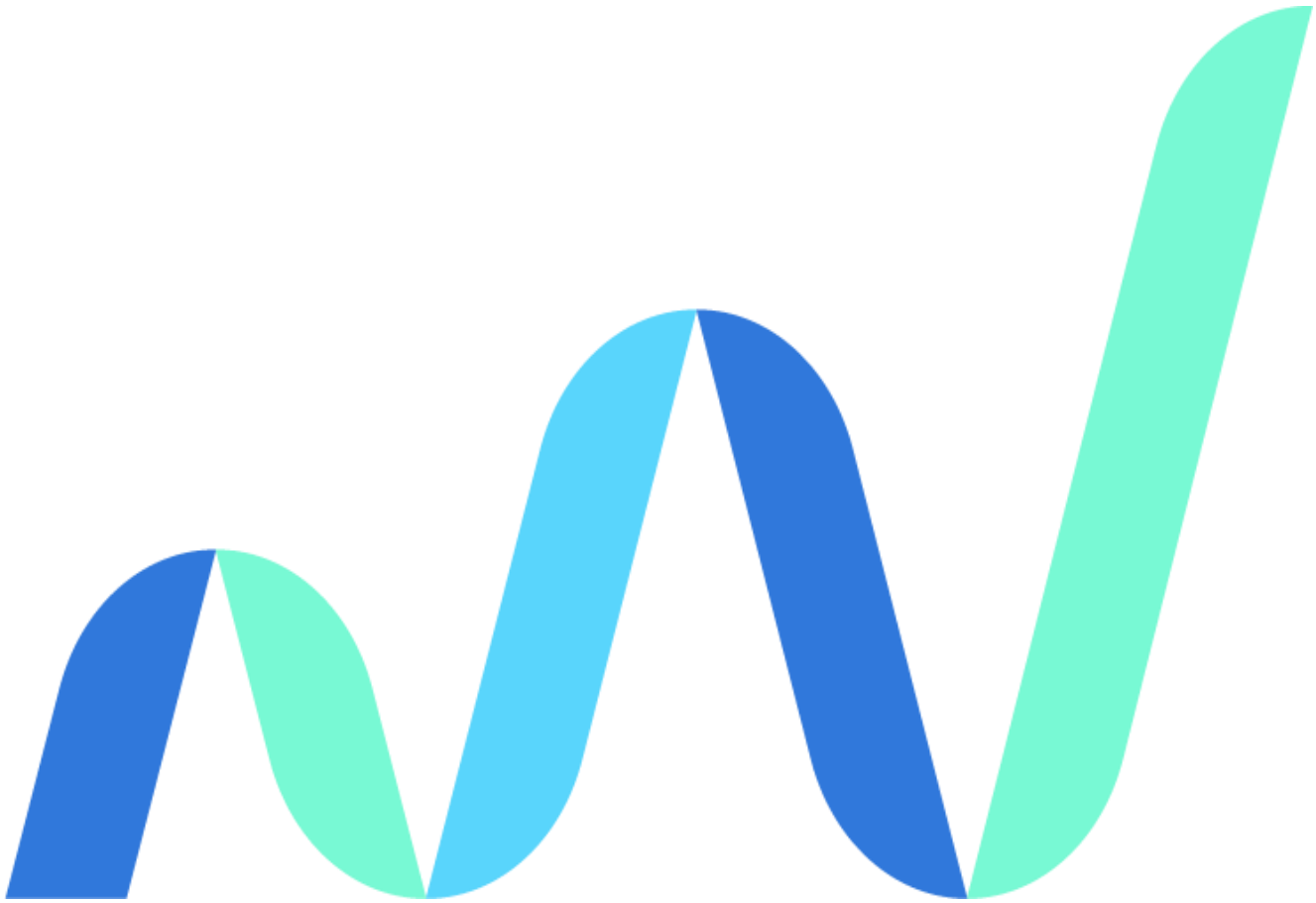
Kibernetinio saugumo bendruomenės būrimas: *Cyber Campus LT* koncepcija

Projekto trukmė: 2023.03.05–2024.09.06
Projekto vadovai:
Rasa Mončiunskaitė ir Dominykas Kugelevičius
Projekto savininkas: Jonas Skardinskas
Data: 2024.09.05



Turinys

Įvadas 3
1. Kodėl reikalinga *Cyber Campus LT* priemonė? 4
1.1. Kibernetinio saugumo ekosistemos dalyvių poreikiai 6
2. *Cyber Campus LT* iniciatyvos siūlymas 7
2.1. Kas yra *Cyber Campus LT* ? 7
2.2. Strateginės veiklos kryptys ir tikslai 7
2.3. Veiklų įgyvendinimas 8
2.4. Bendradarbiavimo galimybės pasitelkiant *Cyber Campus LT* 10
2.5. Bendruomenės struktūra ir jos veikimas 12
2.6. Steigimas ir pozicionavimas 14
3. Rizikų valdymas 15
4. Poveikis 16
4.1. Nauda nariams 16
4.2. Ekosistemai 16
5. Grįžtamasis ryšys 17

Įvadas

Atsižvelgiant į vis didėjančią kibernetinio saugumo svarbą apsaugant nacionalinę infrastruktūrą, taip pat į sparčiai besikeičiančią kibernetinio saugumo situaciją ir vis didėjančias kibernetines grėsmes, atsiranda būtinybė skatinti kibernetinio saugumo inovacijas, švietimą, tarptautinį bendradarbiavimą ir stiprinti partnerystes tiek nacionaliniu, tiek ir Europos Sąjungos lygmeniu. Įvertinus į globalius kibernetinio saugumo iššūkius, Europos Sąjungos kibernetinio saugumo strategijos įgyvendinimo kryptį bei atliepiant Lietuvos kibernetinio saugumo ekosistemos probleminius “skausmo” taškus (nuo fragmentuotos ekosistemos iki inovacijų trūkumo bei nepakankamo tarpinstitucinio bendradarbiavimo), kurie reikalauja sisteminio požiūrio, Nacionaliniam kibernetinio saugumo centrui (NKSC) siūloma *Cyber Campus LT* iniciatyva. Ja siekiama suburti nepriklausomus kibernetinio saugumo specialistus, akademijos, viešojo ir privataus sektorių atstovus ir ,pasitelkiant šią bendruomenę, skatinti kibernetinio saugumo stiprinimą Lietuvoje.

Cyber Campus LT reikalingas, siekiant sukurti stiprią ir dinamišką kibernetinio saugumo ekosistemą, kuri leistų: i) pagerinti bendradarbiavimą tarp sektorių, suburiant viešojo sektoriaus, verslo ir akademines institucijas, siekiant veiksmingesnio kibernetinio saugumo politikos įgyvendinimo ir inovacijų vystymo; ii) spręsti specialistų trūkumo problem, inicijuojant mokymų programas, didinant kibernetinio saugumo žinias ir ugdant aukštos kvalifikacijos specialistus; iii) skatinti inovacijas, sukuriant palankią aplinką joms

gimti, ypač mažoms ir vidutinėms įmonėms, plėtojant naujus kibernetinio saugumo sprendimus; iv) stiprinti Lietuvos pozicijas tarptautinėje arenoje, didinant šalies tarptautiškumą ir prisijungiant prie tarptautinių kibernetinio saugumo projektų bei bendruomenių. *Cyber Campus LT* sukuria erdvę, kurioje įmanoma efektyviai spręsti šiuolaikinius kibernetinius iššūkius, skatinant bendruomeniškumą, inovacijas ir švietimą.

Dokumente aptariamos pagrindinės iniciatyvos priežastys, tikslai, įgyvendinimas bei nauda nariams ir ekosistemai.

1. Kodėl reikalinga *Cyber Campus LT* priemonė?

Cyber Campus LT - NKSC priemonė, skirta kibernetinio saugumo ekosistemai, siekiant suburti ekosistemos žaidėjus į aktyvią nacionalinę lygiavertiškumo pagrindai organizuotą bendruomenę ir ją įgalinti kryptingai veikti, siekiant vieningai kurti Lietuvos kibernetinį atsparumą.

Kelios priežastys lemia poreikį suburti kibernetinio saugumo ekosistemos žaidėjus į aktyvią bendruomenę, pasitelkiant *Cyber Campus LT* priemonę.

