklės paskirtis?
 Pasirinktas atsakymas: Saugoti ir generuoti slaptažodžius saugiai

#4 **Teisingai**
Kas yra dviejų veiksnių autentifikacija (2FA)?
 Pasirinktas atsakymas: Prisijungimas naudojant du skirtingus tapatybės patvirtinimo būdus

58 pav. Vartotojo atlikto testo atsakymų analizės puslapis

4 priedas. Kibernetinio saugumo įgūdžių ir mokymosi poreikių anketa

Sveiki!

Esu Vytautas Krivelis, Kauno technologijos universiteto Informatikos fakulteto magistrantas. Šiuo metu rašau magistrinį darbą tema „Krašto apsaugos sistemos personalo kibernetinio raštingumo ugdymas nuotoliniu būdu“. Šios apklausos tikslas – išsiaiškinti krašto apsaugos sistemoje dirbančių asmenų kibernetinio saugumo įgūdžius, mokymosi poreikius ir požiūrį į nuotolinio mokymosi galimybes.

Jūsų atsakymai bus anonimiški ir naudojami tik moksliniams tikslams. Atsakyti užtruks apie 5–10 minučių.

1. Kokios yra jūsų užimamos pareigos?

Karininkas (-ė)

Puskarininkis (-ė)

Kareivis (-ė)

Civilis (-ė)

2. Kiek metų iš viso dirbate krašto apsaugos sistemoje?

Mažiau nei 1 metus

1–5 metai

6–10 metų

Daugiau nei 10 metų

3. Ar esate kada nors gavę melagingų (phishing) el. laiškų?

Taip, dažnai

Taip, retkarčiais

Ne, niekada

Nežinau

4. Jei gavote melagingų el. laiškų, ar esate kada nors juos atidarę?

Taip, per klaidą

Taip, sąmoningai, bet nepaisiau turinio

Ne, visada juos ištrinu

59 pav. Anketos klausimai 1-4

5. Ar esate gavę apgaulingų SMS žinučių su nuorodomis (smishing)?

- Taip, dažnai
- Taip, retkarčiais
- Ne, niekada
- Nežinau

6. Jei gavote apgaulingų SMS žinučių, ar esate kada nors paspaudę ant nuorodų?

- Taip, per klaidą
- Taip, sąmoningai, bet nesiėmiau jokių veiksmų
- Ne, niekada

7. Ar kada nors jūsų slaptažodis buvo pavogtas ar neteisėtai panaudotas?

- Taip, tai patyriau
- Ne, kiek žinau
- Nežinau

8. Ar naudojate skirtingus slaptažodžius skirtingoms paskyroms?

- Taip, visada
- Taip, dažniausiai
- Ne, dažniausiai naudoju tuos pačius slaptažodžius
- Ne, visada naudoju tą patį slaptažodį

9. Ar naudojate dviejų veiksnių autentifikaciją (2FA) savo paskyrose?

- Taip, visose paskyrose
- Taip, kai kuriose paskyrose
- Ne, nenaudoju

60 pav. Anketos klausimai 5-9

☰

10. Kaip vertinate savo dabartinį kibernetinio saugumo lygį?

1 2 3 4 5 6 7 8 9 10

Labai žemas Labai aukštas

11. Ar žinote, kas yra „konfidencialumas“ kibernetinio saugumo kontekste?

Taip, žinau gerai

Taip, šiek tiek

Ne, nesu susipažinęs

12. Kaip, jūsų nuomone, užtikrinamas duomenų konfidencialumas? (Galima pasirinkti kelis atsakymus)

Naudojant stiprius slaptažodžius

Užšifruojant duomenis

Kontroluojant prieigą prie duomenų

13. Ar žinote, kas yra „vientisumas“ kibernetinio saugumo kontekste?

Taip, žinau gerai

Taip, šiek tiek

Ne, nesu susipažinęs

14. Kokiais būdais, jūsų nuomone, užtikrinamas duomenų vientisumas?

Naudojant atsargines kopijas

Naudojant antivirusines programas

Tikrinant duomenų pakeitimų istoriją

61 pav. Anketos klausimai 10-14

15. Ar žinote, kas yra „prieinamumas“ kibernetinio saugumo kontekste?

- Taip, žinau gerai
- Taip, šiek tiek
- Ne, nesu susipažinęs

16. Kaip, jūsų nuomone, užtikrinamas duomenų prieinamumas?

- Naudojant patikimas serverines sistemas
- Reguliariai atnaujinant programinę įrangą
- Užtikrinant tinklo atsarginį ryšį

