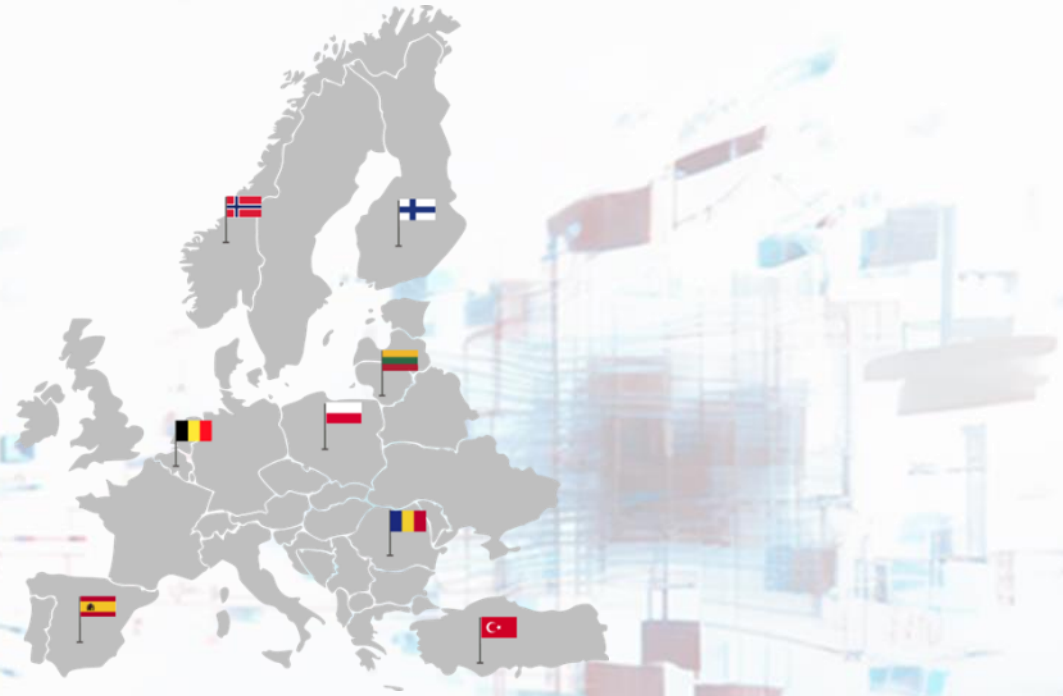
Co-funded by the European Union

MAŽŲ IR VIDUTINIO DYDŽIO ĮMONIŲ KIBERNETINIO SAUGUMO POKYČIŲ AGENTŲ MOKYMO KELIO STRUKTŪRA

CYBER AGENT 2024-06-30

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732



2 darbo paketas: CyberAgent koncepcija ir struktūros projektavimas

2.3 rezultatas: Mažų ir vidutinio dydžio (MVĮ) įmonių kibernetinio saugumo pokyčių agentų mokymo kelio struktūra

2 darbo paketo lyderis – Olemisen Balanssia ry
2.4 rezultato lyderis – Vilniaus universitetas

„MVĮ kibernetinio saugumo pokyčių agentai“ projektas remiamas pagal Erasmus+ programą.

TURINYS

SANTRUMPOS

AMĮ – Aukštojo mokslo institucijos (HEI – Higher Education Institutions)

CBL – Iššūkiais grindžiamo mokymosi modelis (angl. CBL, Challenge-Based Learning Model)

CL – Mokymosi bendradarbiaujant modelis (angl. CL, Cooperative Learning Model)

ECTS – Europos kreditų perkėlimo ir kaupimo sistema (angl. ECTS, European Credit Transfer and Accumulation System)

EK – Europos Komisija

EKS – Europos kvalifikacijų sąranga (angl. EQF, European Qualifications Framework)

GICL – Vadovaujamo tyrimo mokymosi bendradarbiaujant modelis (angl. GICL, Guided Inquiry Collaborative Learning Model)

MVĮ – Mažos ir vidutinio dydžio įmonės (ang. SME, Small and Medium Enterprises)

PBL – Projektais grindžiamo mokymosi modelis (angl. PBL, Project-Based Learning Model)

PMĮ – Profesinio mokymo institucijos (angl. VET, Vocational Education Institutions)

POGIL – Į procesą orientuotas mokymosi modelis (angl. POGIL, Process Oriented Guided Inquiry Learning Model)

VMA – Virtuali mokymosi aplinka (angl. OLE, Online Learning Environment)

PAVEIKSLĖLIŲ SĄRAŠAS

LENTELIŲ SĄRAŠAS

ĮVADAS

Šios ataskaitos tikslas – parengti ir aprašyti naujus profesinio mokymosi būdus (kelius), skirtus Europos MVĮ (mažų ir vidutinio dydžio įmonių) darbuotojų kibernetinio saugumo įgūdžiams tobulinti.

Remiantis MVĮ kibernetinio saugumo pokyčių agentų mokymo poreikių nustatymo rezultatais, išanalizuoti išoriniai ištekliai, susiję su mokymosi rezultatais žinių, įgūdžių ir kompetencijų srityse. Išanalizavus nustatytus mokymosi rezultatus, šioje ataskaitoje pateikiamos gairės dėl dviejų tipų mokymo programų, atitinkančių EQF (Europos kvalifikacijų sąrangos) 4–6 lygius, siekiant apimti įgūdžių ir žinių spektrą, reikalingą projekto tikslinėms grupėms – MVĮ darbuotojams ir studentams, ir pritaikyti mokymo rezultatus prie skirtingų mokymų dalyvių išsilavinimo ir profilio.

- EQF 4-5 lygis bus skirtas MVĮ darbuotojams, neturintiems aukštojo mokslo išsilavinimo, taip pat profesinio mokymo įstaigų (PMĮ) studentams. Šis lygis suteiks pagrindines kibernetinio saugumo žinias ir įgūdžius, o kai kurie moduliai bus šiek tiek specializuoti..
- EQF 5-6 lygis bus skirtas MVĮ darbuotojams, turintiems tinkamą išsilavinimą šiam lygiui įgyvendinti, ir aukštųjų mokyklų studentams. Šiame lygyje bus vykdoma sudėtingesnė ir pažangesnė mokymo veikla.

Buvo nuspręsta atnaujinti EKS lygius iki 4-6, kad jie ne tik apimtų platų mokymosi rezultatų spektrą, kaip minėta anksčiau, bet ir sudarytų galimybę pereiti iš vienos mokymo programos į kitą, kad 4 lygį pasiekę profesinio mokymo studentai ir darbuotojai galėtų kelti kvalifikaciją iki 6 lygio.

1 pav. Iliustracinėje schemoje, atitinkančioje EK gaires, pavaizduoti EKS lygiai, vaizdžiai pristatantys švietimo sistemą.[1]

Mokymo programoje atsižvelgiama į mokymosi rezultatus ir poreikį mokyti MVĮ darbuotojus kelti kvalifikaciją, kad jie galėtų atlikti MVĮ kibernetinio saugumo pokyčių agentų vaidmenį, ir mokyti aukštųjų mokyklų ir profesinio mokymo įstaigų studentus, kad jie galėtų atlikti šį vaidmenį pabaigę studijas. Kiekvieną mokymo programą sudaro aštuoni moduliai, apimantys keturias potemes:

- Techniniai įgūdžiai: atnaujintos žinios apie kibernetinio saugumo grėsmes ir susijusius teisinius klausimus. Praktinės žinios, kaip spręsti kibernetinio saugumo problemas.
- Analitiniai įgūdžiai: kritinio mąstymo nuostatos. Gebėjimas analizuoti ir suprasti vietines grėsmes, jų kilmę, rizikos grupes ir pan.
- Rizikos valdymas: mokymasis pateikti ir aprašyti MVĮ darbo vietų kibernetinio saugumo procedūras. Savo MVĮ darbo vietos kibernetinio saugumo vadovo sukūrimas ir jo laikymosi užtikrinimas.
- Organizaciniai įgūdžiai: kaip MVĮ darbo vietose įdiegti naujas kibernetinio saugumo procedūras ir darbo metodus. Vadovų paramos kibernetinio saugumo srityje vykdymas.

Be to, kuriant Europos MVĮ kibernetinio saugumo įgūdžių tobulinimo mokymosi būdus (kelius), svarbu yra tai, kaip bus įgyvendinami mikrokreditai (angl. micro-credentials). Naudojant mikrokreditus turi būti nurodyti mokymosi rezultatai (žinios, įgūdžiai ir kompetencijos), kursų turinys, mokymas (žinios, įgūdžiai ir kompetencijos), žaidybinimo elementai, mokymų trukmė ir ECTS (Europos kreditų perkėlimo ir kaupimo sistema) kreditų skaičius. Kad mikrokreditai atitiktų

[1] https://europa.eu/europass/en/description-eight-eqf-levels

savo paskirtį, jie turi būti teikiami bendradarbiaujant aukštosioms mokykloms, profesinio rengimo įstaigoms ir privačioms kibernetinio saugumo sektoriaus įmonėms.

Mikro-sekcijos (angl. micro-sections) suteikia besimokantiesiems daugiau laisvės pasirinkti modulius ar jų dalis ir nuspręsti, kokio lygio pažymėjimo jiems reikia: dalyvavimo pažymėjimo arba kurso baigimo pažymėjimo su sertifikavimo testu, t. y. įrodymo, kad kursas baigtas ir įgyta tam tikra kompetencija. Kurso baigimo pažymėjimai išduodami už baigiamojo testo išlaikymą, surinkus ne mažiau kaip 75 % balų, o dalyvavimo pažymėjimai išduodami už dalyvavimą tiesioginiuose, mišriuose ar nuotoliniuose konkrečių temų/modulių mokymuose. Tokia praktika ne tik didina mokymų pritaikomumą ir efektyvumą, bet ir skatina mokymosi motyvaciją, suteikia aiškią vertės perspektyvą dalyvių karjerai ir tolesniam tobulėjimui.

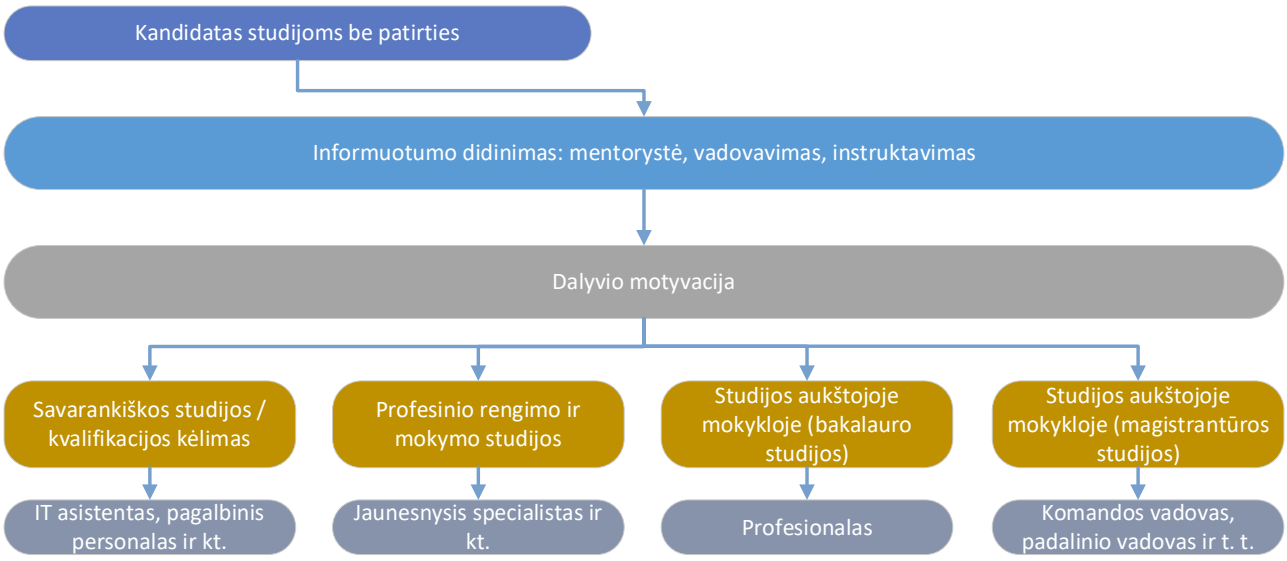
Iš esmės šioje ataskaitoje pateikiamos išsamios CyberAgent modulių rengimo gairės, įskaitant studijų ir profesinės veiklos krypčių turinio aprašymą, mokymo ir vertinimo metodikas bei mokymo programos rengimo veiksmų planą.

1. STUDIJŲ KELIAS

Mokymo(si) kelias – tai visa dalyvio kelionė nuo to momento, kai jis supranta, kad jam reikia tobulinti savo įgūdžius, pradėti ir baigti mokymus, iki to momento, kai jis baigia mokytis ir pradeda taikyti gautas žinias. Mokymosi kelias susideda iš 3 etapų:

- Pasiruošimas studijoms (angl. pre-learning),
- Studijos,
- Karjeros kelias po studijų (angl. post-learning).

Pasiruošimo studijoms etapas pavaizduotas toliau pateiktame paveikslėlyje.



2 pav. Mokymosi kelias prieš pradedant studijas

Šis mokymosi kelias gali būti pritaikytas ir MVĮ darbuotojams. Paveikslėlyje pavaizduota, kad dalyvis pats priima sprendimą mokytis arba jį paveikia informavimo kampanija ir jis supranta mokymosi naudą, galimybes ir karjeros galimybes, kurias galima įgyti pabaigus mokymus.

Taip pat buvo pasiūlytas mokymosi kelias kaip tipinis modulis naudojant VMA (virtuali mokymosi aplinka) struktūrą. Atlikus literatūros analizę ir keletą projektų, kuriuose buvo taikomas mikrokreditų principas[2],[3],[4] siūloma, kad kiekvieną CyberAgent modulį sudarytų 1-5 ECTS (kiekvienas ECTS sudaro 25-30 valandų darbo krūvio), jis pradedamas įvadu, o vėliau suskirstomas į temas, t. y. potemes.