1. Europos Komisija siekia sukurti Europos kibernetinio saugumo atlasą (angl. *European Cybersecurity Atlas, ECS Atlas*)[1], kuris tarnautų kaip žinių valdymo platforma, skirta Europos kibernetinio saugumo ekspertų bendradarbiavimui kartografuoti, kategorizuoti ir skatinti, siekiant įgyvendinti Europos Sąjungos (ES) skaitmeninę strategiją. Už atlaso valdymą ir koordinavimą atsakingas Europos kibernetinio saugumo kompetencijų centras (angl. *European Cybersecurity Competence Centre, ECCC*), jam nacionaliniu lygmeniu talkina Nacionalinių koordinavimo centrų (NKC) tiklas (angl. *National Coordination Centre, NCC*). Lietuvoje ši funkcija patikėta NKSC. Nacionaliniam koordinavimo centrui patikėta kurti aktyvią Kibernetinio saugumo kompetencijos bendruomenę[2] ir kaip jos narius registruoti juridinius asmenis Reglamento (ES) 2021/887[3] straipsnyje nustatyta tvarka[4]. Paminėtina, kad šios bendruomenės nariais negali būti nacionalinio saugumo interesams grėsmę keliantys asmenys. Atkreiptinas dėmesys, kad, pasak ekspertų, šiai dienai juridiniams asmenims nėra aiškiai įvardintos konkrečios naudos gaunamos iš registracijos į Europos kibernetinio saugumo atlasą. Remiantis Kibernetinio saugumo įstatymu (nauja redakcija įsigalioja 2024 m. spalio 18d.), į bendruomenę įtraukiami tik juridiniai asmenys. Tuo tarpu fiziniai asmenys nėra įtraukiami, nors jų nauda gali būti keleriopa:

   i) jų žinios, patirtis ir įžvalgos gali būti kitokios nei juridinių asmenų (įmonių ar organizacijų). Įvairios perspektyvos padeda geriau suprasti kibernetinio saugumo iššūkius ir rasti inovatyvių sprendimų.
   ii) nepriklausomų tyrėjų, ekspertų įtraukimas gali skatinti kūrybiškumą ir inovacijas.
   iii) gali padėti skleisti žinias plačiau visuomenėje. Jie gali veikti kaip ekspertai, kurie teikia informaciją ir švietimą apie kibernetinio saugumo svarbą, taip didinant bendrą visuomenės saugumo lygį.
   iv) gali greičiau reaguoti į besikeičiančias kibernetinio saugumo grėsmes ir prisitaikyti prie naujų iššūkių, nes jie dažnai yra mažiau suvaržyti biurokratinių procedūrų nei didelės organizacijos. Tai leidžia greičiau prisitaikyti prie naujų kibernetinių grėsmių ir diegti reikalingus pokyčius.
   v) gali skatinti teigiamus pokyčius organizacijos viduje.

2. Nagrinėtose užsienio šalių praktikose[5], išskirtinas Maltos pavyzdys, kuris rodo, kad svarbu, buriant kibernetinio saugumo bendruomenę, neapsiriboti tik juridiniais asmenimis. Juridinių asmenų atveju bendruomenės veikloje dažniausiai dalyvauja tik sprendimų priėmėjai, tuo tarpu įtraukimas ir fizinių asmenų į bendruomenės veiklą leidžia pritraukti ir techninę ekspertizę turinčius kibernetinio saugumo specialistus. Taip sukuriama sėkminga sinergija tarp skirtingus vaidmenis ekosistemoje atliekančių specialistų, kuriamas dialogas strateginiu, procesiniu ir taktiniu lygmenimis ir užtikrinamas holistinis kibernetinio saugumo puoselėjimas. Bendruomenės heterogeniškumas skatinamas ir Prancūzijos *Campus Cyber*, kur bendradarbiavimas vyksta tarp skirtingų sektorių.

3. Egzituojanti keturių krypčių kibernetinio saugumo ekosistemos problematika[6], kuri turi įtakos Lietuvos kibernetiniam atsparumui: fragmentuota kibernetinio saugumo ekosistema, inovacijų kibernetinio saugumo srityje trūkumas, nepakankamas kiekis kibernetinio saugumo specialistų, auganti kibernetinių ir hibridinių atakų grėsmė. Šios problemos yra kompleksinės, tad svarbu, kad jų sprendimai būtų sutelkti į galimas to

[1] European Cybersecurity Atlas | European Cybersecurity Atlas (europa.eu)
[2] Nacionalinė kibernetinio saugumo plėtros programa (2023-2030 m.)
[3] Reglamentas - 2021/887 - EN - EUR-Lex (europa.eu)
[4] XIV-2902 Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas (e-tar.lt)
[5] Užsienio šalių praktikos
[6] Kibernetinio saugumo ekosistemos problematika

priežastis. Projekto eigoje išskyrėme tris iššūkių keliančias sritis, kurios turi įtakos minėtoms kompleksiškesnėms problemoms:

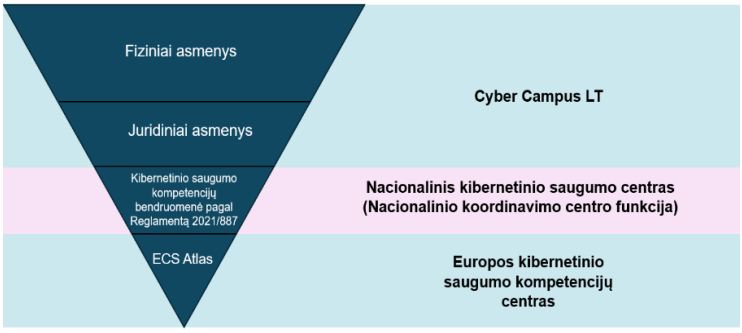
BENDRUOMENIŠKUMAS. Bendradarbiavimo ir dialogo trūkumas kibernetinio saugumo ekosistemoje kelia rimtą iššūkį efektyviam kibernetinio atsparumo stiprinimui šalyje.

ŠVIETIMAS IR UGDYMAS. Egzistuoja jaunosios kartos švietimo, informuotumo ir susidomėjimo kibernetinio saugumo sritimi trūkumas, kuris iš dalies lemia nepakankamą specialistų skaičių šioje srityje.

INOVACIJŲ TRŪKUMAS. Dabartinis kibernetinio saugumo paslaugas ir sprendimus teikiančių įmonių mastas nėra pakankamas pilnai aptarnauti šalies poreikius. Akademinei bendruomenei, kuriančiai inovacijas, sudėtinga gauti prieigą prie viešojo sektoriaus infrastruktūros, siekiant sukurti aukštos technologinės parengties produktą. Tai iš dalies lemia inovacijų trūkumą kibernetinio saugumo srityje.

4. Nacionalinėje kibernetinio saugumo plėtros programoje nurodyta, kad viena iš mažėjančio Lietuvos kibernetinio atsparumo priežasčių yra nenustatytos viešojo ir privataus sektoriaus bendradarbiavimo kryptys.[7] Šią problemą Krašto apsaugos ministerija siekia spręsti vykdant veiklas, kurių pagalba norima geriau išnaudoti viešojo ir privataus sektorių bendradarbiavimo kibernetinio saugumo srityje potencialą. Pasak Krašto apsaugo ministerijos atsakingų asmenų numatoma galimybių studija, kurios pagalba bus sukurto gairės, konkrečiau apibrėšiančios bendradarbiavimo kryptis ir konkrečius veiksmus, siekiant, kad bendradarbiavimas būtų naudingas visoms suinteresuotoms šalims. Savo ruožtu, *Cyber Campus LT* bendruomenės nariai dalyvaudami renginiuose, apklausose ir forumuose, gali teikti grįžtamąjį ryšį apie siūlomus sprendimus ir programas, padėdami užtikrinti, kad sukurtos gairės ir veiksmų planai atitiktų realius poreikius ir iššūkius.

5. Aktyvi, tarpusavio ryšį sukūrusi bendruomenė gali efektyviai pasitarnauti sprendžiant kompleksines problemas, nes jų teikiama nauda yra daugiasluoksnė:
   - lengvesnis ryšio užmezgimas;
   - stiprėjantis ryšys tarp bendruomenės narių;
   - bendradarbiavimo ir keitimosi žiniomis skatimas;
   - tarpusavio pasitikėjimo stiprėjimas;
   - realių problemų iškėlimas ir sprendimai;
   - bendrų tikslų siekimas.



1 pav. *Cyber Campus LT* vaidmuo kibernetinio saugumo kompetencijų bendruomenės kontekste.