17. Ar jūsų organizacijoje yra mokymai, skirti paaiškinti konfidencialumo, vientisumo ir prieinamumo principus?

- Taip, reguliariai
- Taip, kartais
- Ne, niekada

18. Kaip vertinate savo žinias apie šiuos kibernetinio saugumo principus?

- 1 – Labai silpnos
- 2 – Silpnos
- 3 – Vidutinės
- 4 – Geros
- 5 – Labai geros

62 pav. Anketos klausimai 15-18

19. Kaip vertinate savo dabartinį kibernetinio saugumo lygį?

- 1 – Labai žemas
- 2 – Žemas
- 3 – Vidutinis
- 4 – Aukštas
- 5 – Labai aukštas

20. Ar dažnai susiduriate su užduotimis, kurioms reikia kibernetinio saugumo?

- Kasdien
- Kelis kartus per savaitę
- Retai
- Beveik niekada

21. Ar esate dalyvavę kibernetinio saugumo mokymuose per pastaruosius metus?

- Taip
- Ne

22. Kaip vertinate nuotolinio mokymo efektyvumą kibernetinio raštingumo ugdymui?

- 1 – Visiškai neefektyvus
- 2 – Neefektyvus
- 3 – Nei efektyvus, nei neefektyvus
- 4 – Efektyvus
- 5 – Labai efektyvus

63 pav. Anketos klausimai 19-22

23. Kokie veiksniai labiausiai trukdo dalyvauti nuotolinio mokymo programose?

- Laiko trūkumas
- Techninės problemos
- Motyvacijos trūkumas
- Mokymų kokybės trūkumas

...

24. Ar manote, kad nuotolinis mokymas yra tinkama forma kibernetinio raštingumo ugdymui?

- Taip
- Ne
- Neturiu nuomonės

25. Kokius nuotolinio mokymo formatus laikote tinkamiausiais?

- Gyvi mokymai internetu (su dėstytoju realiuoju laiku)
- Savarankiškos mokymosi platformos
- Mišrus mokymas (gyvi mokymai + savarankiškos užduotys)

64 pav. Anketos klausimai 23-25

5 priedas. Kibernetinio saugumo mokymosi platformos vertinimo anketa

Sveiki,

Esu magistrantūros studentas ir vykdu tyrimą, kurio tikslas – įvertinti sukurtos kibernetinio saugumo mokymosi platformos efektyvumą ir patogumą naudoti.

Kviečiu Jus išbandyti platformą ([spausti čia](#)) ir užpildyti šią trumpą anoniminę apklausą. Jūsų atsakymai bus naudojami tik moksliniais tikslais.

Dėkoju už Jūsų laiką ir pagalbą.

1. Ar anksčiau esate dalyvavęs (-usi) nuotoliniuose mokymuose? *

Taip

NE

2. Kaip vertinate savo kibernetinio saugumo žinias prieš naudojantis platforma? *

Labai prastos

Prastos

Vidutinės

Geros

Labai geros

65 pav. Vertinimo anketos klausimai 1-2

3. Kaip vertinate platformos naudojimo paprastumą? *

	1	2	3	4	5	6	7	8	9	10	
Labai sudėtinga	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Labai paprasta

4. Ar platformos struktūra buvo aiški ir suprantama? *

- Taip
- Iš dalies
- Ne

5. Kaip vertinate platformos dizainą (išvaizdą)? *

	1	2	3	4	5	6	7	8	9	10	
labai blogai	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Puikiai