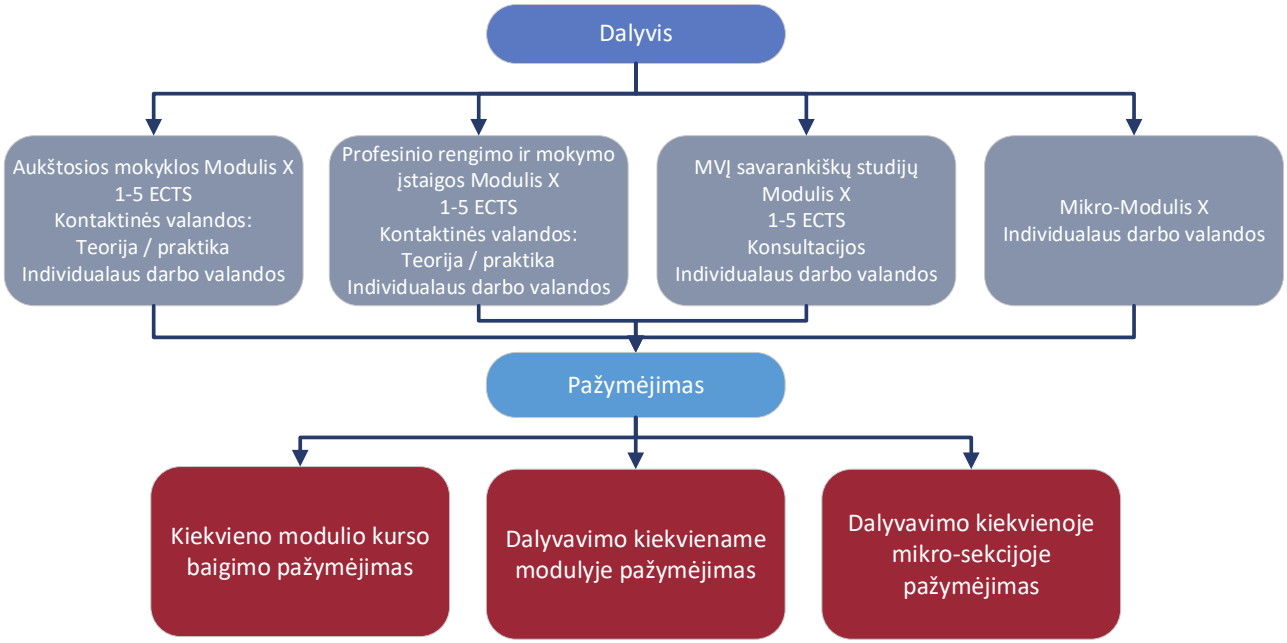
Temų pabaigoje pateikiamas savęs vertinimo testas, sudarytas iš kelių klausimų. Modulio mokomoji medžiaga turėtų sudaryti 6-8 temas, kurių kiekvienoje yra 4-6 potemės. Kursas gali

[2] Nausėdaitė, R., Juška, V., Daunorienė, A., & Ukvalbergienė, K. (2022). Moving Forward and Beyond in Education: Concept of FLEXIBLE LEARNING PATHWAYS. In KTU leidykla "Technologija" eBooks. https://doi.org/10.5755/e01.9786090218204

[3] https://arqus-alliance.eu/call/arqus-microcredential-development-f2f-workshop/

[4] https://www.youtube.com/watch?v=ECH0VvHIyRI, https://ndma.lt/alta2023/

būti baigiamas žinių patikrinimu, kuris nėra privalomas. Taip MVĮ darbuotojams ir mokymo įstaigų mokiniams suteikiama galimybė įgyti ir pademonstruoti konkrečiame modulyje ar mokymo dalyje įgytas kompetencijas.



3 pav. Studijų struktūra

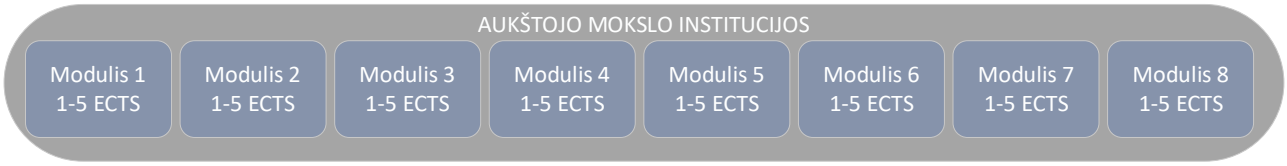
Mikrokreditai integruojami į mokymosi procesą vykdant šią pagrindinę veiklą:

- Mokymo modulių kūrimas: kiekvienas modulis turi būti kruopščiai parengtas atsižvelgiant į konkrečias žinias ir įgūdžius, reikalingus MVĮ sektoriuje, su aiškiais tikslais, mokymosi rezultatais, mokymo ir mokymosi metodais, kurso trukme.
- Praktinės užduotys ir projektai: besimokantieji atlieka praktines užduotis ir rengia projektus, kurie yra vertinami ir aiškiai įrodo įgytus įgūdžius.
- Aiškiai aprašyta žinių vertinimo strategija ir vertinimo kriterijai: kiekvieno modulio pabaigoje organizuojamas žinių vertinimas, kurio metu nustatoma, ar dalyvis pasiekė reikiamus mokymosi rezultatus ir ar jis gali gauti tai patvirtinantį pažymėjimą.

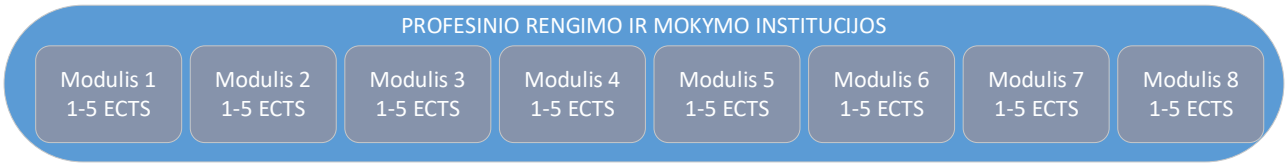
Kadangi projekto tikslinė grupė yra MVĮ darbuotojai, aukštųjų mokyklų ir profesinio mokymo įstaigų studentai, atsižvelgiant į besimokančiųjų galimybes ir poreikius, siūlomos keturių tipų studijos:

- Aukštųjų mokyklų studijos: 8 moduliai, kiekvienas po 1-5 ECTS, kuriuose yra kontaktinės valandos (teorija ir praktika) ir individualaus darbo valandos;
- Profesinio mokymo studijos: 8 moduliai, kiekvienas po 1-5 ECTS, kuriuose yra kontaktinės valandos (teorija ir praktika) ir individualaus darbo valandos;
- Savarankiškos studijos (MVĮ): 8 moduliai, kiekvienas po 1-5 ECTS, kuriuose yra konsultacijos (jei reikia) ir individualaus darbo valandos;

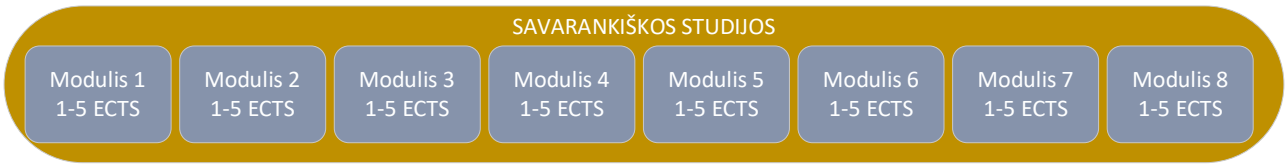
- Mikrokreditai: individualaus darbo valandos, priklausomai nuo pasirinktų temų skaičiaus.



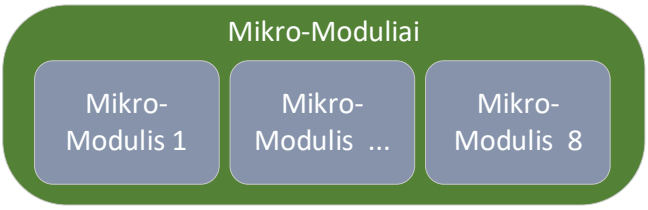
4 pav. Studijų struktūra aukštojo mokslo institucijoms



5 pav. Studijų struktūra profesinio mokymo institucijoms

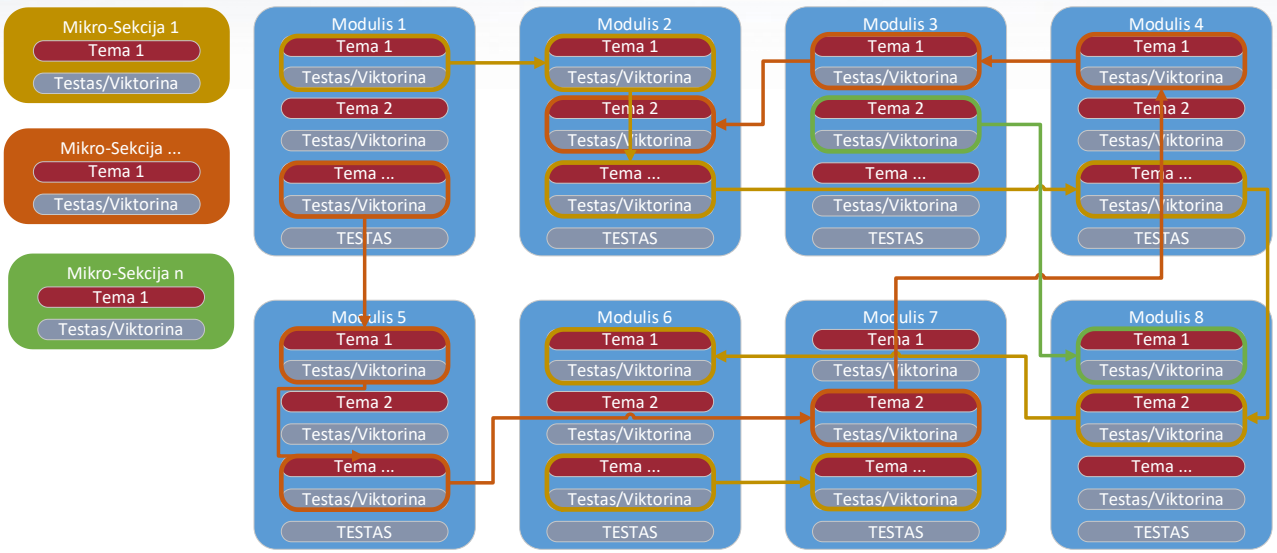


6 pav. Studijų struktūra savarankiškam mokymui



7 pav. Studijų struktūra mikro-moduliams

Aukštųjų mokyklų ir profesinio rengimo ir mokymo įstaigų studentai galės studijuoti po vieną 1-5 kreditų modulį. MVĮ galės studijuoti po vieną modulį arba galima pasiūlyti mikrosekcijas kaip kurso dalį.



8 pav. Mokymosi kelių sąsajos

Visų trijų tipų (aukštosios mokyklos, profesinio rengimo ir mokymo įstaigos, MVĮ) mokymuose studentas gali studijuoti 8 modulius. Mikro-modulių atveju studentas renkasi modulius savo nuožiūra.

Mikro-moduliai – tai trumpos arba ilgesnės apimties skaidriai vertinama mokymosi patirtis. Juos dalyvis gali rinktis kartu su užduotimis arba atskirai. Kiekvienas mikro-modulis vertinamas skirtingu mokymosi krūvio matu (pvz., ECTS) ir baigiamas galutiniu įvertinimu. Sėkmingai atlikę mikro-modulių atsiskaitymus besimokantieji gauna mikrokreditus.

Siūloma, kad kiekvienas aukštosios mokyklos programos modulis galėtų būti išskaidytas į vieną mikro-modulį, kuriame būtų numatytos specializuotos užduotys ir išsamus įgyvendinimo planas. Testų rezultatai gali būti vertinami naudojant ženklelius (angl. badges). Šiuose paveikslėliuose įterpiami metaduomenys, kuriuose išsamiai nurodomos su kiekvienu ženkleliu susijusios kompetencijos ir informacija apie jį turintį dalyvį.

Mikrokreditais (angl. micro-credentials) – tai įrašas apie mokymosi rezultatus, kuriuos dalyvis įgijo po nedidelės apimties mokymosi. Šie mokymosi rezultatai bus vertinami pagal skaidrius ir aiškiai apibrėžtus kriterijus. Mokymosi patirtis, kurią įgijus suteikiami mikrokreditai, skirta suteikti dalyviui konkrečių žinių, įgūdžių ir kompetencijų, atitinkančių visuomenės, asmeninius, kultūrinius ar darbo rinkos poreikius.[5],[6].

[5] Nausėdaitė, R., Juška, V., Daunorienė, A., & Ukvalbergienė, K. (2022). Moving Forward and Beyond in Education: Concept of FLEXIBLE LEARNING PATHWAYS. In KTU leidykla „Technologija“ eBooks. https://doi.org/10.5755/e01.9786090218204

[6] Council Recommendation of 16 June 2022 on a European Approach to Micro-Credentials for Lifelong Learning and Employability.” Official Journal of the European Union, vol. 2022/C, 16 June 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022H0627(02)&from=EN

2. KARJEROS KELIAS

Etapas pabaigus studijas gali būti vadinamas karjeros keliu po studijų. Projekto pradžioje buvo atlikta ESCO profesijų tyrimo analizė (Aprašyta ataskaitoje: D2.2 - Mažų ir vidutinio dydžio įmonių (MVĮ) kibernetinio saugumo pokyčių agentų mokymų poreikių nustatymo ataskaita). Trimis etapais atlikta analizė buvo skirta ištirti įvairias ESCO sistemoje išvardytas kibernetinio saugumo profesijas. Pirmajame etape iš **ESCO portalo** buvo atrinktos ir dokumentuotos su kibernetiniu saugumu susijusios profesijos, pabrėžiant atitinkamus jų įgūdžius, kompetencijas ir žinias. Šios profesijos apėmė tokias pareigybes kaip vyriausiasis IRT saugumo pareigūnas, skaitmeninės kriminalistikos ekspertas, įterptųjų sistemų saugumo inžinierius, etiškas įsilaužėlis, IRT atsparumo vadovas, IRT saugumo administratorius, IRT saugumo inžinierius, IRT saugumo vadybininkas ir žinių inžinierius. Kiekviena profesija buvo apibrėžiama pagal konkrečias pareigas ir sritis kibernetinio saugumo srityje, pradedant įmonės saugumo funkcijomis ir baigiant skaitmeninė kriminalistika, etišku įsilaužimu ir atsparumo planavimu.

Antrajame etape kiekvienai peržiūrėtai ESCO profesijai buvo užpildyta lentelė, kurioje išsamiai nurodytas profesijos pavadinimas ir pagrindinės pareigos. Tai buvo tokios užduotys kaip saugumo priemonių planavimas ir įgyvendinimas, pažeidžiamumo vertinimas, atsparumo ir atkūrimo po nelaimių modelių kūrimas ir žinių pritaikymas kompiuterinėse sistemose.