Apibendrinant pavaizduotoje schemoje (1 pav.) galima matyti, kad *Cyber Campus LT* (kaip NKSC priemonė) apimantis tiek fizinius, tiek juridinius asmenis (pvz. mažas ir vidutines įmones) gali sėkmingai papildyti NKC veiklą ir sukurti daugiau pridėtinės vertės kibernetinio saugumo ekosistemai ir buriamai aktyviai bendruomenei.

[7] Nacionalinė kibernetinio saugumo plėtros programa (2023-2030 m.)

1.1. Kibernetinio saugumo ekosistemos dalyvių poreikiai

Kibernetinio saugumo ekosistemos dalyviai, turi skirtingus poreikius. Vis dėlto, juose erdvės kurti sinergijos taškus yra.

Viešasis sektorius:

- **Kibernetinio saugumo politika ir reglamentavimas**. Sukurti ir įgyvendinti efektyvias kibernetinio saugumo politikas, įstatymus bei reglamentus, kurie apsaugotų valstybę ir jos piliečius nuo kibernetinių pavojų. Siekiant, kad formuojama politika būtų efektyvi svarbu vystyti dialogą su verslo sektoriumi, nes įmonės, gali suteikti vertingos informacijos apie praktinius kibernetinio saugumo aspektus, kurie gali būti naudingi formuojant politiką ir siekiant, kad reguliavimo reikalavimai būtų realistiški ir įgyvendinami.
- **Kritinės infrastruktūros apsauga**. Apsaugoti svarbias infrastruktūras, tokias kaip energetikos, transporto, sveikatos apsaugos ir kitos sistemos, nuo kibernetinių grėsmių.
- **Visuomenės švietimas ir informuotumas**. Didinti piliečių informuotumą apie kibernetinius pavojus ir jų prevencijos priemones.
- **Ekonomikos augimas ir konkurencingumas**: Verslo įmonės, dalyvaudamos ES projektuose, gali gauti reikšmingą finansinę paramą, kuri padeda plėtoti ir įgyvendinti naujus produktus ar paslaugas, kurių šiuo metu Lietuvoje, pasak ekspertų, trūksta.

Privatus sektorius:

- **Eksporto galimybių plėtra ir įsiliejimas į tarptautines vertės grandines.** Verslas turi poreikį plėsti savo veiklą užsienio rinkose, vis dėlto įėjimas į šią rinką reikalauja tarptautinių ryšių ir partneryščių mezgimo.
- **Klientų rato ir projektų galimybių plėtra.** Daliai verslų projektinė veikla suteikia galimybes gauti finansavimą, plėsti veiklą bei įgyvendinti inovatyvius sprendimus ir kartu užsitikrinti augantį skaičių klientų. Kita vertus, dalyvavimas ES ar nacionaliniuose projektuose verslo matomas kaip apsunkintas ir „per lėtas“ procesas.
- **Kvalifikuotų specialistų skaičiaus augimas.** Kibernetinio saugumo sritis greitai keičiasi, verslui svarbu užtikrinti, kad darbuotojai nuolat atnaujintų savo žinias ir gebėjimus, dalyvaudami mokymuose, seminaruose ir kituose švietimo renginiuose**.**
- **TIS2 direktyvos reikalavimų įgyvendinimas**[8]**.** Sukuriamas ekspertinių žinių ir dalinimosi jomis, bendradarbiavimo kibernetiniame saugume poreikį, siekiant įgyvendinti aukštus saugumo reikalavimus.

Akademija:

- **Finansavimas**. Siekiant užtikrinti sėkmingą akademinės veiklos plėtrą, būtinas stabilus ir nuoseklus finansavimas, kuris dažniausiai būna projektinis.
- **Realių problemų sprendimas.** Egzistuoja mokslinių projektų ir straipsnių įgyvendinamų drauge su verslu poreikis, kai taikomi sprendimai viešajam sektoriui.
- **Realūs duomenys**. Moksliniai straipsniai remiantis tikrais, o ne „sintetiniais“ viešojo sektoriaus duomenimis, leistų mokslininkams ir tyrėjams kurti ir testuoti naujas praktikas, plėtoti inovatyvius sprendimus, suteiktų studentams galimybę dirbti su realiomis situacijomis, kas gali pagerinti jų praktinius įgūdžius ir pasirengimą realiam darbui. Šio poreikio atliepimas gali padėti formuoti geresnę politiką ir reguliavimą kibernetinio saugumo srityje, remiantis realiais duomenimis ir išvadomis.
- **Moksliniai straipsniai**. Svarbu skatinti ir vykdyti mokslinius tyrimus bei eksperimentinę veiklą, siekiant plėtoti naujas žinias ir technologijas, šiuos pasiekimus viešinti moksliniuose straipsniuose. Straipsniai apie naujausias grėsmes, tendencijas ir technologijas gali būti naudingi tiek viešajam, tiek ir verslo sektoriams.

Visoms suinteresuotoms šalims svarbus apsikeitimas informacija apie grėsmių vektorius (angl. *Cyber threat intelligence, CTI*). Pasak ekspertų, Lietuvoje vyrauja baudimo kultūra dėl to „niekas nenori rizikuoti“. Bendruomenė gali padėti dalintis informacija apie grėsmes, geriausias (blogas) praktikas ir incidentų valdymo strategijas.

[8] LR Krašto apsaugos ministerija (kam.lt)

2. *Cyber Campus LT* iniciatyvos siūlymas

2.1. Kas yra *Cyber Campus LT* ?

Žvelgiant iš kibernetinio saugumo ekosistemos žaidėjų perspektyvos, lietuviškasis *Cyber Campus LT* funkcionuotų kaip ekosistemai skirta platforma (reali ir virtuali), kur susiburtų aktyvi lygiavertiškumo pagrindais organizuota kibernetinio saugumo bendruomenė, sudaryta iš nepriklausomų ekspertų, verslo, viešojo sektoriaus ir mokslo atstovų, siekiant vieningai kurti Lietuvos kibernetinį atsparumą, pasitelkiant švietimą ir inovacijas.

Vizija
Aktyvios nacionalinės, tarptautiniu mastu pripažintos kibernetinio saugumo bendruomenės Lietuvoje subūrimas, siekiant stiprinti šalies kibernetinį atsparumą.

Misija
Būti jungiančiu dėmeniu kibernetinio saugumo srityje, burti ir proaktyviai įgalinti kibernetinio saugumo srities atstovus dalintis ir semtis žinių, siekti bendrų tikslų švietimo ir inovacijų srityse, vardan vieningai kuriamo Lietuvos kibernetinio atsparumo.

Vertybės.
Pasitikėjimas. Kuriamas nuoseklumo, sąžiningumo ir konfidencialumo pagrindais.
Vienybė. Kartu esam stipresni. Puoselėjama specialistų, organizacijų ir suinteresuotųjų šalių darni ir bendradarbiaujanti aplinka, siekiant bendrai mažinti kibernetines grėsmes ir didinti atsparumą.
Atvirumas. Idėjoms, dalyviams ir nariams, bendradarbiavimui, dialogui, pokyčiams, dalinimuisi žiniomis, įžvalgoms.

2.2. Strateginės veiklos kryptys ir tikslai

Strateginė kryptis	Ilgalaikis tikslas	Veiksmai
Bendruomeniškumas	Suburti ir palaikyti aktyvią bei įtraukią kibernetinio saugumo bendruomenę, kurioje nariai galėtų dalintis žiniomis, patirtimi bei dirbti kartu sprendžiant kibernetinio saugumo problemas.	✓ Seminarų, dirbtuvių, mokymų pagalba tobulinti kibernetinio saugumo bendruomenės kompetencijas. Temos siūlomos tiek *Cyber Campus LT* bendruomenės vadovo, tiek bendruomenės narių. ✓ Organizuojami didesnio masto metiniai renginiai bendruomenės nariams (pvz. hakatonai, pratybos, tarptautinis forumas). ✓ Skatinti dalintis žiniomis tarp bendruomenės narių organizuojamų mini susitikimų metu ir darbo grupėse (žr. Bendruomenės struktūra ir jos veikimas). ✓ Koordinuoti ir aktyvinti bendradarbiavimą tarp kibernetinio saugumo specialistų tematinėse darbo grupėse.
Švietimas	Gerinti mokinių ir studentų skaitmenines ir kibernetinio saugumo kompetencijas bei populiarinti kibernetinio saugumo profesiją. Tai prisidės prie aukšto lygio kibernetinio saugumo specialistų skaičiaus augimo Lietuvoje.	✓ Sukurti ir įgyvendinti kibernetinio saugumo akademiją (angl. *Cybersecurity Academy*). Tai būtų intensyvi 3-6 mėn. praktikos programa, skirta gilinti žinias ir įgūdžius kibernetinio saugumo srityje antro, trečio kurso studentams. Į programos ruošimą ir įgyvendinimą įtraukti viešojo sektoriaus, verslo ir akademijos atstovai. ✓ Sukurti ir įgyvendinti dirbtuves moksleiviams apie kibernetinį atsparumą. Pasitelkiama NKSC turima infrastruktūra,