6. Ar mokymosi medžiaga buvo aiški ir naudinga? *

- Taip
- Iš dalies
- Ne

66 pav. Vertinimo anketos klausimai 3-6

7. Ar testų klausimai buvo suprantami? *

- Taip
 - Iš dalies
 - Ne
-

8. Ar testų sudėtingumas buvo tinkamas? *

- Per lengvas
 - Tinkamas
 - Per sudėtingas
-

9. Ar, Jūsų nuomone, platforma padėjo pagerinti kibernetinio saugumo žinias? *

- Taip
 - Iš dalies
 - Ne
-

10. Ar rekomenduotumėte šią platformą kitiems? *

- Taip
- Ne

67 pav. Vertinimo anketos klausimai 7-10

11. Ar naudotumėtės tokia platforma ateityje? *

Taip

Ne

12. Kas Jums labiausiai patiko šioje platformoje?

Ilgo atsakymo tekstas

13. Ką būtų galima patobulinti?

Ilgo atsakymo tekstas

14. Papildomi komentarai ar pasiūlymai:

Ilgo atsakymo tekstas

68 pav. Vertinimo anketos klausimai 11-14



**LIETUVOS KARIUOMENĖS KARINIŲ ORO PAJĖGŲ
ORO GYNYBOS BATALIONAS**

Biudžetinė įstaiga, Šv. Ignoto 8, LT-01120 Vilnius.
Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 188732677.
Bataliono duomenys: biudžetinės įstaigos filialas, Dariaus ir Girėno g. 144, LT-82141 Radviliškis,
tel. / faks. (0 422) 61 580, filialo kodas 188754563.

Kauno technologijos universitetui

**PAŽYMA
APIE MOKYMO KURSŲ ĮDIEGIMĄ VIRTUALIOJOJE MOKYMOSI APLINKOJE**

2026-05- Nr. IP-
Radviliškis

Pažymėtina, kad Vytautas Krivelis 2026 m. Oro gynybos batalione sukūrė virtualiąją mokymosi platformą, skirtą personalo kibernetinio saugumo įgūdžių ugdymui. Platformoje vartotojai gali nuotoliniu būdu savarankiškai mokytis, susipažinti su teorine medžiaga, atlikti žinių patikrinimo užduotis ir gauti baigimo sertifikatą.

Sistema leidžia pritaikyti mokymosi procesą pagal vartotojo žinių lygį, užtikrina pažangos stebėjimą ir suteikia grįžtamąjį ryšį. Tai didina besimokančiųjų išitraukimą ir padeda efektyviau ugdyti praktinius ir teorinius kibernetinio saugumo įgūdžius. Platforma pasiekama adresu: <https://bagiamasisprojektas.vercel.app/>.

Vado įgaliotas Štabo S1 viršininkas

kpt. Edvinas Juozapaitis

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	KOP Oro gynybos batalionas 188754563, Radviliškis, Dariaus ir Girėno g. 144
Dokumento pavadinimas (antraštė)	PAŽYMA APIE MOKYMO KURSŲ IDIEGIMĄ VIRTUALIOJOJE MOKYMOSI APLINKOJE
Dokumento registracijos data ir numeris	2026-05-08 Nr. IP-16
Dokumento gavimo data ir dokumento gavimo registracijos numeris	–
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	kpt. EDVINAS JUOZAPAITIS, Skyriaus viršininkas, S1
Sertifikatas išduotas	EDVINAS JUOZAPAITIS LT
Parašo sukūrimo data ir laikas	2026-05-08 11:21:50 (GMT+03:00)
Parašo formatas	XAdES-T
Laiko žyme nurodytas laikas	2026-05-08 11:21:59 (GMT+03:00)
Informacija apie sertifikavimo paslaugų teikėją	SK ID Solutions EID-Q 2024E, SK ID Solutions AS EE
Sertifikato galiojimo laikas	2026-05-07 19:07:40 – 2029-05-06 19:07:39
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA-2, VI Registru Centras - i.k. 124110246 LT" išduotą sertifikatą "Dokumentų valdymo sistema DokVIS, Lietuvos Respublikos krašto apsaugos ministerija, i.k. 188602751 LT", sertifikatas galioja nuo 2024-12-18 13:34:30 iki 2027-12-18 13:34:30
Pagrindinio dokumento priedų skaičius	–
Pagrindinio dokumento priedamų dokumentų skaičius	–
Priedamo dokumento sudarytojas (-ai)	–
Priedamo dokumento pavadinimas (antraštė)	–
Priedamo dokumento registracijos data ir numeris	–
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Dokumentų valdymo sistema Avilyš, versija 3.5.90.2
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2026-05-08 11:26:52)
Paieškos nuoroda	–
Papildomi metaduomenys	Nuorašą suformavo 2026-05-08 11:26:52 Dokumentų valdymo sistema Avilyš