Trečiajame etape buvo siekiama susieti ESCO profesijas su atitinkamais mokymosi rezultatais, suskirstant juos į žinias, įgūdžius ir kompetencijas. Šis procesas padėjo suprasti apie išsilavinimo reikalavimus ir numatomus gebėjimus kiekvienai kibernetinio saugumo pareigybei, užtikrinant atitikimą pramonės standartams ir geriausios praktikos pavyzdžiams. Šiais etapais atlikta analizė suteikė vertingų įžvalgų tolesniems tyrimams.

ESCO: vyriausiasis IRT saugumo pareigūnas

ŽINIOS: IRT tinklo saugumo rizika, IRT saugumą reglamentuojantys teisės aktai, vidaus rizikos valdymo politika, organizacijos atsparumas, ...

ĮGŪDŽIAI: ugdyti duomenų konfidencialumą, užtikrinti, kad būtų laikomasi organizacijos IRT standartų, užtikrinti atitiktį teisiniams reikalavimams, ...

KOMPETENCIJOS: vadovauti avarinio atkūrimo pratyboms, palaikyti veiklos tęstinumo planą, valdyti IT saugumo reikalavimų laikymąsi, ...

ESCO: skaitmeninės teismo ekspertizės ekspertas

ŽINIOS: IRT tinklo saugumo rizika, IRT saugumo standartai, kompiuterinė ekspertizė.
kibernetinės atakos, ...

ĮGŪDŽIAI: mokyti apie duomenų konfidencialumą, rinkti duomenis teismo ekspertizės tikslais, nustatyti IRT saugumo riziką,nustatyti IRT sistemos trūkumus, ...

KOMPETENCIJOS: IT saugumo reikalavimų laikymasis, duomenų tvarkymas teisiniais klausimais, skaitmeninių prietaisų teismo ekspertizės atlikimas, ...

ESCO: įterptųjų sistemų saugumo inžinierius

ŽINIOS: daiktų internetas, kompiuterių programavimas, kovos su kibernetinėmis atakomis priemonės, įterptinės sistemos, ...

ĮGŪDŽIAI: analizuoti IRT sistemą, kurti srautų diagramas, apibrėžti saugumo politiką, kurti IRT įrenginio tvarkyklę, ...

KOMPETENCIJOS: neatsilikti nuo naujausių informacinių sistemų sprendimų, valdyti IT saugumo reikalavimus, stebėti sistemą, ...

ESCO: etiškas įsilaužėlis

ŽINIOS: teisiniai reikalavimai IRT produktams, įsiskverbimo testavimo priemonės, programinės įrangos anomalijos, IRT testavimo automatizavimo priemonės, ...

ĮGŪDŽIAI: kurti kodo išnaudojimo įrankius, atlikti IRT auditą, atlikti programinės įrangos testus, nustatyti IRT saugumo riziką, ...

KOMPETENCIJOS: kritiškai spręsti problemas, analizuoti organizacijos kontekstą, stebėti sistemos veikimą, ...

ESCO: IRT saugumo administratorius

ŽINIOS: interneto valdymas, mobiliųjų įrenginių valdymas, operacinės sistemos, organizacinis atsparumas, kokybės užtikrinimo metodikos, ...

ĮGŪDŽIAI: aiškinti techninius tekstus, prižiūrėti IRT tapatybės valdymą, prižiūrėti duomenų bazių saugumą, ...

KOMPETENCIJOS: aiškinti techninius tekstus, prižiūrėti IRT tapatybės valdymą, prižiūrėti duomenų bazių saugumą, ...

ESCO: IRT saugumo inžinierius

ŽINIOS: kibernetinis saugumas, naujos technologijos, informacijos architektūra, informacijos saugumo strategija, ...

ĮGŪDŽIAI: kurti informacijos saugumo strategiją, šviesti duomenų konfidencialumo klausimais, užtikrinti informacijos saugumą, ...

KOMPETENCIJOS: nustatyti duomenų kokybės kriterijus, apibrėžti techninius reikalavimus, tvarkyti užduočių apskaitą, sekti naujausius informacinių sistemų sprendimus, ...

ESCO: IRT saugumo vadybininkas

ŽINIOS: IRT saugumo standartai, IRT sistemų naudotojų reikalavimai, daiktų internetas, atakų vektoriai, kompiuterinė ekspertizė, ...

ĮGŪDŽIAI: apibrėžti saugumo politiką, parengti informacijos saugumo strategiją, parengti IRT saugumo prevencijos planą, ...

KOMPETENCIJOS: vadovauti avarinio atkūrimo pratyboms, prižiūrėti IRT tapatybės valdymą, valdyti IT saugumo reikalavimų laikymąsi, ...

ESCO: IRT atsparumo vadybininkas

ŽINIOS: kibernetinio saugumo vidaus, rizikos valdymo politika, organizacinis atsparumas, ...

ĮGŪDŽIAI: kurti informacijos saugumo strategiją, atlikti IRT auditą, nustatyti IRT saugumo riziką, ...

KOMPETENCIJOS: teisinių nuostatų laikymasis, vadovavimas atkūrimo po avarijos pratyboms, IT saugumo reikalavimų laikymasis, ...

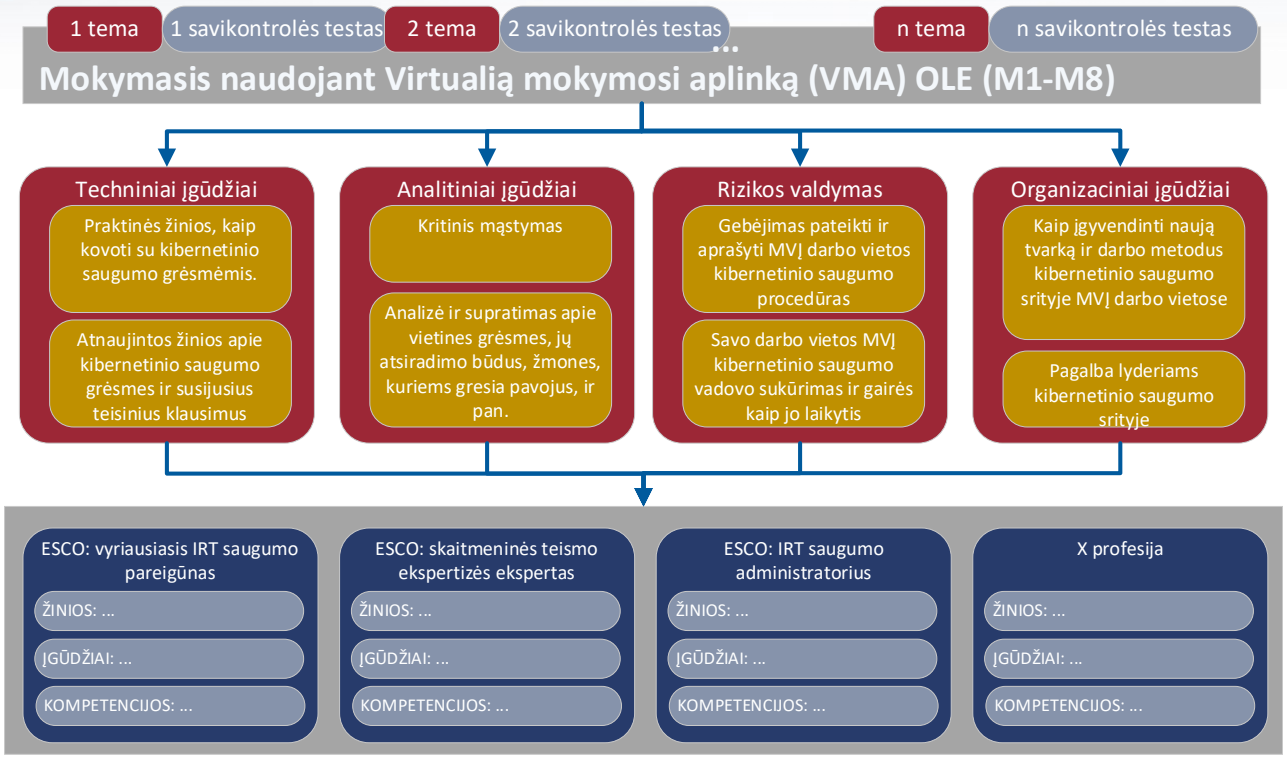
ESCO: žinių inžinierius

ŽINIOS: duomenų bazių kūrimo įrankiai, informacijos išskyrimas, informacijos struktūra, natūralios kalbos apdorojimas, dirbtinio intelekto principai, ...

ĮGŪDŽIAI: naudoti konkrečiai programai skirtą sąsają, naudoti duomenų bazes
naudoti žymėjimo kalbas, ...

KOMPETENCIJOS: kurti semantinius medžius, apibrėžti techninius reikalavimus, valdyti IRT semantinę integraciją, ...

9 pav. Ankstesnėje ataskaitoje apibrėžtos ESCO profesijos



10 pav. Galimi vėlesnio mokymosi keliai

10 paveiksle pavaizduotos galimi karjeros keliai, kurių galima siekti baigus studijas virtualioje mokymosi aplinkoje (VMA) (angl. online learning environment, OLE) (aukštoji mokykla, profesinio rengimo įstaiga, maža ir vidutinio dydžio įmonė) ir įgijus įgūdžių, atitinkančių ESCO profesijas.

Geriau suvokdami karjeros galimybes, aukštųjų mokyklų ir profesinio rengimo įstaigų studentai, studijuojantys kibernetinį saugumą, aiškiau suvoks karjeros galimybes ir galės pasirinkti tolesnę studijų sritį arba dirbti įmonėse konkrečiose pareigose, o IT ir kiti studentai galės pasirinkti CyberAgent modulius kaip individualius studijų modulius, taip tobulindami savo studijų srities kompetencijas, pavyzdžiui, organizacinius ir rizikos valdymo įgūdžius ir kt.

MVĮ darbuotojai turės galimybę kelti kvalifikaciją ir tobulinti savo kompetencijas darbo vietoje. Remdamiesi parengtu karjeros keliu ir rekomenduojamomis karjeros galimybėmis, kitų sričių MVĮ darbuotojai galės persikvalifikuoti į kibernetinio saugumo sritį.

Numatoma aktyviau įtraukti ir studentus, ir MVĮ darbuotojus, integruojant mentorystės schemas, organizuojant informacijos sklaidos renginius, seminarus (projekte numatyta 6 bendri visų partnerių organizuojami seminarai, taip pat kiekvieno partnerio organizuojamos sklaidos kampanijos), kviečiant verslo ir kibernetinio saugumo atstovus, bendradarbiaujant su socialiniais partneriais ir CyberAgent tinklu, siūlant studentams stažuotes ir pan. Be to, mūsų įvairovės iniciatyvomis, įskaitant tikslines informavimo ir paramos programas, siekia sustiprinti moterų dalyvavimą, ir taip kurti įtraukią kibernetinio saugumo darbo aplinką.

Suderinę CyberAgent mokymo modulius su ESCO profesijų reikalavimais, tikimės, kad dalyviai įgytų reikiamų žinių ir įgūdžių sėkmingai karjerai kibernetinio saugumo srityje. Norėdami įvertinti

CyberAgent mokymų dalyvių profesinę sėkmę, planuojama organizuoti apklausas prieš mokymus, po mokymų ir praėjus 3 mėnesiams po mokymų, siekiant išsiaiškinti, kaip jų įgūdžiai prisideda prie organizacijų, kuriose jie dirba, kibernetinio saugumo. Apklausos bus integruotos į mokymo platformą ir bus automatiškai siūlomos kursų dalyviams prieš pradedant kursus, kursų pabaigoje, siekiant įvertinti pažangą ir įvertinti kursus bei jų kokybę. Trečioji apklausa bus skirta išsiaiškinti, ar įvyko kokių nors pokyčių dalyvių karjeroje.

3. MOKYMO METODAI

Remiantis Vilniaus universiteto (VU) Informacijos sistemų ir kibernetinio saugumo studijų programos, Timtal ir Moisil Buzau studijų programų pedagoginių metodų ir išorinės literatūros analize, rekomenduojame CyberAgent mokymų metu naudoti inovatyvius mokymo metodus. Šie metodai galėtų būti įtraukti į studijų modulius, atsižvelgiant į kiekvieno modulio struktūrą ir kitus aspektus.[7]

1 lentelė. Rekomenduojami mokymo metodai

Kategorija	Išsamesnė informacija
Paskaita ir tiesioginis mokymas	- **Teorinės paskaitos**: pagrindinės sąvokos ir teorijos. - **Kviestiniai lektoriai** (sertifikuoti specialistai: Sertifikuotas informacinių sistemų saugumo specialistas (CISSP), Sertifikuotas informacinių sistemų auditorius (CISA), Sertifikuotas informacijos saugumo vadybininkas (CISM), CompTIA Security+, Sertifikuotas etiškas įsilaužėlis (CEH), GIAC Informacijos saugumo pagrindų sertifikuotas (GSEC) specialistas, Sertifikuotas sistemų saugumo specialistas (SSCP), CompTIA pažengęs saugumo specialistas (CASP+), GIAC sertifikuotas incidentų valdymo specialistas (GCIH), etiško įsilaužimo profesionalai: Offensive Security Certified Professional (OSCP)).
Praktika pagrįstas mokymasis	- **Praktinės užduotys**: praktiniai eksperimentai ir praktinės užduotys. - **Praktiniai (angl. hands-on) užsiėmimai**: Realiomis situacijomis grįstos užduotys ir interaktyvios užduotys. - **Techninė vaizdo įrašų analizė**: vaizdo įrašų turinio analizė, skirta techniniams įgūdžiams lavinti. - **Simuliuojamos aplinkos**: o Debesų aplinkai skirtos prieglobos mašinos. o Atliekamos atakos prieš tikslinę mašiną. o Atakų planavimo ir vykdymo mašina (angl. attack box).
Vertinimas ir įsivertinimas	- **Viktorinos, žaidimai, „Daryk ir nedaryk“** Įtraukiantys ir interaktyvūs vertinimai.