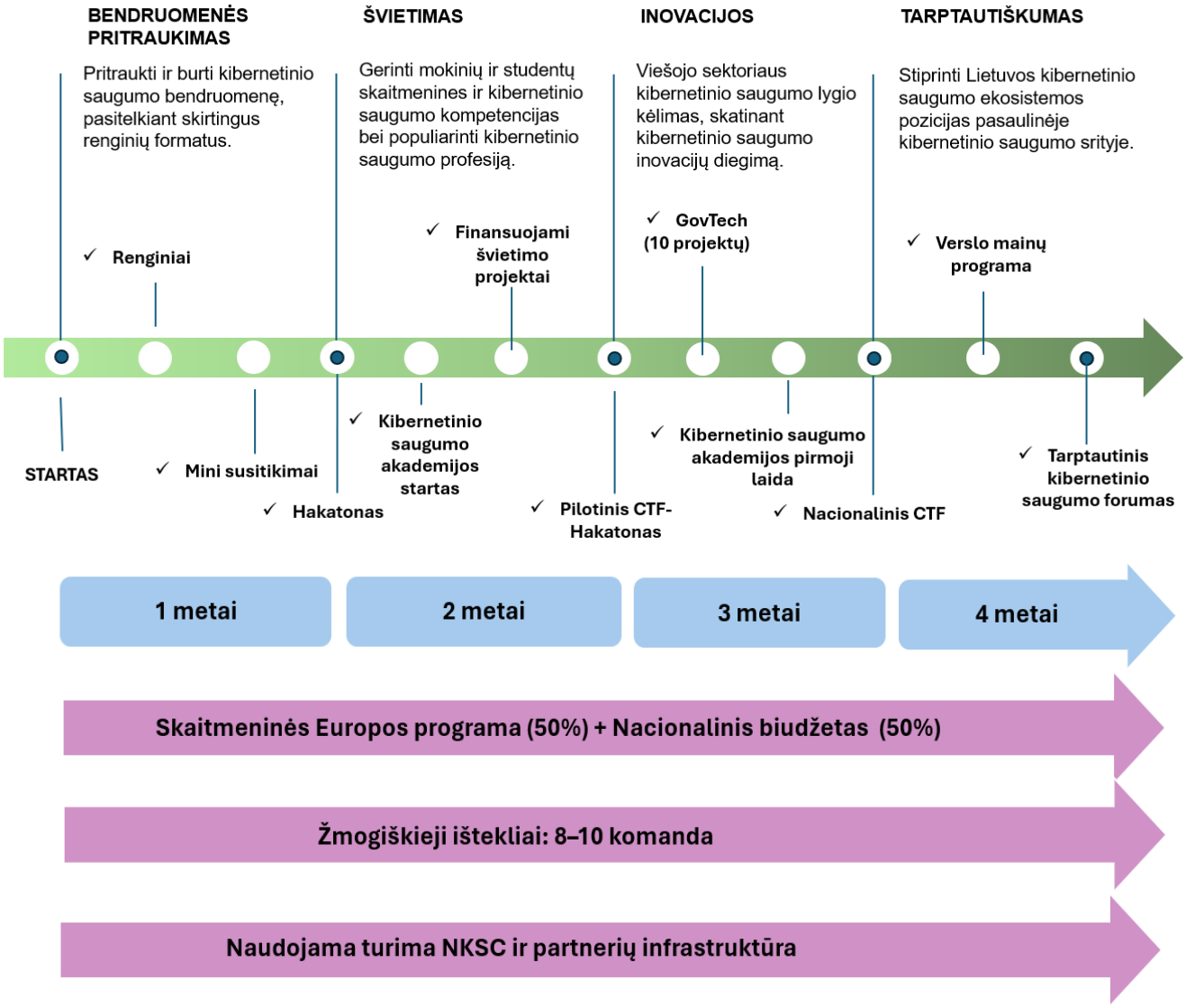
		bendradarbiaujama su universitetų kompetencijų centrais, verslo atstovais. ✓ Skiriamas finansavimas edukacinėms veikloms: moksleivių kibernetinio saugumo pratyboms, stovykloms (50% stovyklų skirtos mergaitėms). Mišriose stovyklose dalyvaujančių mergaičių ne mažiau nei 30%. ✓ Skiriamas finansavimas kibernetinio saugumo pratyboms organizuoti, skirtoms specialistams (angl. *Capture the flag, CTF*).
Inovacijos	Skatinti viešojo sektoriaus įstaigų ir sprendimus kuriančių startuolių, mažų ir vidutinių įmonių, akademijos bendradarbiavimą, siekiant kibernetinio saugumo inovacijų diegimo viešajame sektoriuje ir kritinėje infrastruktūroje. Tai prisidės keliant viešojo sektoriaus kibernetinio saugumo lygį.	✓ Pasitelkiamas GovTechlab veikimo modelis (angl. *know-how*). Sujungiamos viešojo sektoriaus įstaigos ir sprendimus galinčios pasiūlyti organizacijas, komandos. ✓ Iššūkius teikia viešojo sektoriaus įstaigos, priskiriamos ypatingos svarbos ir kitiems svarbiems sektoriams pagal TIS2 direktyvą. ✓ Sprendimus siūlyti galėtų tiek verslo sektoriaus (startuoliai, mažos ir vidutinės įmonės), tiek akademijos, tiek jungtinių komandų atstovai. ✓ Rekomenduojama per metus įgyvendinti 10 projektų.
Tarptautiškumas	Stiprinti Lietuvos kibernetinio saugumo ekosistemos pozicijas pasaulinėje kibernetinio saugumo srityje.	✓ Plėsti ir stiprinti tarptautinius ryšius kibernetinio saugumo srityje. Siūloma verslo mainų programa bendradarbiaujant su užsienio kibernetinio saugumo bendruomenėmis (pvz. Prancūzijos *Campus Cyber*, Švedijos *Cybercampus* ir kt.). Tikslinė auditorija: startuoliai, mažos ir vidutinės įmonės, akademija. ✓ Didinti Lietuvos tarptautinį matomumą. Rekomenduojama drauge su partneriais organizuoti tarptautinę konferenciją. Tikslinė auditorija: Lietuvos ir užsienio šalių kibernetinio saugumo ekspertai, potencialūs investuotojai iš užsienio.

2.3. Veiklų įgyvendinimas

Trumpalaikiai tikslai (1-2 metai):

- ✓ *Cyber Campus LT* įtraukimas į Nacionalinę kibernetinio saugumo plėtros programą (2023-2030 m.). Šio tikslo įgyvendinimas padės užtikrinti veiklos tęstinumą.
- ✓ Bendruomenės narių sąrašo sąrašo vystymas. Siektinas minimalus aktyvių bendruomenės narių skaičius per dvejus metus yra 100 fizinių ir 20 juridinių asmenų.
- ✓ Kibernetinio saugumo akademijos (angl. *Cybersecurity Academy*) programos jaunimui ir pirmųjų edukacinių dirbtuvių moksleiviams sukūrimas ir įgyvendinimas. Į procesus įtraukiami verslo ir akademijos atstovai.
- ✓ Tarptautinių ryšių su kibernetinio saugumo organizacijomis ir ekspertais mezgimas. Rekomenduojama palaikyti Kurk Lietuvai projekto metu užmegztą ryšį su užsienio šalių kibernetinio saugumo bendruomenėmis (pvz. Prancūzijos *Campus Cyber*, Izraelio *Cyber7*, Maltos nacionaliniu koordinavimo centru, Švedijos *Cybercampus Sverige*) ir kitomis Lietuvai draugiškų šalių kibernetinio saugumo bendruomenėmis.

Siūlomas *Cyber Campus* LT įgyvendinimas per pirmuosius ketverius veiklos metus (2 pav.).