[7] Teaching Cybersecurity: A Project-Based Learning and Guided Inquiry Collaborative Learning Approach https://scholar.utc.edu/cgi/viewcontent.cgi?article=1945&context=theses

	- **Savikontrolės testai**: vertinimo testai, skirti besimokantiesiems įsivertinti žinias temų pabaigoje.
Savarankiškos studijos	- **Savarankiškas mokymasis**: šis metodas palaiko individualius mokymosi kelius ir gali būti sustiprintas skaitmeniniais ištekliais ir moduliniu turiniu, prie kurio studentai gali prisijungti pagal poreikį.
Bendradarbiavimas ir mokymasis tarpusavyje	- **Mokymasis bendradarbiaujant, komandinis darbas:** grupiniai projektai ir bendros užduotys. - **Kolegų mokymas ir mokymasis**: besimokantieji moko ir mokosi vieni iš kitų. - **Grupinė ir (arba) individuali mentorystė**: labiau patyrusių asmenų teikiamos rekomendacijos.
Technologijomis pagrįstas mokymasis	- **Kibernetinio saugumo mokymosi platformos naudojimas**: besimokančiųjų įtraukimas žaidimų elementais mokymosi platformose. - **Kibernetinio saugumo įgūdžiams tobulinti skirtos varžybos „Capture the flag“**: konkurenciniai renginiai, skirti kibernetinio saugumo įgūdžiams stiprinti. - **Konkursai:** konkursų metu tikrinami studentų įgūdžiai ir žinios praktinėje, taikomojoje aplinkoje, o jų konkurenciniu būdu įvertinamos jų kompetencijos.
Bendruomenės ir visuomenės įtraukimas	- **Šviečiamieji renginiai**: specialūs renginiai organizuojami tokių iniciatyvų, kaip kibernetinio saugumo mėnuo, metu. - **Vieši pristatymai**: seminarai, konferencijos ir internetiniai seminarai. - **Socialiniai tinklai**: socialinės žiniasklaidos ir tinklų naudojimas mokymuisi ir dalyvavimui. - **Dienos stovykla**: paprastai apima įtraukiančius, stovykloje vykstančius renginius, kuriuose gali vykti seminarai, paskaitos ir suteikiamos galimybės užmegzti ryšius.
Inovatyvūs mokymosi modeliai	- **BSCS 5E mokymo modelis (BSCS 5E Instructional Model (5Es))** – 5Es orientuotas į šiuos etapus, kuriuos sudaro: įsitraukimas, tyrinėjimas, aiškinimas, įtvirtinimas, vertinimas. - **Iššūkiais grindžiamas mokymosi modelis (Challenge-Based Learning Model (CBL))** –

	ankstyvasis CBL įgyvendinimas pateikia pagrindą, kurį sudaro šeši etapai: iššūkio apibūdinimas, idėjų generavimas ir smegenų šturmas, įvairių perspektyvų, kurios kelia klausimus ir palaiko, peržiūra, geriausių sprendimų tyrimas ir peržiūra, hipotezių tikrinimas, rezultatų ir išvadų pasidalijimas. - **Mokymosi bendradarbiaujant modelis** (Cooperative Learning Model (CL)) – panašus į 5E ir CBL modelius, mokymasis bendradarbiaujant skatina aktyvų mokymąsi mažose grupėse, o studentai gauna atlygį už savo pasiekimus, kuris gali būti įvertinimas, materialinis atlygis, pavyzdžiui, sertifikatas ar stipendija, arba mokytojo patvirtinimas. - **Projektais grindžiamo mokymosi modelis** (Project-Based Learning Model (PBL)) – projektais grindžiamas mokymasis ir probleminis mokymasis naudoja tą pačią PBL santrumpą ir abu yra orientuoti į problemų sprendimo, kritinio mąstymo, komandinio darbo, bendravimo ir kūrybiškumo įgūdžių tobulinimą, tačiau juos sudaro skirtingi etapai: savarankiškas ir grupinis tyrimas, kūrimas ir pristatymas, analizės ir proceso vertinimas. - **Į procesą orientuotas mokymosi modelis (Process Oriented Guided Inquiry Learning Model (POGIL))** – pagal šį metodą studentai tyrinėja sąvoką (studentai sugalvoja sąvoką ir ją paaiškina); mokymosi ciklas užbaigiamas teorinės sąvokos taikymu. - **Vadovaujamo tyrimo bendradarbiavimu grįstas mokymosi modelis (Guided Inquiry Collaborative Learning Model (GICL))** – tai naujas metodas, iš esmės pagrįstas POGIL modeliu.

Siekiant užtikrinti, kad įvairios siūlomos mokymo strategijos turėtų kuo didesnį poveikį, rengiant išsamią modulio mokymo programą ir mokymo medžiagą, kiekvienas metodas bus atrinktas ir suderintas su konkrečiais kibernetinio saugumo modulių mokymosi tikslais. Papildomus metodus taip pat gali pasirinkti lektoriai / mentoriai, kurie ves CyberAgent mokymus. Mokymo medžiagos rengimo etape bus rengiami mokymai pilotinių mokymų dėstytojams, siekiant juos informuoti apie mokymo tikslus, eigą ir atsakomybę bei parengti juos veiksmingai dėstyti pgal CyberAgent programą. Pilotinių mokymų metu taip pat bus renkami besimokančiųjų ir

instruktorių atsiliepimai, kad būtų galima stebėti taikomų mokymo metodų veiksmingumą ir prireikus juos koreguoti.

Moduliai bus rengiami įvairiomis mokymo formomis:

- **nuotoliniu formatu**,
- **sinchroninio mokymosi būdu** (visapusiška mokytojo pagalba),
- ir **asinchroniniu mokymusi** (mokytojo pagalba, kai jos reikia), mišraus mokymosi ir savarankiško mokymosi būdu.

Kadangi numatomi įvairūs mokymo vykdymo būdai, šiame etape mokymo metodai pateikiami kaip gairės.

4. MODULIO STRUKTŪRA

Išanalizavus VU Informacijos sistemų ir kibernetinio saugumo studijų programos, tarptautinių projektų (CyberPhish, FuseIT, dComFra) ir komercinių platformų, tokių kaip Udemy ir Coursera, modulių struktūrą, buvo sukurta tipinė modulių struktūra, kurią būtų galima taikyti tiek aukštųjų mokyklų, tiek profesinio mokymo įstaigų moduliams.

Pagrindinis tikslas – sukurti 8 modulius, kurie būtų skirti aukštųjų mokyklų studentams (EKS 5- 6 lygis), profesinio mokymo studentams ir MVĮ (EKS 4-5 lygis) ir mikromodulius visų tipų studentams.

11 pav. Modulio struktūra

* Rekomenduojama, kad po kiekvienos potemės būtų pateikiami savikontrolės (savirefleksijos) klausimai. Tačiau modulio rengimo etape, atsižvelgiant į pasirinktą studijų tipą, gali būti pasirinktas kitoks vertinimo metodas ar variantas, pavyzdžiui, studentams gali būti pateiktos praktinės užduotys, simuliacijos ir t. t., o savarankiškai besimokantiesiems siūlomi savikontrolės klausimai.

** Žinių vertinimo testas nėra privalomas. Jei besimokantysis nori gauti kurso baigimo pažymėjimą, patvirtinantį įgytas žinias, šis testas yra privalomas. Tačiau besimokantysis turi galimybę gauti kurso baigimo pažymėjimą, kad įrodytų, jog išklausė mokymus – tokiu atveju šis testas yra neprivalomas.

Siekiant užtikrinti, kad kiekvienas mokymo modulis būtų tiesiogiai susietas su praktiniu taikymu, kiekvieno modulio aprašyme bus pateikti aiškūs teorijos taikymo praktikoje pavyzdžiai. Tai apima ne tik išsamius modulių pritaikomumo scenarijus, bet ir konkrečias užduotis, kurias studentai atliks, kad įtvirtintų teorines žinias realiose kibernetinio saugumo situacijose.

Kiekviename modulyje turėtų būti ugdomi techniniai, analitiniai, rizikos valdymo ir organizaciniai įgūdžiai, skirtingomis proporcijomis. Pasibaigus bet kuriai modulio (temos) daliai, pateikiamas savikontrolės testas, skirtas besimokančiųjų žinioms patikrinti. Tai ne tik leidžia įvertinti įgytas žinias, bet ir fiksuojama besimokančiojo pažanga, dalyvis renka taškus ir ženkliukus (angl. badges), o tai leidžia dalyviui labiau įsitraukti į mokymosi procesą.

Laikantis ECTS reikalavimų, kur kiekvienas ECTS yra 25-30 valandų darbo krūvis. Pagal tai kiekvienas modulis gali būti lygus 1-5 ECTS. Darbo krūvis galėtų būti paskirstytas taip:

2 lentelė. Darbo krūvio valandos

	Modulių skaičius	**Iš viso ECTS**	**Nuotolinės valandos teoriniams įgūdžiams**	**Nuotolinės valandos praktiniams įgūdžiams**	**Individualaus darbo valandos**	**Iš viso darbo krūvio valandų**
Moduliai aukštųjų mokyklų studentams (EQF lygiai 5-6)	8	8-40	20%	20%	60%	200-1200
Moduliai profesinio mokymo įstaigų studentams (EQF lygis 4-5)	8	8-40	15%	25%	60%	200-1200
Savarankiškos studijos (mišrus mokymasis)	8	8-40	10%		90%	200-1200
Savarankiškos studijos (internetu)	8	8-40				200-1200
Mikromoduliai	1-8	1-40				25-1200

3 lentelė. Rekomenduojamas modulių darbo krūvis

Modulis	ECTS	Iš viso valandų	Kontaktinės valandos	Kontaktinės valandos (teorija)	Kontaktinės valandos (praktika)	Individualaus darbo valandos
Aukštųjų mokyklų Modulio pavadinimas	1-5	25-150	40%	20%	20%	60%
Profesinio mokymo modulio pavadinimas	1-5	25-150	40%	15%	25%	60%
Savarankiškos studijos (mišrus mokymasis)	1-5	25-150	10%			90%
Savarankiškos studijos (internetu)	1-5	25-150				100%
Mikromoduliai						10%-100%

Kiekvienas modulis turėtų turėti savo aprašymą. Išanalizavus VU, Timtal ir kitas programas, kuriose naudojami mikrokreditai, kiekvienam CyberAgent moduliui siūloma tipinė modulio struktūra (kurios pavyzdys pateikiamas 1 priede).

4 lentelė. Tipinė CyberAgent modulių struktūra

Kategorija	Detali informacija
Modulio identifikavimas (pagrindinė informacija apie modulį)	- Modulio pavadinimas - Modulio kodas - Lektorius - Institucija arba departamentas, kuriame dėstomas modulis - Kursų vedimo būdas - Kalba - Sąlygos
Modulio trukmė ir darbo krūvis	- Bendra trukmė (ECTS skaičius) - Studentų darbo krūvis valandomis

(aiškiai nurodyti laiko sąnaudas ir struktūrą)	- Kontaktinio darbo valandos - Individualaus darbo valandos
Mokymo tikslai ir mokymosi rezultatai (išsami informacija apie tai, ko moduliu siekiama ir ko besimokantieji išmoks)	- Modulio tikslas ir rezultatai - Mokymosi rezultatai o Techniniai įgūdžiai o Analitiniai įgūdžiai o Rizikos įgūdžiai o Organizaciniai įgūdžiai
Mokymo ir studijų metodai	- Mokymo ir studijų metodai
Vertinimas (paaiškinimas, kaip besimokantieji bus vertinami)	- Vertinimo metodai - Užduotys (laboratoriniai darbai, projektai, pristatymai, ataskaitos ir kt.) - Vertinimo strategija, vertinimo kriterijai
Priemonės ir ištekliai	- Įranga, programinė įranga ir technologijos
Kurso turinys	- Modulio temos ir potemės
Šaltiniai	- Šaltinių sąrašas - Papildomi šaltiniai

Laikoma, jog vienas ECTS yra 25-30 valandų (kontaktinės arba nuotolinė valandos + individualus mokymasis).

Modulio struktūra turėtų būti bent dviejų lygių:

- **Pirmasis lygis** – temos. Šiame lygmenyje pagrindiniai modulio elementai galėtų būti įvadas, įvadinis testas, baigiamasis testas ir bazinis elementas – tema.
- **Antrasis lygis** – potemės, pagrindiniai modulio mokymo(si) elementai.

Kiekvieną modulio pirmąjį lygį turėtų sudaryti:

- **ĮVADAS** į modulį (tekstinis aprašymas, vaizdo įrašo įvadas): modulio aktualumas ir nauda, baziniai modulio tikslai ir rezultatai, reikalinga programinė ir techninė įranga, reikalavimai dalyviams.
- **TEMOS** – pagrindinės kurso temos, teorinė medžiaga ir teoriniai mokymo metodai.
- **POTEMĖS** – kiekvienos temos potemės, praktinė analizė ir užduotys, analitiniai mokymo metodai. Į temas ir potemes gali būti įtraukta tekstinė informacija, vaizdo ir garso įrašai, pristatymai, nuorodos į papildomą literatūrą.

- **MODULIO įvadinis testas** (jei reikia). Vidutinio ir pažengusio lygio įvadinis testas turėtų patvirtinti, kad besimokantysis yra įgijęs pakankamai žinių ir įgūdžių ankstesniuose lygiuose.
- **MODULIO patvirtinimo testai.** Patvirtinimo testas turėtų objektyviai patikrinti besimojančiojo įgūdžius ir parodyti jo kompetenciją pagal modulio reikalavimus.
- **Gairės** mentoriams / instruktoriams. Šiame dokumente turėtų būti pateiktos metodinės rekomendacijos mentoriams / instruktoriams dėl modulio ugdymo elementų naudojimo.

Kiekvieną modulio antrąjį lygį turėtų sudaryti:

- **ĮVADAS**: temos tikslai ir rezultatai (trumpas aprašymas).
- **POTEMĖS**: visi būtini mokymo(si) elementai, padedantys besimokančiajam įsisavinti atitinkamus įgūdžius.
- **TEMOS testas:** trumpos rekomendacijos mentoriams / instruktoriams dėl modulio įgyvendinimo ir taikymo. Kiekvieną potemę turėtų sudaryti ugdymo elementai, kurių turinys atitinka modulio aprašo užduotis. Kiekvienoje potemėje galėtų (turėtų) būti pateiktas potemės testas, patvirtinantis, kad besimokantysis atitinkamus įgūdžius įsisavino pakankamai aukštu lygiu.

Modulio mokymo medžiaga turėtų apimti 6–8 temas, kurių kiekvienoje yra 4–6 potemės ir bent vienas temos testas. Taigi modulyje turėtų būti (apytiksliai) 30-40 mokomųjų elementų (metodai aprašyti skyriuje „Mokymo metodai“) ir 6-8 testai bei vienas modulio baigiamasis testas.