2 pav. *Cyber Campus LT* įgyvendinimas pagal strategines kryptis ir reikalingi resursai (finansiniai, žmogiškieji, infrastruktūra).

Pateikiamoje schemoje veiklų įgyvendinimo eiliškumas yra laipsniškas, su laiku vykstantis paraleliai t.y. kiekvienais metais pridedant po vieną veiklos kryptį tuo pačiu tęsiant pradėtą. Po pirmųjų ketverių veiklos metų rekomenduojama įvertinti veiklos rezultatus ir prireikus koreguoti veiklų intensyvumą.

Atsakinga institucija. *Cyber Campus LT* koncepcija yra perduota Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos tolesniam įgyvendinimui. Siūloma, kad NKSC būtų pagrindinė institucija (vykdytoja), atsakinga už *Cyber Campus LT* veiklų įgyvendinimą bendradarbiaujant su kitomis viešosiomis įstaigomis ir organizacijomis. Atkreiptinas dėmesys, kad galimas ir alternatyvus įgyvendinimo scenarijus, kuris aptariamas dalyje „Steigimas ir pozicionavimas“. Svarbu lanksčiai prisitaikyti prie besikeičiančių aplinkybių ir užtikrinti, kad būtų pasirinktas efektyviausias modelis *Cyber Campus LT* tikslams pasiekti.

Finansavimas. *Cyber Campus LT* veikla gali būti finansuojama iš Skaitmeninės Europos programos[9] lėšų. Atkreiptinas dėmesys, kad šio finansavimo intensyvumas yra 50%. Kita dalis lėšų (50%) turėtų būti skiriama iš Nacionalinio biudžeto. Siektina, kad *Cyber Campus LT* priemonė būtų įtraukta į Nacionalinę kibernetinio saugumo plėtros programą, taip užtikrinant jos tęstinumą. Projekto metu sukurtas *Cyber Campus LT* pasiūlymas pristatytas Krašto apsaugos ministerijai, siekiant svarstyti galimybę finansuoti *Cyber Campus LT* veiklą.

[9] Digital Europe Programme - European Commission (europa.eu)

Žmogiškieji ištekliai. Vertinant *Cyber Campus LT* veiklas, jų pobūdį ir apimtį, rekomenduojama suburti dedikuotą 8-10 specialistų komandą, kurią sudarytų bendruomenės vadovas, komunikacijos vadovas, ir keli projektų vadovai, atsakingi už skirtingų iniciatyvų vykdymą. Vis dėlto atsižvelgiant į turimus išteklius ir veiklos pradžios galimybes, iniciatyva galėtų startuoti su mažesne, trijų žmonių komanda, į kurią įeitų bendruomenės vadovas, komunikacijos vadovas ir vienas projektų vadovas. Nepaisant pradinės komandos dydžio, ilgalaikėje perspektyvoje būtina skirti papildomus žmogiškuosius išteklius, kad būtų užtikrintas visų suplanuotų veiklų įgyvendinimas ir veiklos plėtra.

Infrastruktūra. *Cyber Campus LT* veiklai (seminarams, mokymams, dirbtuvėms, susitikimams) būtų naudojama NKSC turima infrastruktūra (Goštauto g. 12, Vilnius). Didesnės apimties metiniams renginiams (pvz. hakatonai, *CTF* pratybos, tarptautinė konferencija) būtų reikalinga infrastruktūra nuomai. Siekiama, kad įgyvendinant atitinkamas *Cyber Campus LT* veiklas būtų pasitelkiama ir potencialių partnerių infrastruktūra (pvz. universitetų kompetencijų centrai), siekiant efektyviai išnaudoti turimus valstybės išteklius.

Bendradarbiavimas. *Cyber Campus LT* siekia sukurti efektyvią kibernetinio saugumo ekosistemą Lietuvoje ir suburti aktyvią bendruomenę, todėl bendradarbiavimas su įvairiomis institucijomis yra svarbus šios iniciatyvos aspektas. Bendradarbiavimas turėtų vykti keliomis kryptimis: i) su universitetais (įgyvendinant kibernetinio saugumo akademiją, seminarus, dirbtuves moksleiviams). Universitetų kompetencijų centrai gali tapti partnerių infrastruktūros dalimi, kuri būtų pasitelkiama organizuojant mokomuosius renginius; ii) su valstybinėmis įstaigomis (pvz. VšĮ Investuok Lietuvoje ar VšĮ Inovacijų agentūra), kurios gali tapti svarbiais partneriais skatinant inovacijas ir pritraukiant investicijas į kibernetinio saugumo sektorių; iii) su asociacijomis ir verslo atstovais. *Cyber Campus LT* turėtų būti atviras bendradarbiavimui su įvairiomis asociacijomis, veikiančiomis kibernetinio saugumo srityje. Tokios asociacijos gali suteikti vertingų žinių, išteklių ir tinklų. Taip pat svarbu įtraukti verslo atstovus, kurie išreiškia norą bendradarbiauti. Įtraukiant verslo sektorių, galima užtikrinti, kad *Cyber Campus LT* iniciatyvos atitiktų realius rinkos poreikius ir skatintų inovacijas bei pritaikomumą praktikoje; iv) tarptautiniai partneriai. Kadangi kibernetinis saugumas yra globali iššūkis, *Cyber Campus LT* turėtų siekti bendradarbiauti su tarptautinėmis organizacijomis ir kitų šalių kibernetinio saugumo centrais. Tai galėtų padėti keistis žiniomis, patirtimi ir technologijomis, stiprinti Lietuvos pozicijas tarptautinėje kibernetinio saugumo bendruomenėje.

Viešinimas. Viešinimo kampanija padės skleisti žinią apie *Cyber Campus LT* egzistavimą ir tikslus tiek visuomenei, tiek verslo, akademinei ir viešojo sektoriaus bendruomenėms, užtikrinant, kad projekto svarba ir galimybės būtų plačiai žinomos. Efektyvus viešinimas skatins įvairių organizacijų, universitetų ir verslo sektoriaus atstovų įsitraukimą, stiprinant bendradarbiavimą bei pritraukiant naujus partnerius ir investicijas į kibernetinio saugumo sektorių. Viešinimo kampanijos metu pabrėžiant *Cyber Campus LT* pasiekimus ir naudą, bus galima užtikrinti ilgalaikį projektų palaikymą ir jų finansavimą, taip padedant užtikrinti veiklos tęstinumą ir plėtrą. Galiausiai strategiškai ir kryptingai viešinant veiklą *Cyber Campus LT* taptų kibernetinio saugumo ambasadoriumi visuomenėje taip skatinant kibernetinio saugumo sąmoningumą.

2.4. Bendradarbiavimo galimybės pasitelkiant *Cyber Campus LT*

Ekspertai teigia[10], kad nepakankamas viešojo ir privataus sektorių bendradarbiavimas didina neracionalių kibernetinį saugumą reglamentuojančių teisės aktų ir reikalavimų atsiradimą, neišnaudojamas kibernetinio saugumo specialistų rengimo potencialas, silpnėja tarpusavio pasitikėjimas, o tai įtakoja investuojamų kaštų į kibernetinio saugumo užtikrinimą privačioje infrastruktūroje didėjimą neišnaudojant visų įmanomų kibernetinio atsparumo priemonių valstybės mastu. Taip pat neišnaudojamas inovacijų potencialas. Specialistai išreiškia nuomonę, kad valstybinis sektorius dažnai teikia pirmenybę importuotiems produktams, nes akademinė bendruomenė ir verslo sektorius nepasiūlo brandžių ar inovatyvių vietinių kibernetinio saugumo sprendimų.

Viešojo ir privataus sektorių partnerystės elementai kibernetinio saugumo srityje susideda iš[10]:

1. Atsakomybių paskirstymo,
2. Suteikiamos ar gaunamos naudos (žinios, patirtis, garantijos, dalyvavimas teisinės bazės kūrime ar specialistų ruošime, prieigos prie valdomų išteklių ir pan.),
3. Ryšių palaikymo (tame tarpe pasitikėjimo ugdymo ar bendradarbiavimo krizės akivaizdoje).

Cyber Campus LT bendruomenė sukuria galimybę išgryninti viešojo ir privataus sektoriaus bendradarbiavimo kryptis ir sektorių partnerystės potencialo realizavimą kibernetinio saugumo srityje, sudarant palankias sąlygas

[10] Viešojo ir privataus sektorių partnerystė užtikrinant kibernetinį saugumą Lietuvoje (Verslo vadybos magistro baigiamasis darbas, J.Breivė, 2018 m.).

bendram neformaliam dialogui. Paraleliai siūlomos viešojo sektoriaus, verslo ir akademijos bendradarbiavimo kryptys *Cyber Campus LT* formate:

Švietimas. Kibernetinio saugumo akademijos (*Cybersecurity Academy*) programos kūrime dalyvautų viešojo sektoriaus (NKSC), verslo ir akademijos atstovai. Teikdami ekspertines žinias, padėtų sukurti praktinių 3-6 mėn. mokymų programą pagal naujausias kibernetines grėsmes ir technologijų tendencijas, remiantis ENISA kibernetinių kompetencijų matrica. Viešojo sektoriaus, įskaitant NKSC, privataus sektoriaus ir akademijos bendradarbiavimas būtų esminis *Cybersecurity Academy* programos sėkmės veiksnys. Viešasis sektorius užtikrintų, kad programa atitiktų nacionalinius saugumo standartus ir mokytų spręstų aktualiausias grėsmes, teikdami ekspertines žinias bei infrastruktūrą praktiniams mokymams. Privatus sektorius dalyvautų kuriant ir atnaujinant mokymo turinį, dalindamasis naujausiomis technologijomis ir praktiniais pavyzdžiais, kurie atitinka rinkos poreikius. Akademija prisidėtų teikdama teorines žinias ir mokslinius tyrimus, integruodama šiuolaikines kibernetinio saugumo tendencijas į mokymo programą, ir užtikrintų, kad studentai įgytų gilias žinias. Ši trilypė partnerystė užtikrintų, kad *Cybersecurity Academy* programa būtų išsami, inovatyvi ir orientuota į realius kibernetinius iššūkius bei rinkos poreikius.

Inovacijos. Adaptuojant GovTech modelį ir pritaikant jį nacionalio saugumo stiprinimui, sujungiami viešojo sektoriaus apibrėžti iššūkiai su komandomis iš verslo sektoriaus ir akademinės bendruomenės, turinčiomis inovatyvių idėjų ar sprendimų kibernetinio saugumo tematika, taip skatinant naujų technologijų kūrimą, bendradarbiavimo stiprinimą bei inovatyvių sprendimų pritaikymą realiose situacijose, užtikrinant greitesnį ir efektyvesnį reagavimą į grėsmes, gerinant viešojo sektoriaus kibernetinį atsparumą. Taip sukuriamos prielaidos ir fasilituojamas kibernetinio saugumo inovacijų diegimas ypatingos svarbos sektoriuose (kaip apibrėžiama TIS2 direktyvoje).

Lentelėje 1 nurodomas suinteresuotųjų šalių potencialus įsitraukimas į *Cyber Campus LT* įgyvendinamas veiklas pagal sektorius ir veiklos kryptis. Taip pat nurodomas NKSC vaidmuo veiklų įgyvendinime.

Lentelė 1. Siūlomas suinteresuotųjų šalių įsitraukimas į *Cyber Campus LT* įgyvendinamas veiklas.

	Verslas	Akademija	Viešasis sektorius	NKSC vaidmuo
Bendruomeniškumas	Taip	Taip	Taip	Vykdo/Administruoja
Renginiai, reminarai, dirbtuvės bendruomenės nariams	Taip	Taip	Taip	Vykdo/Administruoja
Metiniai renginiai	Taip	Taip	Taip	Vykdo/ Administruoja
Darbo grupių organizavimas/ koordinavimas	Taip	Taip	Taip	Vykdo
Švietimas	Taip	Taip	Taip	Vykdo/ Administruoja
Kibernetinio saugumo akademija	Taip	Taip	Taip	Vykdo
Moksleivių dirbtuvės	Taip	Taip	Taip	Vykdo
Stovyklos moksleiviams	Taip	Taip	Ne	Administruoja
Pratybos moksleiviams	Taip	Taip	Ne	Administruoja
Inovacijos	Taip	Taip	Taip	Administruoja
Govtech modeliu paremtas iššūkių projektai, kuriant inovacijas	Taip	Taip	Taip	Administruoja
Tarptautiškumas	Taip	Taip	Taip	Vykdo
Verslo mainų programa	Taip	Ne	Ne	Vykdo
Tarptautinė konferencija	Taip	Taip	Taip	Vykdo

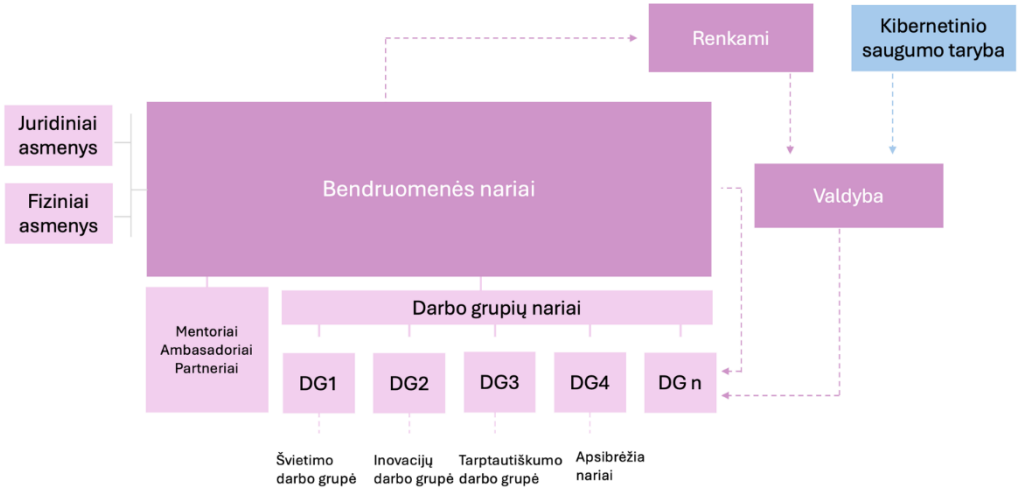
2.5. Bendruomenės struktūra ir jos veikimas

Bendruomenės nario apibrėžimas

Atsižvelgiant į Maltos nacionalinio koordinavimo centro (NKC-MT) pavyzdį[11] ir Reglamente (ES) 2021/887 nurodytą apibrėžtį, siūloma, kad *Cyber Campus LT* bendruomenės nariai turi turėti kibernetinio saugumo ekspertinių žinių bent vienoje iš toliau išvardintų sričių:

- **Akademija, moksliniai tyrimai arba inovacijos** – narys siekia mokslinių tyrimų ir inovacijų galimybių, kad sukurtų kibernetinio saugumo sprendimus ir (arba) išspręstų konkrečios srities problemas; arba aktyviai prisideda prie akademinių iniciatyvų kibernetinio saugumo srityje ir (arba) vadovauja akademinei institucijai, kuri siūlo specialius kibernetinio saugumo mokymus ir (arba) švietimą.
- **Produktų kūrimas** – narys kuria konkrečius kibernetinio saugumo sprendimus (techninę ir (arba) programinę įrangą) pramoniniais ir (arba) komerciniais tikslais.
- **Mokymas ir švietimas** – narys yra universitetas, mokymo įstaiga ir (arba) sertifikavimo įstaiga, vykdanti oficialias su kibernetine sritimi susijusias švietimo programas.
- **Saugumo valdymas ir operacijos** – narys pats valdo ir prižiūri savo informacijos saugumo programą (apimančią kibernetinę riziką), skirtą procesams ir kontrolės priemonėms įgyvendinti, reguliarioms peržiūroms ir bandymams atlikti, taip pat įvairioms kitoms saugumo veiklos funkcijoms, įskaitant reagavimą į incidentus, vykdyti.
- **Techninis standartizavimas ir specifikacijos** – narys dalyvauja rengiant, siūlant ir (arba) įgyvendinant kibernetinio saugumo oficialius ir techninius standartus bei specifikacijas nacionaliniu, ES arba pasauliniu lygmeniu.
- **Įstatymai, reglamentai ir etika** – narys dalyvauja kibernetinio saugumo teisėkūros, reguliavimo ir etinių aspektų, pavyzdžiui, kibernetinių nusikaltimų, duomenų privatumo, intelektinės nuosavybės ir skaitmeninio operacinio atsparumo, srityse.