5. CYBERAGENT MOKYMŲ TURINYS IR UGDYMO PROGRAMA

Mokymo programos kūrimo eiga

CyberAgent mokymų turinys ir ugdymo programa sudaryta remiantis ACM, IEEE, AIS SIGSEC ir IFIP jungtinės darbo grupės parengtas Kibernetinio saugumo antrosios pakopos studijų programų gaires (2017) [8] (toliau – Gaires). Kadangi bendras CyberAgent projekto tikslas – didinti Europos MVĮ vidines kibernetinio saugumo kompetencijas, mokymo programa atitinka šiose Gairėse pateiktas organizacinio saugumo žinių sritį.

Atsižvelgiant į tai, pirmasis mokymo programos kūrimo žingsnis yra iš anksto apibrėžtų CyberAgent projekto temų ir modulių sugretinimas su Gairėse rekomenduojamomis ir aprašytomis žinių sritimis ir pagrindinėmis temomis (p. 59-70). Susiejimas pagrįstas logine šių dviejų šaltinių sąsaja, kurią aptarė ir dėl kurios susitarė projekto partneriai.

[8] The Joint Task Force on Cybersecurity Education. (2017). Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity: A Report in the Computing Curricula Series. Association for Computing Machinery, 31 December 2017. Available at: https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf [Accessed 3 March 2024]

Antrasis žingsnis – priskirti konkrečius mokymosi rezultatus, nustatytus ir aprašytus D2.2 „Mažų ir vidutinio dydžio įmonių kibernetinio saugumo pokyčių agentų mokymų poreikių nustatymo ataskaitoje“, su pirmiau susietomis žinių sritimis ir pagrindinėmis temomis. Pažymėtina, kad skirtingos kibernetinio saugumo profesijos gali turėti įvairių skirtingų žinių, įgūdžių ir kompetencijų, kaip pažymėta D2.2 dokumente. Toliau pateiktoje rekomenduojamoje mokymo programoje atsispindi numatomų CyberAgent žinių, įgūdžių ir kompetencijų rinkinys, kuris gali būti pritaikytas prie konkrečių profesijų ar besimokančiųjų grupių poreikių.

Atsižvelgiant į tai, šio tyrimo rezultatai yra pateikti toliau, 5 lentelėje.

5 lentelė. Mokymo programos kūrimo eiga

Temos ir moduliai	Žinių sritys ir pagrindinės temos	Mokymosi rezultatai Aukštosios mokyklos	Mokymosi rezultatai Profesinio rengimo institucijos
Techniniai įgūdžiai			
- **atnaujintos žinios apie kibernetinio saugumo grėsmes ir susijusius teisinius klausimus**	**Saugumo programos valdymas** - Projektų valdymas - Išteklių valdymas - Saugumo rodikliai - Kokybės užtikrinimas ir kokybės kontrolė	**Žinios:** besimokantieji įgis išsamias žinias apie pažangius kibernetinio saugumo principus, įskaitant sudėtingas kibernetines grėsmes ir atakų vektorius, nacionalinius ir tarptautinius kibernetinio saugumo teisės aktus, standartus ir atitikties reikalavimus, susijusius su jų sektoriumi. **Įgūdžiai:** besimokantieji įgis įgūdžių kurti ir įgyvendinti pažangias rizikos vertinimo ir valdymo strategijas, kad būtų sumažinta nustatyta rizika, naudojant pažangius metodus ir priemones. **Gebėjimai:** besimokantieji bus kompetentingi vadovauti kibernetinio saugumo projektams ir komandoms, įgyvendinančioms strateginę kibernetinio saugumo politiką ir sistemas, suderintas su organizacijos tikslais ir atitikties įsipareigojimais.	**Žinios**: besimokantieji įgis praktinių žinių apie naujausias kibernetinio saugumo grėsmes, įskaitant „phishing“, išpirkos reikalaujančias programas ir DDoS atakas, bei kaip jas valdyti veiksmingai valdant projektus ir išteklius bei įgyvendinant kokybės užtikrinimo ir kontrolės priemones. **Įgūdžiai**: besimokantieji įgis įgūdžių naudoti priemones ir programinę įrangą apsaugai nuo kintančių kibernetinių grėsmių ir taikyti patikimą saugumo praktiką projektų ir išteklių valdyme, kad pagerintų bendrus saugumo rodiklius ir kokybės kontrolę savo organizacijose. **Kompetencijos:** besimokantieji bus kompetentingi vertinti ir mažinti galimas saugumo grėsmes, veiksmingai informuoti apie kibernetinio saugumo problemas ir tiksliai pranešti apie grėsmes ir pažeidimus atitinkamais savo organizacijos kanalais.

- **Praktinės žinios, kaip kovoti su kibernetinio saugumo grėsmėmis**	**Sistemų administravimas** - Operacinės sistemos administravimas - Duomenų bazių sistemos administravimas - Tinklo administravimas - Debesijos administravimas - Kibernetinės fizinės sistemos administravimas - Sistemos atsparumo didinimas - Prieinamumas	**Žinios:** besimokantieji įgis išsamių žinių apie operacinių, duomenų bazių, tinklo, debesų ir kibernetinių-fizinių sistemų administravimą ir kitose srityse, kurios leis jiems veiksmingai stiprinti sistemas ir užtikrinti jų prieinamumą, kartu taikant naujausius kibernetinio saugumo gynybos mechanizmus. **Įgūdžiai:** besimokantieji įgis įgūdžių, kaip naudojant pažangius metodus ir priemones kurti ir diegti saugias sistemų architektūras, įskaitant operacines sistemas, duomenų bazes, tinklus ir debesų infrastruktūras.. **Kompetencijos:** besimokantieji gebės kurti ir įgyvendinti strategines kibernetinio saugumo sistemas sistemų administravimui, vadovauti projektams ir komandoms, siekiant sustiprinti sistemų apsaugą ir prieinamumą, taip pat priimti etiškus sprendimus, palaikant patikimą kibernetinio saugumo praktiką įvairiose administravimo srityse.	**Žinios:** besimokantieji įgis praktinių žinių, kaip administruoti ir apsaugoti operacines sistemas, duomenų bazes, tinklus, debesis ir kibernetines fizines sistemas nuo įprastų kibernetinių grėsmių, tokių kaip „phishing“, išpirkos reikalaujančios programos ir DDoS atakos, kartu įgyvendinant veiksmingą rizikos valdymo politiką. **Įgūdžiai:** besimokantieji įgis įgūdžių, kaip nustatyti galimą kibernetinio saugumo riziką ir pažeidžiamumą įvairiose sistemų platformose, naudotis specializuotomis priemonėmis ir programine įranga, kad sustiprintų sistemų atsparumą ir prieinamumą, ir įgyvendinti pagrindines kibernetinio saugumo praktikas, tokias kaip saugus slaptažodžių kūrimas, saugus naršymas ir saugus neskelbtinų duomenų tvarkymas. **Kompetencijos:** besimokantieji bus kompetentingi vertinti ir mažinti saugumo grėsmes sistemos administravimo srityje, veiksmingai informuoti apie kibernetinio saugumo problemas ir nedelsiant pranešti apie bet kokias grėsmes ir pažeidimus atitinkamais organizacijos kanalais.

Analitiniai įgūdžiai			
- **Kritinis mąstymas**	**Analitinės priemonės** - Veiklos matavimai (rodikliai) - Duomenų analizė - Saugumo žvalgyba	**Žinios:** besimokantieji įgis daugiau žinių apie nacionalinius ir tarptautinius kibernetinio saugumo teisės aktus, standartus, atitikties reikalavimus ir kitus su konkrečia pramonės šaka susijusius teisės aktus. **Įgūdžiai:** besimokantieji įgis įgūdžių naudoti veiklos matavimus, duomenų analizę ir saugumo žvalgybą, kad galėtų kurti ir įgyvendinti veiksmingas rizikos valdymo strategijas. **Kompetencijos:** besimokantieji bus kompetentingi naudotis analitinėmis priemonėmis, kad galėtų kurti strateginę kibernetinio saugumo politiką, vadovaudamiesi kritiniu mąstymu, ir priimti sprendimus dėl kibernetinio saugumo praktikos, suderintos su organizacijos tikslais ir atitikties įsipareigojimais.	**Žinios:** besimokantieji įgis praktinių žinių, kaip taikyti veiklos matavimus, duomenų analizę ir saugumo žvalgybą siekiant apsaugoti organizacijos turtą. **Įgūdžiai:** besimokantieji įgis įgūdžių naudotis analitinėmis priemonėmis, kad nustatytų galimą kibernetinio saugumo riziką ir pažeidžiamumą, taikytų duomenimis pagrįstas įžvalgas kibernetinio saugumo praktikai stiprinti ir naudotų veiklos matavimus slaptažodžių, naršymo, el. pašto ir duomenų tvarkymo saugumui vertinti ir didinti. **Gebėjimai:** besimokantieji bus kompetentingi vertinti ir mažinti galimas saugumo grėsmes naudodami analitines priemones, tiksliai pranešti apie grėsmes ir pažeidimus atitinkamais organizacijos kanalais.
- **Analizuoti ir suprasti vietines grėsmes, jų atsiradimo būdus, žmones, kuriems gresia pavojus, ir pan.**	**Saugumo operacijos** - Saugumo konvergencija - Pasauliniai saugumo operacijų centrai (GSOC)	**Žinios:** besimokantieji įgis išsamių žinių apie vietines kibernetines grėsmes, naudodamiesi pasaulinių saugumo operacijų centrų įžvalgomis ir dabartinėmis kibernetinio saugumo gynybos strategijų tendencijomis.	**Žinios:** besimokantieji įgis praktinių žinių apie vietines kibernetines grėsmes ir jų kilmę, įvertins, kaip šios grėsmės veikia organizacijos turtą. **Įgūdžiai:** besimokantieji įgis įgūdžių nustatyti vietines kibernetinio saugumo grėsmes ir pažeidžiamumus, naudotis

		Įgūdžiai: besimokantieji įgis įgūdžių, kaip naudoti pažangias pasaulinių saugumo operacijų centrų metodikas ir priemones, kad sukurtų veiksmingas rizikos valdymo strategijas ir parengtų planus, kaip veiksmingai sumažinti vietines kibernetinio saugumo grėsmes. **Gebėjimai:** besimokantieji bus kompetentingi rengti ir įgyvendinti strategines kibernetinio saugumo politikos priemones, skirtas vietinėms grėsmėms šalinti pasitelkiant pasaulinius saugumo operacijų centrus.	tokiomis priemonėmis ir programine įranga, kaip saugus slaptažodžių kūrimas, saugus naršymas ir saugus duomenų tvarkymas, pritaikyta konkrečiai aplinkai. **Gebėjimai:** besimokantieji bus kompetentingi vertinti ir mažinti vietines saugumo grėsmes, naudodamiesi pasaulinių saugumo operacijų centrų įžvalgomis, efektyviai informuoti apie kibernetinio saugumo problemas ir tiksliai pranešti apie grėsmes ir pažeidimus atitinkamais organizacijos kanalais.
Rizikos valdymas			
- **užtikrinti ir apibūdinti kibernetinio saugumo procedūras MVĮ darbo vietose**	**Rizikos valdymas** - Rizikos nustatymas - Rizikos vertinimas ir analizė - Vidinės grėsmės - Rizikos matavimo ir vertinimo modeliai ir metodikos - Rizikos kontrolė	**Žinios:** besimokantieji įgis pažangių žinių apie rizikos valdymo procesus, įskaitant rizikos identifikavimą, vertinimą ir kontrolę, kad galėtų sukurti ir aprašyti veiksmingas kibernetinio saugumo procedūras, pritaikytas konkretiems MVĮ darbo vietų poreikiams ir atitinkančias nacionalinius ir tarptautinius standartus. **Įgūdžiai:** besimokantieji įgis įgūdžių taikyti pažangias metodikas ir priemones, kad galėtų atlikti išsamų rizikos vertinimą, parengti ir įgyvendinti veiksmingas rizikos valdymo strategijas	**Žinios:** besimokantieji įgis praktinių žinių apie rizikos nustatymo, vertinimo ir kontrolės procesus bei rizikos valdymo strategijas, kad galėtų veiksmingai apsaugoti MVĮ darbo vietas. **Įgūdžiai:** besimokantieji įgis įgūdžių nustatyti ir analizuoti galimą kibernetinio saugumo riziką MVĮ aplinkoje, naudoti tinkamas priemones ir programinę įrangą grėsmėms mažinti, skatinti ir įgyvendinti pagrindines kibernetinio saugumo praktikas, įskaitant saugų slaptažodžių kūrimą, saugų naršymą ir saugų neskelbtinų duomenų tvarkymą.