Siekiant užtikrinti sėkmingą bendruomenės veiklą, siūlomas *Cyber Campus LT* veiklos valdymas ir misijomis grįstas veikimas (3 pav.).



3 pav. *Cyber Campus LT* veiklos valdymas ir misijoms grįstas veikimas.

[11] Malta-NCC

Cyber Campus LT bendruomenės nariais tampa tiek fiziniai, tiek juridiniai asmenys:

- atitinkantys aukščiau nurodytą srities apibrėžimą;
- aktyviai dalyvaujantys *Cyber Campus LT* veikloje (pvz. darbo grupėse, renginiuose, susitikimuose);
- registruoti vidinėje duomenų bazėje;
- veikiantys pasirinktoje rolėje (pvz. kaip partneriai, ambasadoriai, mentoriai, darbo grupių nariai);

Valdyba. *Cyber Campus LT* valdyba sudaroma iš renkamų bendruomenės narių ir Kibernetinio saugumo tarybos narių. Valdyboje patvirtinami prioritetiniai klausimai, iššūkiai spręstini darbo grupėse. Rekomenduojama valdybos narius periodiškai rotuoti. Bendruomenės narių įtraukimas į sprendimų priėmimą, didina narių motyvaciją, bei skatinta tarpusavio bendradarbiavimą.

Darbo grupės. Bendruomenės nariai kviečiami įsitraukti į darbo grupes, kurios formuojamos tiek pagal *Cyber Campus LT* strategines kryptis (švietimas, inovacijos, tarptautiškumas), tiek ir pagal pačių benduomenės narių keliamus iššūkius, probleminius klausimus (pvz. dalinimasis informacija apie grėsmių vektorius (angl. *Cyber Threat Intelligence (CTI*), NIS2, DORA ir pan.) ar dominančias tematikas (pvz. dirbtinis intelektas). Temos pasirinkimas leidžia grupei koncentruotis į aktualias kibernetinio saugumo problemas arba projektus, kuriuos jos nariai yra motyvuoti spręsti ir kuriems jie turi reikiamų kompetencijų. Remiantis Prancūzijos *Campus Cyber* pavyzdžiu, rekomenduojama, kad suformuotos darbo grupės veikla truktų ne ilgiau nei 18 mėn., galutinis veiklos rezultatas būtų sutartinis produktas naudingas ekosistemos stiprinimui. Darbo grupių veikimą įgalintų bendruomenės vadovas. Kiekviena darbo grupė turėtų savo moderatorių. Rekomenduojamas reguliarus dalinimasis darbo grupių veiklos rezultatais bendruomenėje.

Darbo grupių tikslai, pasitelkiant bendruomenės narių kompetencijas, gali būti keleriopi:

- konkrečių sprendimų ar įrankių sukūrimas naudingas ekosistemai;
- dalinimasis žiniomis bendruomenės narių kompetencijoms ugdyti;
- jaunųjų specialistų mentorystė;
- bendruomenės narių ryšių stiprinimas;

.

Mentoriai. Žinių ir patirties skleidėjai, padedantys užtikrinti bendruomenės narių profesinį augimą, inovacijų kūrimą bei ilgalaikę bendruomenės sėkmę.

Ambasadoriai. Bendruomenės veidai ir balsai, kurie padeda užtikrinti organizacijos matomumą visuomenėje.

Partneriai. Veiklos ir strateginių tikslų įgyvendinimo dalyviai, kurie prisideda savo ištekliais, žiniomis ir patirtimi. Jų vaidmuo yra svarbus ne tik stiprinant bendruomenės veiklą, bet ir plečiant jos įtaką bei pasiekiamumą.

Bendruomenės įgalinimas

Bendruomenės vadovo(-ės) vaidmuo yra būtinas aktyviai kibernetinio saugumo bendruomenei, jos įgalinimui. Vadovas (-ė) padeda kurti ryšius, skatina žinių dalijimąsi ir bendradarbiavimą, užtikrina narių įtraukimą ir motyvaciją. Ši rolė veikia kaip tiltas tarp skirtingų sektorių, padeda užtikrinti, kad bendruomenė būtų dinamiška, aktyvi ir atspari iššūkiams.

Bendruomenės vadovo (-ės) atsakomybės:

- Supranta ir atliepia viešojo, privataus sektoriaus ir akademinės bendruomenės poreikius.
- Incijuoja partnerystes ir žinių dalijimąsi tarp bendruomenės narių.
- Skatina bendradarbiavimą.
- Organizuoja nariams renginius.
- Aktyviai įtraukia narius į bendruomenines veiklas, darbo grupes.

Cyber Campus LT įgyvendinimo etapai yra orientuoti tiek į veiklos pradžią, tiek ir jos tęstinumą. Siekiant sukurti aktyvią ir įtraukiančią bendruomenę, įgyvendinimą išskyrėme į tris etapus:

I. Aktyvios bendruomenės formavimas, kurio metu siekiama suburti žmones su bendrais interesais ir tikslais, vertybėmis, skatinant dalijimąsi žiniomis ir patirtimi per įvairius formatus (pvz., informaciniai renginiai, tinklaveika, dirbtuvės, metiniai renginiai, išvažiuojamieji renginiai).

II. Bendruomenės narių įgalinimas įtraukiant į *Cyber Campus LT* valdybą, darbo grupes, virtualią platformą nuotoliniam dalyvavimui, siekiant, kad į bendruomenę būtų įtraukti specialistai iš visos Lietuvos. Proaktyvus narių įtraukimas kuriant ir vykdant *Cyber Campus LT* veiklas, taip užtikrinant ilgalaikį įsitraukimą ir tvarų veiklos vystymąsi.

III. Veikimo etape aktyvių bendruomenės narių indėlis padeda įgyventinti iškeltus tikslus (pvz. kibernetinio saugumo akademijos sukūrimas ir įgyvendinimas, sprendimai realioms problemoms, inovacijos ir jų diegimas).

2.6. Steigimas ir pozicionavimas

Steigiant *Cyber Campus LT* galimi keli scenarijai:

- *Cyber Campus LT* – NKSC iniciatyva (pvz. VŠĮ Investuok Lietuvoje ir Kurk Lietuvai programa), padalinys.
- VŠĮ *Cyber Campus LT* – įkuriama atskira viešoji įstaiga (pvz. VŠĮ Pinigų plovimo prevencijos kompetencijų centras[12]). Vis dėtlo, nepriklausomai nuo pasirinkto scenarijaus, rekomenduojama *Cyber Campus LT* pozicionuoti kaip atskirą nuo NKSC iniciatyvą, siekiant užtikrinti neutralumo ir lygiavertiškumo principų veikimą, kuriais ir vadovausis *Cyber Campus LT.* Toliau pateikiami alternatyvų privalumai ir trūkumai (Lentelė 2).

Lentelė 2. Palyginimas *Cyber Campus LT* steigimo scenarijų privalumų ir trūkumų.

Cyber Campus LT	
Privalumai	**Trūkumai**
Atskiras identitetas orientuotas bendruomeniškumo puoselėjimą, švietimą, inovacijas. Platesnės auditorijos pritraukimas iš akademijos, privataus sektoriaus ir tarptautinių partnerių.	*Cyber Campus LT* gali neturėti tvirto autoriteto ir įtakos, kurie būdingi nacionalinei vyriausybinei institucijai. Veiklos pradžioje pritrūks žinomumo, gali turėti įtakos gebėjimui skatinti nacionalines iniciatyvas.
Tinkamas formatas, jei siekiama dalintis informacija apie grėsmių vektorius.	Būnant NKSC dalimi, galimos kliūtys užmegzti partnerystes su privačiomis bendrovėmis ir tarptautinėmis institucijomis, kurios teiktų pirmenybę nepriklausomam subjektui.
Prieiga prie valstybinio finansavimo ir išteklių.	Dalyviai potencialiai gali žiūrėti kaip į reguliuotoją, baudėją, mažiau „atsiverti“, lyginant su VŠĮ.
VŠĮ Cyber Campus LT	
Privalumai	**Trūkumai**
Galimybė pritraukti finansavimą iš įvairesnių šaltinių. Finansavimas didžiąja dalimi privatus – palengvina administracinę, biurokratinę naštą.	Dalininkų surinkimas ir interesų derinimas.
Verslo požiūris ne į kaip reguliuotoją, lengvesnis ryšio, partnerysčių kūrimas tarp viešojo ir privataus sektoriaus.	Necentralizuotas finansavimas: sudėtingesnė prieiga prie valstybinio finansavimo ir išteklių, stiprus poreikis užsitikrinti atskirą finansinę paramą iš privačių šaltinių.
Daugiau laisvės pradėti novatoriškas programas, formuoti įvaizdį.	

[12] Pinigų plovimo prevencijos kompetencijų centras (amlcenter.lt)

3. Rizikų valdymas

Pradedant *Cyber Campus LT* veiklą, būtina įsivertinti galimas rizikas ir pasiruošti jų valdymui. Iniciatyva gali susidurti su įvairiomis iššūkių sritimis, įskaitant bendruomenės įsitraukimą, finansavimą, tarptautinį bendradarbiavimą ir identiteto klausimą. Lentelėje 3 pateikiamos identifikuotos rizikos, galimi veiksmai jų valdymui, užtikrinant iniciatyvos sėkmę ir tęstinumą.

Lentelė 3. Rizikų valdymo galimybės

Rizika	Paaiškinimas	Valdymas
Bendruomenės įsitraukimas	Žemas potencialių narių suinteresuotumas, viešojo ir privataus sektoriaus atstovai neįžvelgs reikšmingos naudos dalyvauti *Cyber Campus LT* veikloje.	✓ Reguliari komunikacija ir veiklos, naudingas, įtraukus turinys. ✓ Įtraukimas į sprendimų priėmimo procesus ir atvirumas. ✓ Politinis palaikymas.
Finansavimo trūkumas	Negautas Skaitmeninės Europos programos ir/arba nacionalinis finansavimas.	✓ Finansavimo šaltinių diversifikacija. ✓ Efektyvus resursų valdymas. ✓ Strateginis partnerių pritraukimas. ✓ Laiku ir tinkamai paruošta paraiška Skaitmeninės Europos programai.
Tarptautinio bendradarbiavimo trūkmas	Mažas Lietuvos kibernetinio saugumo potencialo matomumas pasaulyje.	✓ Aktyvi partnerysčių paieška. ✓ Lietuvos žinomumo didinimas kibernetinio saugumo tematikoje.
Cyber Campus LT identitetas	Tapatybės painiava, *Cyber Campus* LT ir NKSC vaidmenys gali būti nesuprantami suinteresuotosioms šalims.	✓ *Cyber Campus LT* išorinis pozicionavimas nesiejant tiesiogiai su NKSC. ✓ Aiški komunikacija. ✓ Viešosios įstaigos statusas.
Interesų konfliktas	Nesutampantys viešojo ir privataus sektoriaus prioritetai.	✓ Aiškus tikslų ir vaidmenų apibrėžimas. ✓ Reguliarus dialogas ir bendradarbiavimas. ✓ Skaidrumas *Cyber Campus LT* veikloje.

4. Poveikis

4.1. Nauda nariams

Sėkmingai kibernetinio saugumo ekosistemai reikalingas platus bendradarbiavimas tarp įvairių suinteresuotųjų šalių – atskirų specialistų, verslo, akademijos ir viešojo sektoriaus. Kiekviena iš šių grupių turi specifinių poreikių ir jų atliepimo galimybių, kurių išnaudojimas gali prisidėti prie sprendimų kūrimo ir įgyvendinimo. Lentelėje 4 pateikiamos naudos, kurias kiekviena iš grupių gali gauti iš aktyvaus dalyvavimo *Cyber Campus LT* veiklose.

Lentelė 4. Naudos *Cyber Campus* LT bendruomenės nariams

Specialistams	Verslui	Akademijai	Viešajam sektoriui
Tinklaveika ir atvira visiems erdvė susitikimams	Rinkos poreikius atitinkantys specialistai	Erdvė išbandyti idėjas sprendžiant realius kibernetinio saugumo iššūkius	Erdvė išgryninti viešojo ir privataus sektoriaus bendradarbiavimo kryptis
Kompetencijų kėlimas	Susipažinimas ir prieiga prie užsienio rinkos	Ekspertinių žinių taikymas kibernetinio saugumo inovacijų kūrime ir taikyme	Viešojo ir privataus sektoriaus partnerystės potencialo realizavimas kibernetinio saugumo srityje
Aktualių problemų iškėlimas ir sprendimai naudingi ekosistemai	Partnerysčių kūrimas		

4.2. Ekosistemai

Tikslingesnė politika ir valdymas. Organizuota bendruomenė gali pasisakyti už geresnę kibernetinio saugumo praktiką ir politiką, daryti įtaką sprendimų priėmėjams ir skatinti teigiamus pokyčius kibernetinio saugumo reguliavimo srityje ir ekosistemoje.

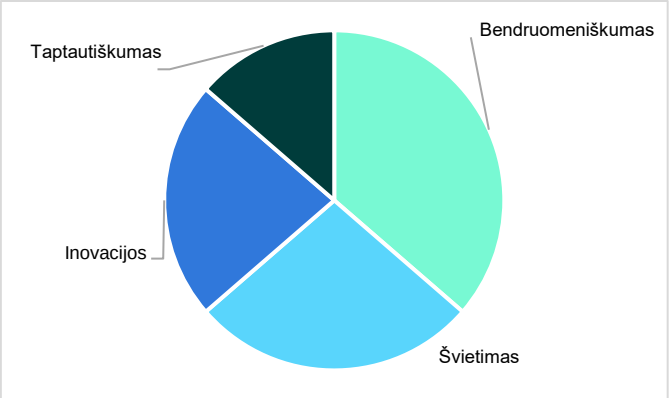
Kibernetinis visuomenės sąmoningumas ir kultūrinis pokytis. Jaunosios kartos kibernetinio sąmoningumo ugdymas turi potencialo prasiskverbti ir išplisti plačiau visuomenėje. Savo ruožtu didėtų visuomenės ir organizacijų suvokimas apie kibernetinio saugumo svarbą, taip kuriant ilgalaikę kibernetinio saugumo kultūrą Lietuvoje.

Investicijų pritraukimas. Centralizuota, tarptautiniu mastu žinoma kibernetinio saugumo bendruomenė turi potencialo paskatinti ir prisidėti prie investicijų pritraukimo kibernetinio saugumo srityje.

Stiprinamas nacionalinis saugumas. Aktyvi ir stipri bendruomenė, suteikia galimybes kurtis stipriam, skaidriam ir efektyviam, pasitikėjimu grįstam bendradarbiavimui tarp viešojo ir privataus sektoriaus kibernetinio saugumo srityje. Sukuriamos prielaidos operatyviai reaguoti į besikeičiančias kibernetinio saugumo grėsmes ir technologijas. Kibernetinio saugumo srities ankstyvasis ugdymas ir profesinis mokymas prisideda prie aukštos kvalifikacijos technologinės darbo jėgos ugdymo ir skatina tolesnę technologinę pažangą.

5. Grįžtamasis ryšys

Cyber Campus LT koncepcijos pristatymo renginyje 2024 m. rugpjūčio 27d. dalyvavo 75 ekosistemos dalyviai iš viešojo sektoriaus, verslo ir akademijos. Anoniminėje apklausoje po renginio, kurioje dalyvavo 20 suinteresuotų pusių respondentų, *Cyber Campus LT* siūlymo patrauklumas ir aktualumas vertintas labai gerai: vidutiniškai 4.5 ir 4.6 balo atitinkamai iš penkių galimų. Paklausus, kuri *Cyber Campus LT* strateginė kryptis apklausos dalyviams atrodo patraukliausia (t.y. matytų save toje veikloje dalyvaujant?), nurodė, kad bendruomeniškumas ir jo puoselėjmas pasirodė patraukliausi (4 pav.). Ekosistemos dalyviai išsakė poreikį žinoti, kada bus pradėta *Cyber Campus LT* veikla, kaip tapti nariais, kokie tolesni žingsniai. Visa tai rodo ekosistemos žaidėjų susidomėjimą ir poreikį *Cyber Campus LT* bendruomenės būrimui.



4 pav. Strateginių krypčių patrauklumas tarp kibernetinio saugumo ekosistemos dalyvių.

Cyber Campus LT koncepcija yra perduota NKSC prie Krašto apsaugos ministerijos, siekiant tolesnio įgyvendinimo.

Rasa Mončiunskaitė
Projekto vadovė

+370 699 69425
info@kurklt.lt

Dominykas Kugelevičius
Projekto vadovas

Upės str. 23,
08128, Vilnius,
Lithuania

www.kurklt.lt