		ir parengti patikimas kibernetinio saugumo procedūras, pritaikytas konkrečiai MVĮ darbo vietoms. **Kompetencijos:** besimokantieji bus kompetentingi rengti ir įgyvendinti strateginę kibernetinio saugumo politiką, skirtą MVĮ darbo vietoms.	**Kompetencijos:** besimokantieji gebės įvertinti ir sumažinti saugumo grėsmes MVĮ darbo vietose, veiksmingai informuoti apie kibernetinio saugumo problemas ir procedūras bei tiksliai pranešti apie atitinkamas grėsmes ir pažeidimus atitinkamais organizacijos kanalais.
- **Sukurti darbo vietos MVĮ kibernetinio saugumo vadovą ir kaip jo laikytis**	**Veiklos tęstinumas, veiklos atkūrimas po nelaimių, incidentų valdymas ir personalo sauga** - Reagavimas į incidentus - Atkūrimas po nelaimės - Veiklos tęstinumas - Saugumo sąmoningumas, mokymai ir švietimas - Saugumo praktikos samdant darbuotojus - Saugumo praktikos atleidžiant darbuotojus - Trečiųjų šalių saugumas - Saugumas peržiūros procesuose - Specialūs darbuotojų asmeninės informacijos privatumo klausimai	**Žinios:** besimokantieji įgis išsamių žinių apie tai, kaip sukurti ir įgyvendinti išsamų MVĮ darbo vietos kibernetinio saugumo vadovą, apimantį pažangius kibernetinio saugumo principus, naujausius gynybos mechanizmus ir nacionalinių bei tarptautinių teisės aktų ir standartų laikymąsi incidentų valdymo, veiklos tęstinumo ir personalo saugumo srityse. **Įgūdžiai:** besimokantieji įgis įgūdžių, kaip sukurti ir tvarkyti MVĮ darbo vietos kibernetinio saugumo vadovą, taikant pažangias metodikas rizikai vertinti, veiksmingoms rizikos valdymo ir reagavimo į incidentus strategijoms kurti bei išsamiems veiklos tęstinumo planams, pritaikytiems jų organizacijos poreikiams, rengti. **Kompetencijos:** besimokantieji bus kompetentingi kurti ir įgyvendinti kibernetinio saugumo vadovą MVĮ,	**Žinios:** besimokantieji įgis praktinių žinių, kaip sukurti išsamų MVĮ darbo vietos kibernetinio saugumo vadovą, į kurį būtų įtrauktos reagavimo į incidentus, veiklos atkūrimo, veiklos tęstinumo ir personalo saugumo strategijos, apsaugančios organizacijos turtą ir neskelbtinus duomenis. **Įgūdžiai:** besimokantieji įgis įgūdžių, kaip nustatyti galimą kibernetinio saugumo riziką, naudoti priemones ir programinę įrangą, kad apsisaugotų nuo grėsmių, ir taikyti geriausią kibernetinio saugumo praktiką, kad sukurtų ir tvarkytų MVĮ vadovą, kuriame būtų aptariamas saugus slaptažodžių kūrimas, naršymas, el. pašto saugumas ir duomenų apsauga. **Kompetencijos:** besimokantieji bus kompetentingi vertinti ir mažinti saugumo grėsmes, veiksmingai informuoti apie kibernetinio saugumo politiką ir praktiką bei sistemingai pranešti apie saugumo

		efektyviai vadovauti saugumo projektams ir komandoms, užtikrinti suderinamumą su organizacijos tikslais ir atitikties įsipareigojimais.	incidentus savo MVĮ, kaip nurodyta jų individualiame kibernetinio saugumo vadove.
Organizaciniai įgūdžiai			
- **Kaip įdiegti naujas kibernetinio saugumo procedūras ir darbo metodus MVĮ darbo vietose**	**Saugumo valdymas ir politika** - Organizacinis kontekstas - Privatumas - Įstatymai, etika ir atitiktis - Saugumo valdymas - Vadovų ir valdybos lygmens komunikacija - Vadovų politika	**Žinios:** besimokantieji įgis išsamių žinių apie tai, kaip MVĮ darbo vietose įgyvendinti naujas kibernetinio saugumo procedūras ir darbo eigą, atsižvelgiant į dabartinius kibernetinio saugumo principus, tendencijas ir atitiktį nacionaliniams bei tarptautiniams teisės aktams, susijusiems su jų pramone. **Įgūdžiai:** besimokantieji įgis įgūdžių taikyti pažangias metodikas, kad galėtų atlikti rizikos vertinimą, kurti ir įgyvendinti naujas kibernetinio saugumo procedūras ir rengti reagavimo strategijas, užtikrindami veiksmingą valdymą ir atitiktį MVĮ darbo vietose. **Kompetencijos:** besimokantieji bus kompetentingi kurti ir įgyvendinti strateginę kibernetinio saugumo politiką, vadovauti iniciatyvoms, kuriomis siekiama sukurti naujas procedūras ir darbo eigą MVĮ darbo	**Žinios:** besimokantieji įgis praktinių žinių, kaip integruoti naujas kibernetinio saugumo procedūras ir praktiką MVĮ darbo vietose, laikantis kibernetinio saugumo teisės aktų, standartų, strategijų ir politikos, susijusios su informacijos saugumu, rizikos valdymu ir duomenų apsauga. **Įgūdžiai:** besimokantieji įgis įgūdžių taikyti kibernetinio saugumo priemones ir programinę įrangą, kad galėtų įgyvendinti naujas saugumo procedūras, nustatyti ir mažinti riziką bei skatinti pagrindines kibernetinio saugumo praktikas, tokias kaip saugus slaptažodžių kūrimas, naršymas ir duomenų tvarkymas MVĮ darbo vietų valdymo sistemoje. **Kompetencijos:** besimokantieji bus kompetentingi vertinti ir mažinti galimas saugumo grėsmes, veiksmingai informuoti apie kibernetinio saugumo pokyčius ir politiką bei tiksliai pranešti apie saugumo incidentus MVĮ pagal valdymo ir atitikties reikalavimus.

		vietose, ir priimti etinius sprendimus, atitinkančius organizacijos tikslus ir atitikties reikalavimus.	
- **Vadovų palaikymo užtikrinimas kibernetinio saugumo srityje**	**Kibernetinio saugumo planavimas** - Strateginis planavimas - Operatyvinis ir taktinis valdymas	**Žinios:** besimokantieji įgis išsamių žinių, kaip integruoti pažangius kibernetinio saugumo principus ir dabartines tendencijas į strateginį planavimą ir veiklos valdymą. **Įgūdžiai:** besimokantieji įgis strateginio planavimo ir operatyvinio valdymo įgūdžių, leidžiančių veiksmingai kurti ir įgyvendinti kibernetinio saugumo strategijas, kuriomis sprendžiami nauji pavojai ir užtikrinamas patikimas taktinis atsakas. **Kompetencijos:** besimokantieji bus kompetentingi kurti ir įgyvendinti strategines kibernetinio saugumo sistemas, vadovauti kibernetinio saugumo iniciatyvoms ir jas valdyti.	**Žinios:** besimokantieji įgis praktinių žinių, kaip integruoti kibernetinio saugumo strateginį planavimą ir operatyvinį valdymą, siekiant apsaugoti organizacijos turtą, laikytis atitinkamų teisės aktų ir standartų, įgyvendinti veiksmingas informacijos saugumo strategijas ir rizikos valdymo politiką. **Įgūdžiai:** besimokantieji įgis įgūdžių, kaip nustatyti kibernetinio saugumo riziką, naudoti strateginio planavimo ir operatyvinio valdymo priemones, kad apsisaugotų nuo grėsmių, ir skatinti pagrindinių kibernetinio saugumo praktikų įgyvendinimą savo, kaip vadovų, palaikymo vaidmenį. **Kompetencijos:** besimokantieji bus kompetentingi vertinti ir mažinti saugumo grėsmes, veiksmingai informuoti apie kibernetinio saugumo strategijas ir problemas bei patikimai pranešti apie incidentus ir pažeidžiamumą atitinkamais kanalais savo organizacijose.

6. KURSO VERTINIMO STRATEGIJA

Žinių vertinimas yra neatsiejama mokymosi proceso dalis ir skatina geriau įsisavinti žinias. Šiame skyriuje aprašomas kurso vertinimo metodas, kuris reikalingas siekiant užtikrinti, kad visi CyberAgent kursų dalyviai pasiektų reikiamus mokymosi rezultatus ir kompetencijas. Kursų vertinimo procesas suskirstytas į dvi pagrindines dalis: savęs vertinimą ir žinių vertinimo testus, kurie pritaikyti tiek aukštojo mokslo (AMI), tiek profesinio mokymo (PMI) studentams, atsižvelgiant į skirtingus jų poreikius ir mokymosi tikslus.

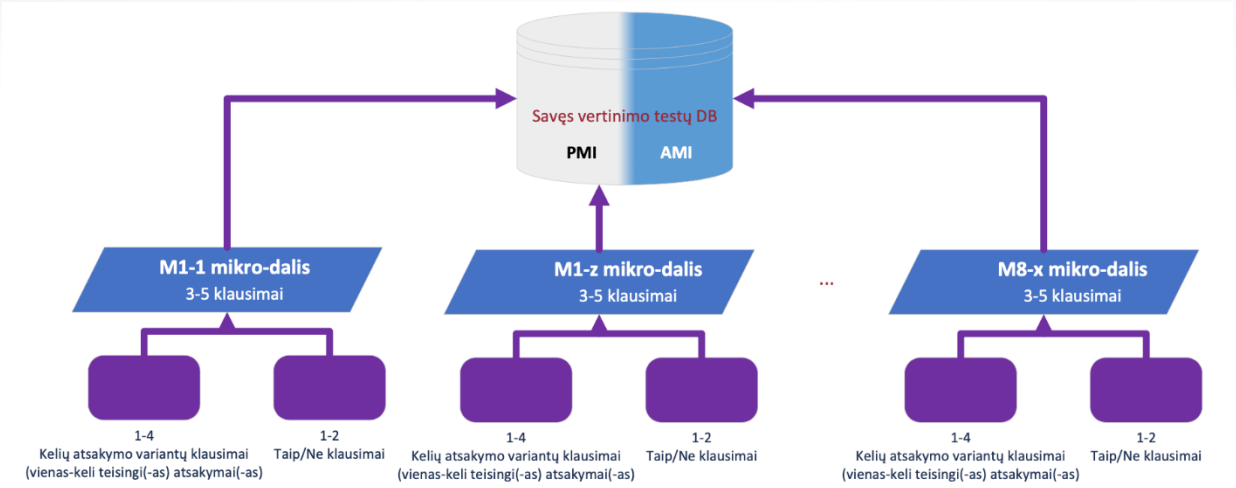
Kadangi modulių temos gali būti tos pačios ir aukštosiose mokyklose, ir profesinio mokymo įstaigose, kai kurie klausimai gali būti tinkami ir aukštosioms mokykloms, ir profesinio mokymo įstaigoms. Taigi rengiant klausimus bus galima nurodyti, ar klausimas skirtas tik profesinio rengimo ar tik aukštojo mokslo įstaigoms, ar abiem. Šis žymėjimo būdas bus naudojamas tik rengiant klausimus, nes tai palengvins jų rengimą. Kai klausimai bus importuoti į platformą, duomenų bazės bus skirtingos profesinio mokymo ir aukštojo mokslo įstaigoms.

12 pav. Savęs vertinimo ir žinių vertinimo duomenų bazės

1. Savęs vertinimo testai: baigę kiekvieną kurso temą, besimokantieji atliks savęs vertinimo testus. Šie testai skirti suteikti tiesioginį grįžtamąjį ryšį ir padėti dalyviams įsivertinti, kaip jie supranta ką tik išnagrinėtą medžiagą. Šis etapas skatina savirefleksiją ir padeda įtvirtinti kiekvienos temos mokymosi tikslus. Be to, jis leidžia besimokantiesiems išsiaiškinti sritis, kuriose jiems gali prireikti tolesnio mokymosi ar paaiškinimų, ir skatinama aktyviai siekti mokymosi tikslų.

Naudodami savęs vertinimo testus kursų dalyviai galės nustatyti pradinį žinių lygį ir pasitikrinti pažangą po kiekvienos mokymo temos.

Rekomenduojama parengti 3-5 klausimų savęs vertinimo testą, kuriame būtų derinami taip/ ne (angl. true/false), sutapimo (angl. match) ir (arba) kelių atsakymų variantų klausimai. Kita kurso tema turėtų būti atrakinama tik teisingai atsakius į visus klausimus. Neturėtų būti jokių laiko ribojimų ar bandymų skaičiaus apribojimų. Bandymų metu klausimai turėtų būti atsitiktinai parenkami iš duomenų bazės.



13 pav. Savęs vertinimo duomenų bazės struktūra

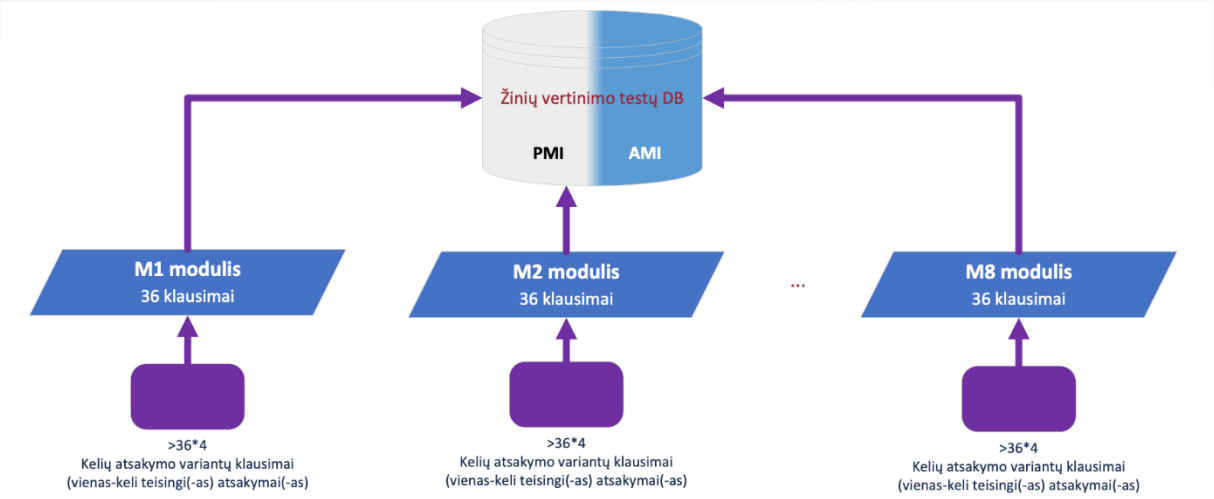
2. Žinių vertinimo testas*: baigę visas vieno kurso temas, dalyviai galės atlikti baigiamąjį testą, kad gautų kurso baigimo pažymėjimą. Šiuo išsamiu vertinimu tikrinamas bendras jų kurso turinio supratimas ir įsisavinimas. Baigiamuoju testu įvertinama, kaip besimokantieji įsimena medžiagą, ir nustatoma, kaip gerai jie gali pritaikyti žinias platesniame kontekste.

* Rengiant mokymo programą ir medžiagą, bus apsvarstytos kitos kursų baigimo ir žinių vertinimo metodikos, pavyzdžiui, atvejų analizė, praktinės užduotys ir refleksijos ataskaitos, kurios leis išsamiau įvertinti dalyvių analitinio ir kritinio mąstymo įgūdžius. Šį metodą taip pat galės taikyti aukštųjų mokyklų ir profesinio mokymo įstaigų dėstytojai, dėstantys kursus.

Naudodami žinių vertinimo testą kursų dalyviai galės nustatyti savo galutinį žinių lygį, o jei jį išlaikys – gauti kursų baigimo ženklelį (sertifikatą).

Rekomenduojama parengti 36 klausimų žinių įvertinimo testą, kuriame būtų derinami teisingi ir klaidingi, atitikmenų ir kelių atsakymų variantų klausimai. Turėtų būti nustatytas 45 minučių laiko ribojimas ir leidžiamas tik vienas bandymas. Testas turėtų būti atliekamas atsitiktine tvarka parenkant klausimus iš duomenų bazės.

Be to, atliekant vertinimą reikėtų atsižvelgti ir į sukčiavimo prevenciją, todėl rekomenduojama parengti maždaug keturis klausimų rinkinius. Kai kurie profesinio mokymo ir aukštojo mokslo žinių patikrinimo klausimai gali sutapti, todėl kūrimo metu turėsime tris atributus: PMĮ, AMĮ arba PMĮ ir AMĮ.



14 pav. Žinių vertinimo duomenų bazės struktūra

Ši dviejų etapų vertinimo strategija ne tik padeda veiksmingai mokytis, suteikdama kelis grįžtamojo ryšio ciklus, bet ir įgalina besimokančiuosius aktyviai dalyvauti mokymo procese.

Savęs vertinimo testai ir žinių vertinimo testai bus rengiami pagal kursų programą ir remiantis šio projekto rezultatais bei rekomendacijomis.

KLAUSIMŲ DUOMENŲ BAZĖS SUDĖTIS

Siekiant užtikrinti pakankamai didelę ir subalansuotą klausimų bazę, kiekvienai PMĮ arba AMĮ kurso temai bus sukurti ne mažiau kaip 5 teisingi ir klaidingi klausimai ir 5 klausimai su keliais atsakymų variantais.

Darant prielaidą, kad kiekviename kurse bus ne mažiau kaip 10 temų, kiekviename PMĮ arba AMĮ kurse turėtų būti ne mažiau kaip 10-20 proc. teisingų ir klaidingų klausimų, 90-80 proc. klausimų su keliais atsakymų variantais. Tai yra bendros rekomendacijos, tačiau kuratorius / instruktorius galės pasirinkti klausimų struktūrą pagal kurso temą.

Atsižvelgiant į PMĮ / AMĮ mokymosi tikslų ir rezultatų skirtumus, bendra vieno kurso klausimų duomenų bazės sudėtis turėtų būti tokia, kaip parodyta toliau pateiktoje lentelėje.

6 lentelė. Klausimų tipai

	Teisingas / klaidingas arba atitikties klausimai	**Klausimai su keliais atsakymų variantais**
Bendroji kurso dalis	20%	80%
PMĮ kurso dalis	20%	80%
AMĮ kurso dalis	20%	80%
Iš viso PMĮ ir AMĮ kursams:	20%	80%

KLAUSIMŲ SUDARYMO GAIRĖS

Savęs vertinimo ir žinių vertinimo testų klausimai turi būti parengti anglų kalba, o vėliau lokalizuoti į partnerių kalbas.

Kuriant tiek savęs vertinimo, tiek žinių patikrinimo testo klausimus, būtina užtikrinti, kad klausimai būtų aiškūs, glausti ir suprantami visiems besimokantiesiems, nepriklausomai nuo jų patirties. Toks požiūris užtikrina, kad vertinimai tiksliai atspindėtų besimokančiųjų kurso turinio supratimą ir jų gebėjimą pasiekti nurodytus įgūdžius ir tikslus, išdėstytus kurso programose.

Bendrosios klausimų sudarymo gairės:

Kuriant testo klausimus bus taikomos aiškios gairės: klausimai turi būti suprantami ir tiesiogiai susiję su kurso mokymosi tikslais, nenaudojant sudėtingų terminų ar painių formuluočių. Taip pat bus vengiama kultūriniu požiūriu specifinių ar painių klausimų, kad būtų užtikrintas teisingumas ir prieinamumas visiems kursų dalyviams. Toliau pateikiamos tolesnės rekomendacijos dėl klausimų struktūros.

Aiškumas ir paprastumas: klausimai turi būti paprasti, juose neturi būti vartojama sudėtinga kalba ar žargonas, kurie galėtų supainioti ar suklaidinti kandidatus. Tikslas – įvertinti kandidatų žinias ir dalyko supratimą, o ne jų gebėjimą iššifruoti sudėtingus klausimus.

Tiesioginis ryšys ir aktualumas: kiekvienas klausimas turėtų būti tiesiogiai susijęs su pagrindiniais įgūdžiais ir kurso programos tikslais. Reikėtų vengti nesusijusio ar šalutinio turinio, kad būtų išlaikytas dėmesys numatytiems mokymosi rezultatams vertinti.

Kultūrinis jautrumas ir atsižvelgimas į skirtingą patirtį: užtikrinti, kad klausimai nereikalautų specifinių kultūrinių žinių ar patirties, būtų prieinami ir sąžiningi įvairių sluoksnių kandidatams.

Jokių apgaulingų klausimų: kiekvieno klausimo tikslas turi būti aiškus, kandidatų neturi būti bandoma suklaidinti ar apgauti. Klausimais, kuriais siekiama kandidatus suklaidinti arba patikrinti jų gebėjimą įžvelgti triukus, nėra veiksmingas jų dalyko supratimo vertinimas.

Vienareikšmiškas ir glaustas pateikimas: klausimai turėtų būti suformuluoti taip, kad neliktų vietos interpretacijoms, užtikrinant, kad visi besimokantieji klausimą suprastų vienodai. Klausimai turi būti glausti, vengiant nereikalingo išplėtimo, kuris galėtų užgožti pagrindinę mintį.

Teigiamos formuluotės: venkite neigiamų formuluočių klausimuose (pvz., „Kuris iš toliau išvardytų dalykų NĖRA...“). Neigiamos frazės gali sukelti painiavą ir klaidingą interpretaciją, ypač egzamino sąlygomis. Vietoj to visus klausimus formuluokite vengdami neiginių, kad būtų aišku, ko klausiama, ir išvengtumėte galimų nesusipratimų.

Konkrečios klausimų sudarymo gairės:

Klausimai su keliais atsakymų variantais: įsitikinkite, kad visi variantai yra realūs ir susiję su klausimu. Teisingas atsakymas turėtų būti neginčijamai teisingas, o neteisingi atsakymai turėtų būti aiškiai neteisingi žmogui, kuris supranta medžiagą.

Teisingi / klaidingi (taip / ne) klausimai: pateikite aiškius, faktais pagrįstus teiginius, tiesiogiai susijusius su kurso turiniu, kad nekiltų dviprasmybių dėl jų teisingumo.

Sąvokų atitikimo klausimai: įsitikinkite, kad abu sąrašai (pvz., terminai vienoje pusėje ir apibrėžimai kitoje) yra aiškiai susiję ir, kad kiekvienas atitikimas yra aiškiai pagrįstas. Venkite nevienodų sąrašų, kuriuose nesutampa elementų skaičius, nebent aiškiai nurodyta, kad kai kurie elementai nebus naudojami arba gali būti naudojami kelis kartus.

Pilotinių mokymų metu bus analizuojama informacija apie žinių vertinimo metodikas ir vertinimo procesą, renkant grįžtamąjį ryšį iš besimokančiųjų ir dėstytojų / instruktorių / kuratorių. Tai leis įvertinti žinių vertinimo metodų tinkamumą ir prireikus papildyti ar patobulinti vertinimo metodą.

ŽAIDYBINIMO ELEMENTŲ NAUDOJIMAS

Šiame skyriuje aprašomi CyberAgent kursuose planuojami įdiegti žaidybinimo elementai. Žaidybinimas – tai procesas, kai į tradicinę mokymosi veiklą įtraukiami žaidybinimo principai, siekiant padidinti dalyvių motyvaciją ir įsitraukimą. Šie elementai buvo pasirinkti remiantis naujausiais švietimo technologijų tyrimais, kurie rodo, kad žaidybinimas gali gerokai pagerinti mokymosi rezultatus, padidinti besimokančiųjų motyvaciją mokytis ir jų įsitraukimą į mokymosi procesą.

Kursuose bus integruoti tokie žaidybinimo elementai kaip ženkliukai (angl. badges), taškai, rangavimai ir spalvoti slapyvardžiai, atspindintys dalyvio patirtį ir pasiekimus.

- Ženkliukai (angl. badges) bus skiriami už:

- **Modulio užbaigimą.**
- **Už išlaikytą testą pagal išlaikymo procentą.** Pavyzdžiui, dalyviui bus skiriamas bronzinis ženklelis už minimalų išlaikymo balą baigiamajame teste, sidabrinis – už minimalų išlaikymo balą 75 %, auksinis – už išlaikymo balą 76–90 % ir platininis – už išlaikymo balą 90–100 %. Tokiu atveju vienas dalyvis gali turėti 8 šio tipo ženkliukus.
- **Temos baigimą.**
- **Prisijungimą prie sistemos kiekvieną dieną dešimt dienų iš eilės.**
- **Specialų veiklos ženkliuką** kiekvienai temai taip pat galės suteikti kurso mentorius / dėstytojas.

- **Taškai ir balai** apskaičiuojami remiantis savęs vertinimo testo rezultatais + galutiniais testo rezultatais su daugikliu.

CyberAgent kurso dalyviai negalės matyti savo pažangos individualiai, tačiau galės varžytis su kitais dalyviais grupėse arba komandose (pagal didžiausią surinktų taškų skaičių, taip pat pagal daugiausiai ženkliukų). Taip skatinama ne tik individuali, bet ir komandinė konkurencija ir bendradarbiavimas, o tai svarbu ugdant bendradarbiavimo įgūdžius.

Kiekvienas dalyvis, prisijungęs prie kurso, matys savo slapyvardį, kuris bus žymimas spalvomis pagal kurso eigą ir sukauptą patirtį (baigtus/užfiksuotus kursus).

Tai padės kursų dalyviams geriau įsitraukti į mokymo procesą. Kurso dalyviai gali kelis kartus pakartoti tą patį testą ir taip pagerinti savo rezultatą (taškai skiriami už didžiausią teisingai atliktų savęs vertinimo testų skaičių).

Specialus algoritmas apskaičiuoja kiekvieno dalyvio rezultatą, atsižvelgdamas į atsakymo laiką, testo pakartojimų skaičių ir kitus parametrus, taip sumažindamas sukčiavimo galimybę.

Visos žaidybinimo taisyklės bus aiškiai aprašytos ir pateiktos dalyviams, kad visi lengvai suprastų, kaip galima pasiekti skirtingus žaidybinimo lygius ir kaip jie apskaičiuojami.

7. CYBERAGENT MOKYMOSI/MOKYMO PROCESAS

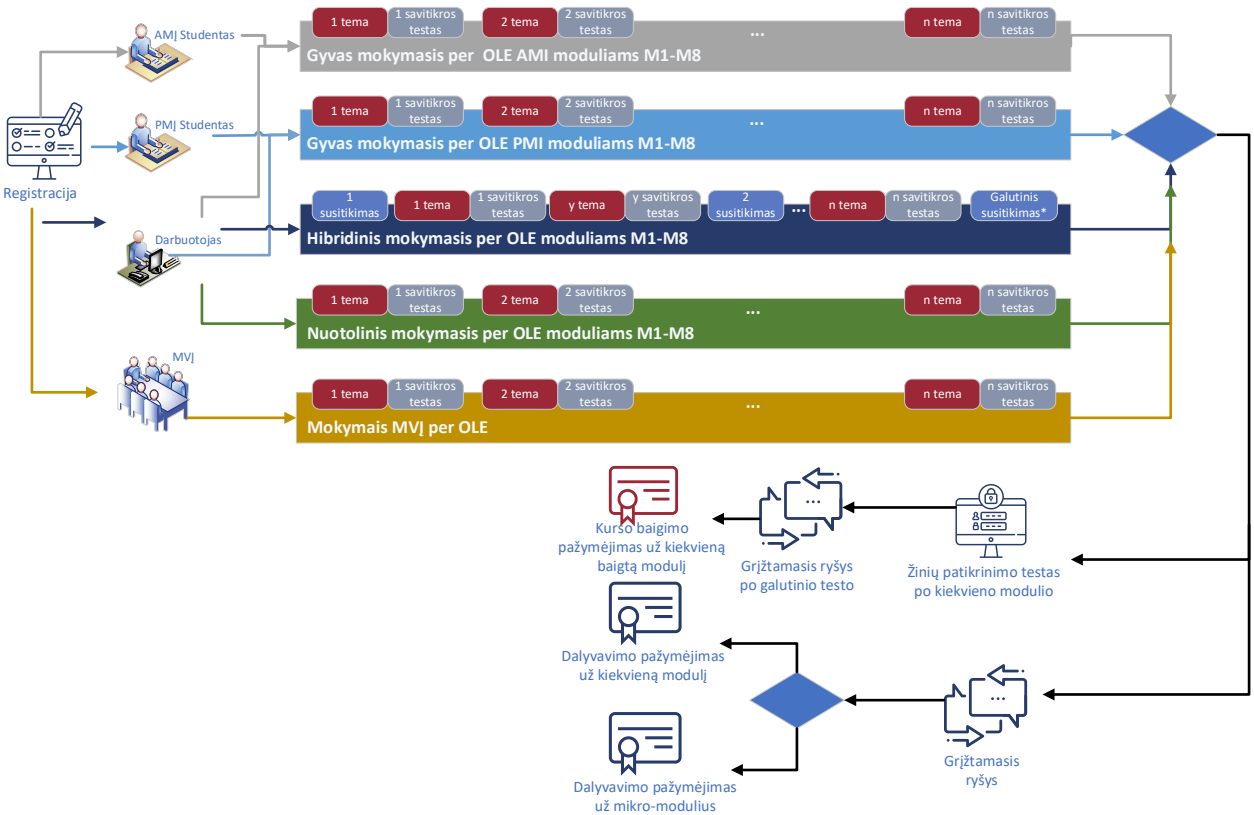
Šiame skyriuje apibendrinama visų šio dokumento skyrių informacija ir išsamiai aprašomas mokymosi ir (arba) mokymo procesas, kuris prasideda nuo registracijos į CyberAgent kursą mokymosi platformoje ir baigiasi kurso baigimu arba pažymėjimo išdavimu.

Cyberagent kursai yra skirti įvairiems besimokantiesiems, įskaitant aukštųjų mokyklų studentus, profesinio mokymo įstaigų studentus, taip pat MVĮ darbuotojus. Siekiame, kad kiekvienas dalyvis turėtų galimybę pasirinkti jam tinkamiausią mokymosi būdą, atsižvelgiant į asmenines aplinkybes ir mokymo įstaigos organizacinę politiką.

Nepaisant pasirinkto mokymosi metodo, dalyviai registruojasi CyberAgent platformoje ir mokymų metu naudojasi šia platforma.

Registracija

Potencialūs dalyviai, norintys dalyvauti CyberAgent kursuose, turi užpildyti registracijos formą ir pasirinkti norimus modulius bei pageidaujamą mokymosi būdą. Pateikiama koncepcinė schema, kuri padės dalyviams mokytis nuo pirmojo iki aštuntojo CyberAgent modulio.



15 pav. CyberAgent mokymosi / mokymo kelias

Registracijos proceso metu bus užtikrintas dalyvių informacijos konfidencialumas, atsižvelgiant į BDAR reikalavimus. Registracijos metu dalyviai turės galimybę susipažinti su mokymo platformos taisyklėmis, privatumo ir duomenų apsaugos taisyklėmis.

Dalyvių registracijos duomenys yra prieinami tik paskirtiems partnerio organizacijos asmenims, laikantis organizacijos vidaus politikos. Pilotinių mokymų metu projekto partnerių dalyvių duomenys gali būti prieinami CyberAgent koordinatoriui, kiti partneriai neturi teisės matyti vieni kitų dalyvių duomenų. Pasibaigus projektui, koordinatorius gali naudotis tik nuasmenintais kitų partnerių duomenimis, skirtais projekto rezultatams stebėti, kaip nurodyta projekto paraiškoje, iki 5 metų po projekto pabaigos.

CyberAgent siūlo specialiai pritaikytas mokymo galimybes, atitinkančias įvairių mūsų tikslinių grupių poreikius. Aukštųjų mokyklų ir profesinio rengimo ir mokymo įstaigų studentai gali dalyvauti mokymuose per universitetų kontaktines sesijas (mokymus). MVĮ darbuotojai gali pasirinkti jų poreikius geriausiai atitinkantį mokymosi būdą: mišrųjį mokymąsi, mokymąsi tik internetu arba, prisijungti prie aukštosios mokyklos ar profesinio mokymo įstaigų paskaitų.

Mokymai taip pat gali būti siūlomi didesnėms įmonėms, kuriose dirba daug darbuotojų. Tokiais atvejais mokymo metodas bus pritaikytas konkretiems poreikiams, tačiau mokymų metu naudojami CyberAgent kursų moduliai.

Užsiregistravę platformoje, dalyviai pasirenka mokymosi metodą ir pradeda mokytis. Baigę modulį ar jo dalį, jie gali gauti dalyvio pažymėjimą arba kurso baigimo pažymėjimą, kuris išduodamas, jei dalyvis išlaiko modulio testą ne mažiau kaip 75 % balų.

Galiausiai, prieš gaudami sertifikatą, dalyviai turi užpildyti atsiliepimų (grįžtamojo ryšio) formą. Šis grįžtamasis ryšys yra labai svarbus nuolatiniam mūsų mokymo pasiūlymų tobulinimui ir dalyvių pasitenkinimo užtikrinimui.

Mokymosi/apmokymo būdai

Darbuotojai gali naudotis keliomis galimybėmis susipažinti su kurso turiniu:

- Jei AMĮ ar PMĮ įstaigos leidžia darbuotojams dalyvauti paskaitose kaip kviestiniams dalyviams, darbuotojas gali dalyvauti paskaitose kartu su studentais. Tokie kviestinių dalyvių užsiėmimai gali būti organizuojami 1-2 kartus per metus pagal paskelbtą paskaitų tvarkaraštį.
- Darbuotojai gali rinktis mišrų mokymo metodą, kai mokymai vyksta konkrečiomis datomis, o jų rekomenduojama trukmė - 2-4 mėnesiai. Rekomenduojama sudaryti ne mažesnes kaip 10 dalyvių grupes, o vienoje grupėje gali būti ne daugiau kaip 30 dalyvių. Mišrūs mokymai apima tiesiogines ir internetines konsultacijas kurso pradžioje, jo metu ir pabaigoje, kad būtų lengviau gauti tiesioginį grįžtamąjį ryšį ir pasirengti galutiniam žinių patikrinimui.
- Darbuotojai gali pasirinkti mokymosi internetu būdą, kuris leidžia mokytis savo tempu, nenustatant kurso baigimo trukmės.
- Daugiau informacijos apie CyberAgent modulius pateikiama **1 skyriuje „Studijų kelias“.**

Studentų įsitraukimas

Į kibernetinio saugumo studijų programą įstoję studentai, priklausomai nuo jų akademinės įstaigos nuostatų, gali pasirinkti skirtingus kelius. Jiems gali būti privaloma baigti kai kuriuos arba visus CyberAgent modulius arba, priklausomai nuo vidaus universiteto politikos, studentai,

atitinkantys kriterijus, gali pasirinkti studijuoti vieną arba kelis CyberAgent modulius. AMĮ arba PMĮ studentai paprastai dalyvauja moduliuose per tradicines auditorines paskaitas, kurias teikia jų įstaiga, arba gali pasirinkti savarankiško mokymosi metodus, kad pasiruoštų baigiamajam žinių patikrinimo testui.

MVĮ įsitraukimas

Organizacijose, kuriose kibernetinio saugumo mokymai laikomi būtinais, įmonės atstovas gali registruoti organizaciją į vidaus mokymus. Tokiais atvejais, atskirai susitarus su mokymo įstaiga ir (arba) instruktoriais, mokymų metodas, tvarkaraštis ir pažymėjimų išdavimas gali būti pritaikytas konkretiems organizacijos poreikiams pagal esamus modulius.

Grįžtamojo ryšio rinkimas

Baigę modulį dalyviai turi užpildyti anoniminę atsiliepimų formą, kurią galima rasti mokymų portale. Grįžtamasis ryšys daugiausia bus renkamas iš kursų dalyvių, tačiau taip pat bus renkamas ir iš mentorių / instruktorių. Renkant grįžtamąjį ryšį bus vertinamas organizacijos dalyvių patenkinimo lygis, kursų organizavimo aspektai, mokymosi procesas, įgytų kompetencijų panaudojimas praktikoje, kursų turinys, vertinimo strategijos, žaidybinimo elementų įtraukimas, tobulintinos sritys ir kt.

Grįžtamojo ryšio rezultatai bus reguliariai peržiūrimi ir pateikiami projekto valdymo komandai, kad būtų galima greitai reaguoti ir tobulinti mokymo strategijas atsižvelgiant į realius poreikius ir rinkos pokyčius.

Tik užpildę šią formą, dalyviai gali gauti dalyvavimą patvirtinantį pažymėjimą arba kursų baigimo pažymėjimą ar sertifikatą.

Kursų baigimo sertifikatas

Sėkmingai išlaikius patikrinimo testą, dalyviui išduodamas kursų baigimo sertifikatas. Kiekviename modulyje yra vienas baigiamasis testas.

Dalyvavimo sertifikatas

Dalyviai, kurie nusprendžia nelaikyti žinių patikrinimo testo, gali gauti dalyvio sertifikatą. Šis sertifikatas gali būti išduodamas baigus vieną modulį arba kelias kurso mikrosekcijų dalis.

IŠVADOS IR APIBENDRINIMAS

Šioje ataskaitoje parengti struktūruoti MVĮ kibernetinio saugumo pokyčių agentų mokymosi keliai, pritaikyti prie konkrečių įvairių švietimo ir profesinių lygių – nuo aukštojo mokslo iki profesinio rengimo ir tiesioginių MVĮ darbuotojų mokymų – poreikių. Sukurtoje mokymo programoje, kurią sudaro aštuoni išsamūs moduliai, integruoti techniniai, analitiniai, organizaciniai ir rizikos valdymo įgūdžiai, kurie yra labai svarbūs siekiant veiksmingai įgalinti būsimus kibernetinio saugumo specialistus.

Struktūrizuotas požiūris į mokymosi būdus užtikrina visapusišką MVĮ darbuotojų mokymosi kelią. Tai padeda įsisavinti žinias ir jas pritaikyti praktiškai, nes yra numatyti keli etapai: pasirengimo mokytis, mokymosi ir etapas pabaigus studijas. Mikromoduliai užtikrina lankstumą ir galimybę prisitaikyti prie individualių poreikių, sustiprina mokymąsi mikrokreditais, suteikiančiais pripažintą kompetenciją. Šis suderinimas su pramonės standartais labai prisideda prie MVĮ kibernetinio saugumo gebėjimų stiprinimo, ruošiant darbuotojus dabartiniams iššūkiams ir ateities pažangai. Toliau pateikiamoje karjeros kelių analizėje aprašyta kibernetinio saugumo pareigybės, kaip apibrėžta ESCO sistemoje, palengvinant tikslingą mokymosi metodą, kuris parengia asmenis veiksmingai integruotis į kibernetinio saugumo darbo rinką, galiausiai padidinant jų karjeros perspektyvas ir profesinį tobulėjimą.

Išnagrinėta pedagoginių metodų įvairovė kibernetinio saugumo mokymo programoje turėtų sudaryti sąlygas dinamiškai ir lanksčiai mokymosi aplinkai, kuri atitiktų skirtingus mokymosi stilius ir poreikius. Įvairių mokymo metodų, įskaitant teorines paskaitas, praktines laboratorines pratybas, žaidybinimą ir bendrus projektus, įtraukimas užtikrina, kad studentai būtų ne tik žinių gavėjai, bet ir aktyvūs mokymosi proceso dalyviai. Ši visapusiška strategija turėtų padidinti studentų įsitraukimą, supratimą ir geriau juos paruošti realiems kibernetinio saugumo iššūkiams. Mokymo metodų pritaikomumas prie konkretaus modulio reikalavimų turėtų dar labiau suasmeninti mokymosi patirtį, užtikrinant, kad kiekvieno dalyvio mokymosi rezultatai būtų kuo geresni.

Sistemingai priskiriant projekto CyberAgent temas ir modulius tarptautiniu mastu pripažintiems žinių moduliams, mokymo programa ne tik atitinka, bet ir numato dinamiškus kibernetinio saugumo srities reikalavimus. Toks metodinis požiūris užtikrina, kad kiekvienas mokymosi rezultatas būtų strategiškai susietas su realiomis kompetencijomis, kurios yra labai svarbios siekiant veiksmingai valdyti kibernetinio saugumo grėsmes. Mokymo programos pritaikomumas leidžia ją pritaikyti įvairioms profesinėms užduotims šioje srityje, ruošiant besimokančiuosius ne tik neatidėliotiniems iššūkiams, bet ir ilgalaikei karjerai kibernetinio saugumo srityje.

Pateikta kurso vertinimo strategija yra kibernetinio saugumo programų studentų gebėjimų ir pažangos vertinimo sistema. Dviejų etapų metodas, apimantis savęs vertinimo testus ir išsamius žinių vertinimo testus, leidžia studentams aktyviai įsitraukti nagrinėjant medžiagą, nuolat vertinti savo supratimą ir atitinkamai koreguoti mokymosi strategijas. Sukūrus vertinimą taip, kad jis būtų pritaikytas tiek AMĮ, tiek PMĮ įstaigų studentams, naudojant specialiai jiems pritaikytus klausimus, strategija užtikrina aktualumą ir tinkamumą kiekvienam išsilavinimo lygiui, taip pagerinant

mokymosi patirtį. Taikant šį metodą galima aiškiai įvertinti dalyvių žinių įsisavinimą ir pasirengimą jas taikyti praktiškai. Be to, įdiegus žaidybinimo elementus, pavyzdžiui, ženkliukus ir vertinimo sistemas, ne tik motyvuojami studentai, bet ir skatinama konkurencinga, bet kartu kuriama bendradarbiavimu grįsta mokymosi aplinka.

Galiausiai, CyberAgent mokymosi ir mokymo proceso metu sukuriama išsami ir pritaikoma mokymo sistema, tinkama įvairiems besimokantiesiems iš AMĮ, PMĮ ir MVĮ. Ši sistema leidžia taikyti įvairius dalyvavimo metodus, įskaitant kontaktinį (tiesioginį), mišrųjį ir nuotolinį mokymąsi, taip užtikrinant, kad kibernetinio saugumo mokymas būtų lankstus ir prieinamas. Užsiregistravus CyberAgent platformoje pradedamas mokymosi procesas, kurio metu dalyviai pasirenka pageidaujamus modulius ir mokymosi metodus, o sėkmingai baigus mokymąsi ir atlikus įvertinimą išduodami pažymėjimai. Tokia struktūra ne tik palaiko individualizuotas mokymosi trajektorijas, bet ir atitinka griežtus privatumo standartus, būtinus dalyvių konfidencialumui užtikrinti visame mokymo procese.

Šiame dokumente pateiktos rekomendacijos ir gairės bus naudojamos kitame etape rengiant išsamias CyberAgent mokymo programas, mokymo medžiagą, žinių testus ir vertinimus, praktines užduotis ir kitą mokymo turinį, kuris bus integruotas į CyberAgent mokymo platformą.

PRIEDAS 1. MODULIO APRAŠYMAS

MODULIO APRAŠYMAS

Modulio pavadinimas	Modulio kodas
...	

Dėstytojas (-ai)	Institucija arba departamentas, kuriame teikiamas modulis
...	...

Pateikimo būdas	Kalba
Kontaktiniu būdu, internetu, mišrus, konsultacijos	*Anglų, ...*

Būtinosios sąlygos
...

Suteiktų ECTS kreditų skaičius	Studento darbo krūvis	Kontaktinės darbo valandos	Individualios darbo valandos
5	...	...	...

Modulio tikslas ir rezultatai		
...		
Modulio mokymosi rezultatai	**Mokymo ir mokymosi metodai**	**Vertinimo metodai**
Techniniai įgūdžiai		
Analitiniai įgūdžiai		
Rizikos valdymo įgūdžiai		
Organizaciniai įgūdžiai		

Reikalingos priemonės (įranga, programinė/techninė įranga)
...

Modulio turinys: temų skirstymas	Kontaktinės darbo valandos					Individualios darbo valandos ir užduotys	
	Paskaitos (AMĮ/ PMĮ)	Konsultacijos (MVĮ)	Praktika (AMĮ/ PMĮ)	Testai	**Visi kontaktiniai darbai**	**Individualus darbas**	Užduotys
1							
...							
n							
Viso							

Vertinimo strategija	Lyginamasis svoris procentais	Vertinimo kriterijai
Savarankiškas testas 1		...
...		...
Savarankiškas testas n		...
Žinių vertinimo testas		...
AMĮ/PMĮ sertifikavimas -> Savarankiškas testas I + ...+ Savarankiškas testas n + Žinių vertinimo testas		
SVĮ ir (arba) Savarankiškų studijų pažymėjimas -> Savarankiškas testas I + ...+ Savarankiškas testas I + Žinių vertinimo testas		
Mikromoduliai, mikrosekcijos -> Savarankiškas testas I (neprivaloma), Savarankiškas testas n (neprivaloma)		

Studijų medžiaga (Pavardė, vardas, inicialai. (Metai, mėnuo, diena). Straipsnio pavadinimas. Žurnalo / leidinio pavadinimas, tomo numeris (numerio numeris), viso straipsnio puslapių numeriai, leidėjas, URL).
Privaloma literatūra
...
Rekomenduojama literatūra
...

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau