Co-funded by the European Union

MAŽŲ IR VIDUTINIO DYDŽIO ĮMONIŲ KIBERNETINIO SAUGUMO POKYČIŲ AGENTŲ MOKYMŲ POREIKIŲ NUSTATYMO ATASKAITA

CYBER AGENT

2024-04-30

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

2 darbo paketas: CyberAgent koncepcija ir struktūros projektavimas

2.2 rezultatas: Mažų ir vidutinio dydžio įmonių (MVĮ) kibernetinio saugumo pokyčių agentų mokymų poreikių nustatymo ataskaita

2 darbo paketo lyderis – Olemisen Balanssia ry
2.2 rezultato lyderis – Olemisen Balanssia ry

TURINYS

ĮVADAS

Šios ataskaitos tikslas – išanalizuoti ir nustatyti mokymų poreikius, siekiant nustatyti kibernetinio saugumo pokyčių agentui, dirbančiam mažoje ar vidutinio dydžio įmonėje (MVĮ), reikalingas kompetencijas. Siekiant šio tikslo buvo atlikta rinkoje siūlomų švietimo programų apžvalga ir aiškinamasi apie MVĮ kibernetinio saugumo poreikius, norint užpildyti dabartinių kibernetinių kompetencijų spragas ir apibrėžti reikalingų įgūdžių rinkinį.

Kadangi kibernetinės grėsmės tampa vis sudėtingesnės, MVĮ būtina užtikrinti, kad jos turėtų tinkamai parengtus darbuotojus kovai su šiomis grėsmėmis. Šiame kontekste labai svarbus vaidmuo tenka kibernetinio saugumo srities pokyčių vykdytojams. Šioje projekto ataskaitoje kibernetinio saugumo sritis analizuojama iš įvairių perspektyvų: švietimas ir mokymas, lyčių įtrauktis ir dabartinė padėtis MVĮ ir mokyklose.

1. METODOLOGIJA

Atliekant tyrimą buvo derinami keli metodai: dokumentų ir šaltinių analizė (angl. desk research) ir empirinio tyrimo analizė (angl. field research).

Šio tyrimo metu buvo atliekama išsami literatūros analizė ir apžvalga apie kiekvienoje partnerėje šalyje:

- esamas ir kuriamas aukštojo mokslo ir profesinio mokymo institucijų kibernetinio saugumo srities programas. Atliekant šią analizę partneriai naudojo straipsnius, baltųjų knygų (angl. white papers), tyrimų ir ataskaitų, susijusių su kibernetinio saugumo mokymo turiniu ir poreikiais, informaciją;
- aukštojo mokslo ir profesinio mokymų kursus, jų mokymo programas ir jų atitikimas realiems kibernetinio saugumo iššūkiams.

Rengiant ataskaitą siekiami šių uždaviniai:

- Kiekvienoje projekto partnerės šalies aukštojo mokslo ir profesinio mokymo institucijose nustatyti kibernetinio saugumo kursų mokymo programų sudedamąsias dalis.
- Įvertinti, kaip šios mokymo programos atitinka kibernetinio saugumo iššūkius.
- Nustatyti, ar yra konkrečių strategijų ar programų, skirtų įtraukti daugiau moterų į kibernetinio saugumo studijas.

Pirminių šaltinių analizės etape atliktos 2 apklausos. Viena jų skirta aukštojo mokslo institucijų ir profesinio mokymo institucijų dėstytojams, siekiant suprasti dabartinių mokymo programų niuansus. Antroji skirta mažoms ir vidutinio dydžio įmonėms (MVĮ), siekiant suprasti kibernetinio saugumo situaciją įmonėse, jų darbuotojų įsitraukimą į kibernetinį saugumą, kibernetinio saugumo iššūkius ir poreikius, susijusius su kibernetiniu saugumu. Atliekant šį tyrimą taip pat buvo siekiama nustatyti darbuotojų charakteristikas, susijusias su kibernetiniu saugumu, mokymo poreikius, apie moterų įsitraukimą į kibernetinio saugumo sritį.

Apklausos buvo atliekamos visose projekto partnerėse šalyse ir šio tyrimo metu apklausta 190 dėstytojų iš aukštojo mokslo ir profesinio mokymo institucijų ir 176 darbuotojai iš mažų ir vidutinio dydžio organizacijų.

Apklausa Nr. 1: Projekto MVĮ kibernetinio saugumo pokyčių agentų poreikių nustatymas – **aukštojo mokslo ir profesinio mokymo institucijų apklausa**

Institucijos tipas	**Atsakymai**	**Moterys**	**Vyrai**	**Lytis nenurodyta**
Aukštojo mokslo institucijos	104	28	73	3
Profesinio mokymo institucijos	86	36	48	2
Viso	**190**	**64**	**121**	**5**

Apklausa Nr. 2: Projekto MVĮ kibernetinio saugumo pokyčių agentų poreikių nustatymas – **MVĮ apklausa.**

Institucijos tipas	**Atsakymai**
Smulkiojo ir vidutinio verslo įmonės	176
Viso	**176**

Apklausų klausimynai kartu su atsakymų statistika pateikiami C ir D prieduose.

2. TYRIMAS (VISI PARTNERIAI)

2.1. ŠVIETIMO IR MOKYMO PROGRAMOS

Šiame skyriuje aprašomas tyrimas ir pateikiamos įžvalgos, gautos atlikus dokumentų, šaltinių ir apklausų analizę, išryškinant projekto partnerėse šalyse teikiamų mokymų programų privalumus ir trūkumus.

2.1.1. KIBERNETINIO SAUGUMO MOKYMŲ APŽVALGA

Siekiant apibūdinti dabartinę kibernetinio saugumo švietimo situaciją visose šalyse partnerėse ir nustatyti svarbius kibernetinio saugumo švietimo ir mokymų aspektus, atlikta išsami kibernetinio saugumo švietimo aplinkos analizė.

Atlikus paiešką AIKOS duomenų bazėje paaiškėjo, kad Lietuvoje[1] iš viso yra šešios oficialios kibernetinio saugumo mokymo programos, kurias siūlo Lietuvos institucijos ir, kurios apima tiek bakalauro, tiek magistro studijų pakopas:

Studijų kryptis	Programa	Institucija	ECTS	Laipsnis
Informatikos inžinerija	Informacijos ir informacinių technologijų sauga[2]	Kauno technologijos universitetas	120	Informatikos mokslų magistras
Vadyba	Kibernetinio saugumo valdymas[3]	Mykolo Romerio universitetas	90	Verslo vadybos magistras
Informatikos inžinerija	Informacijos ir informacinių technologijų sauga[4]	Vilniaus Gedimino technikos universitetas	120	Informatikos mokslų magistras
Informatikos inžinerija	Informacijos sistemos ir kibernetinė sauga[5]	Vilniaus universitetas	210	Informatikos mokslų bakalauras
Informatikos inžinerija	Informacinių sistemų technologijos ir kibernetinė sauga[6]	Marijampolės kolegija	180	Informatikos mokslų profesinis bakalauras
Informatikos inžinerija	Kibernetinės sistemos ir sauga[7]	Kauno kolegija	180	Informatikos mokslų profesinis bakalauras

Kibernetinio saugumo magistrantūros programose taikomi skirtingi, tačiau vienas kitą papildantys principai. Kauno technologijos universitetas akcentuoja mokslinių tyrimų metodologiją, informacijos saugumo metodus ir teisinius elektroninės erdvės aspektus, daugiausia dėmesio skiria saugių IT sistemų projektavimo ir diegimo įgūdžių ugdymui. Vilniaus Gedimino technikos universitetas teikia pirmenybę sisteminio požiūrio į informacijos saugumo klausimus specialistų rengimui, derindamas mokslo žinias su informacijos saugumo užtikrinimo metodais ir technologijomis, ugdydamas kritinį mąstymą ir lyderystę. Mykolo Romerio universitetas išskirtinai orientuojasi į kibernetinio saugumo vadybą, siekiant parengti specialistus,

[1] Paieškai atlikti naudoti šie raktiniai žodžiai *kibernetinis, saugumas* ir šių raktinių žodžių kombinacijos. Šaltinis: https://www.aikos.smm.lt/Puslapiai/Pradinis.aspx
[2] https://www.aikos.smm.lt/studijuoti/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=LO&f=MokGal&key=8618_2023&pt=of&ctx_sr=8Gzz1EUqIeKfy0cWNVrrVdABKo0%3d
[3] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=2845&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[4] https://www.aikos.smm.lt/studijuoti/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=LO&f=MokGal&key=1442_2023&pt=of&ctx_sr=8Gzz1EUqIeKfy0cWNVrrVdABKo0%3d
[5] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=9664&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[6] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=2775&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[7] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=3797&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d

gebančius prižiūrėti šiuolaikines IT aplinkas ir spręsti sudėtingas kibernetinio saugumo užduotis, daug dėmesio skiriant strateginiam valdymui dinamiškame technologiniame kontekste.

Kibernetinio saugumo bakalauro studijų programos yra orientuotos į kvalifikuotų informatikos ir kibernetinio saugumo specialistų rengimą, tačiau kiekviena jų turi skirtingus akcentus. Vilniaus universiteto programa orientuota į visapusiškų informatikos inžinerijos pagrindų suteikimą, daugiausia dėmesio skiriant saugių informacinių sistemų analizei, projektavimui, kūrimui ir priežiūrai. Marijampolės kolegija, taip pat siekia rengti kompetentingus informatikos specialistus, daugiau dėmesio skiria praktiniams aspektams, pavyzdžiui, kompiuterių tinklų ir sistemų kūrimui, priežiūrai ir administravimui. Kauno kolegija išsiskiria tuo, kad siekia parengti specialistus, gebančius ne tik kurti ir diegti kibernetines sistemas, bet ir vadovauti komandoms, suprasti etines, teisines ir socialines pasekmes, efektyviai dirbti daugiakultūrinėje aplinkoje. Nors visos trys institucijos bakalauro studentams siekia suteikti techninių kibernetinio saugumo įgūdžių, jų tikslai skiriasi – nuo techninio išprusimo (Vilniaus universitetas), praktinio pritaikymo ir minkštųjų įgūdžių ugdymo (Marijampolės kolegija) iki techninių, vadovavimo ir etinių aspektų derinio (Kauno kolegija).

Atliekant šią analizę taip pat nustatytos keturios registruotos neformaliojo suaugusiųjų švietimo programos kibernetinio saugumo srityje, kuriose daugiausia dėmesio skiriama įgūdžiams, būtiniems atpažįstant, tiriant ir užkertant kelią kibernetinėms atakoms, ypač naudojant kriptografiją. Nors visos programos turi bendrą pagrindinį tikslą, jų metodai ir apimtys skiriasi. Vienos jų daugiausia dėmesio skiria kibernetiniam saugumui ir prevencinėms strategijoms, o kitos siūlo platesnę mokymo programą, įskaitant programavimą, apimančią tokias sritis kaip socialinė inžinerija, tapatybės valdymas ir rizikos valdymas. Pažymėtina, kad kelios programos prasideda nuo programavimo pagrindų ir pereina prie pažangių kibernetinio saugumo temų, tinkamų pradedantiesiems. Viena išskirtinė programa, parengta bendradarbiaujant su „Cybint“, skirta tiems, kurie turi mažai IT žinių, ir siūlo praktinius, realaus pasaulio įgūdžius studijuojantiems tiek dienine, tiek neakivaizdine forma. Šiomis programomis bendrai siekiama ugdyti įvairias kibernetinio saugumo kompetencijas, pradedant programavimo pagrindais ir baigiant išsamiu, į taikymą orientuotu mokymusi.

Suomijoje su kibernetiniu saugumu susijusioms švietimo programoms įtakos turėjo kelios Suomijos nacionalinio saugumo ir gynybos stiprinimo politikos kryptys. Daugėja mokslinių tyrimų ir plėtros iniciatyvų, švietimo ir mokymo programų bei sertifikuotų kibernetinio saugumo srities specialistų. Suomijos kibernetinio saugumo strategija (2019)[8] ir Kibernetinio saugumo plėtros programa (2021 m.) pabrėžia, kad svarbu ugdyti nacionalinę kibernetinio saugumo kompetenciją pasitelkiant švietimą ir mokslinius tyrimus. Kalbant apie mokyklinio ugdymo sistemą, siekiama, kad mokiniai įgytų įgūdžių ir žinių, padedančių saugiai naršyti skaitmeniniame pasaulyje, taip pat žinių apie kibernetines grėsmes ir apsaugos priemones.[9]

[8] https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/
[9] https://jyx.jyu.fi/bitstream/handle/123456789/86003/Lehto-IWS-018.pdf?sequence=1&isAllowed=y

Suomijos profesinio mokymo sistemoje kibernetinis saugumas daugumoje šaltinių nėra aiškiai išskiriamas kaip atskira ar specializuota sritis. Tačiau tai nebūtinai reiškia, kad kibernetinis saugumas visiškai neįtrauktas į profesinio mokymo programas. Atsižvelgiant į didėjančią skaitmeninio raštingumo ir kibernetinio saugumo svarbą visuose sektoriuose, šios temos integruojamos į IT ir techninio švietimo programas. Svarbu pažymėti, kad Suomijos profesinio mokymo teikėjai turi autonomiją siūlyti savo mokymus pagal regioninius ir konkrečios srities reikalavimus. Suomijos profesinis švietimas ir mokymas neseniai patyrė didžiausią per beveik 20 metų reformą. 2018 m. reformos tikslas – sukurti veiksmingesnę ir lankstesnę, kompetencijomis grindžiamą ir į klientus orientuotą profesinio mokymo sistemą, padidinti jos efektyvumą ir geriau suderinti kvalifikacijas su darbo rinkos poreikiais. Tai daugiausia pasiekta švelninant reguliavimą ir suteikiant daugiau savarankiškumo ir atsakomybės profesinio mokymo teikėjams.[10] Tai reiškia, kad kai kurios institucijos gali siūlyti labiau specializuotus modulius tokiose srityse kaip kibernetinis saugumas, atsižvelgiant į vietos pramonės poreikius ir bendradarbiavimo ryšius. Remiantis Lehto tyrimais, kibernetinis saugumas nėra atskiras dalykas, o integruotas į kitus dalykus, ypač informacinių ir ryšių technologijų (IRT) kontekste. Atsakomybė už mokymą tenka pedagogams, kurie kibernetinio saugumo ugdymą įtraukia į savo dėstomus dalykus. Dėl tokio požiūrio skirtingose mokymo įstaigose ir pakopose tai įgyvendinama nevienodai, todėl išryškėja poreikis taikyti struktūriškesnį ir nuoseklesnį požiūrį į kibernetinio saugumo mokymą, įskaitant galimą kibernetinio saugumo mokymo kaip atskiro dalyko arba kaip svarbesnės IRT ugdymo dalies sukūrimą.

Suomijos universitetai siūlo visapusiškas kibernetinio saugumo studijų programas. Šios programos skirtos suteikti studentams išsamių žinių ir įgūdžių įvairiose kibernetinio saugumo srityse. Daugelis jų siūlo informacijos saugumo ir informacinių technologijų magistro laipsnį, daugiausia dėmesio skiriant šių koncepcijų realiam taikymui. Šias studijų programas galima studijuoti kontaktiniu ir nuotoliniu būdu.

Belgijos kibernetinio saugumo sektoriuje didėja kvalifikuotų specialistų poreikis – 2022 m. lapkričio mėn. duomenimis buvo siūloma 4 000 laisvų kibernetinio saugumo darbo vietų. Siekiant šią spragą kuo skubiau užpildyti, pradėtos įgyvendinti įvairios iniciatyvos ir švietimo programos, skirtos šalies kibernetinio saugumo ekspertams ugdyti. Daugybė Belgijos institucijų, pavyzdžiui, KU Leuven, Solvay verslo mokykla, Howest taikomųjų mokslų universitetas ir daugelis kitų, parengė specializuotas programas anglų, prancūzų ir olandų kalbomis, kuriomis galima pasiekti plačią auditoriją. Tačiau Belgijos organizacijos Agoria atliktame tyrime pabrėžiama, kad reikia nuolat mokytis ir tiems specialistams, kurie nebestudijuoja, siekiant juos nuolat informuoti apie kibernetinį saugumą ir jos keliamas grėsmes. 2021-2025 m. Belgijos kibernetinio saugumo strategijoje pripažįstamas aukštas kibernetinio saugumo integravimo į šalies akademinę aplinką lygis ir pabrėžiamas pagrindinis universitetų ir kitų švietimo įstaigų vaidmuo skatinant mokslinių tyrimų ir plėtros pastangas šioje srityje. Belgijos kibernetinio saugumo centro (Centre for Cybersecurity Belgium (CBB) duomenų bazės duomenimis, Belgijoje aukštosios mokyklos siūlo 33 kursus (bakalauro, magistrantūros ir sertifikavimo), o tai sudaro įvairias profesinio rengimo ir mokymo programas, kurias siūlo tiek viešasis, tiek privatusis sektoriai. CBB yra institucija,

[10] https://www.cedefop.europa.eu/files/8133_en.pdf

prižiūrinti, koordinuojanti ir kontroliuojanti Belgijos kibernetinio saugumo strategijos įgyvendinimą, ir šiuo metu rengia nemokamus darbuotojų kibernetinio saugumo žinių mokymus Belgijos darbuotojams, siekiant stiprinti gyventojų kibernetinio saugumo žinias. Apskritai Belgijos kibernetinio saugumo strategijoje pabrėžiama kibernetinio saugumo žinių ir įgūdžių svarba pasitelkiant švietimą ir įsipareigojama didinti akademinių kursų skaičių, skatinti šios srities mokslinius tyrimus, skatinti STEM švietimą ir užtikrinti praktinio mokymo galimybes, kad būtų išspręsta didėjanti specialistų paklausa Belgijos kibernetinio saugumo srityje.

Norvegijoje kibernetinis saugumas neįtrauktas į pagrindinius dalykus, kuriuos galima studijuoti profesinio mokymo lygmeniu. Šios programos elementai yra įtraukti į profesinio mokymo programą „Kompiuteriai ir elektronika“. Švietimo ministerija nėra parengusi kibernetinio saugumo sistemos, tik bendrųjų skaitmeninio raštingumo pagrindų įgūdžių programoje, skirtoje visoms švietimo įstaigoms, paminėta, kad studentai turėtų mokėti naudotis skaitmeniniais ištekliais tinkluose ir už jų ribų, taip pat užtikrinti informacijos ir duomenų saugumą.

2023 m. Nacionalinėje kibernetinio saugumo kompetencijų strategijoje[11] pažymima profesinių mokyklų studentų švietimo kibernetinio saugumo srityje svarba. Tai labai aktualu ir svarbu daugeliui profesinio mokymo dalykų. Profesinio mokymo programose trūksta kibernetinio saugumo mokymo medžiagos, o dėstytojams trūksta įgūdžių mokyti, ypač tokiose srityse kaip privatumas, išmaniųjų namų technologijos ir daiktų internetas. Egzistuojančios kibernetinio saugumo mokymo programos, pavyzdžiui, GenCyber ir CyberFirst, konkrečiai neatsižvelgia į šios profesinio mokymo programos poreikius[12,13].

Bendradarbiaujant su Oslo universitetu (UiO), Norvegijos mokslo ir technologijų universitetu (NTNU) ir atrinktais profesinio rengimo mokyklų destytojais, planuojama parengti kibernetinio saugumo mokomąją medžiagą, kuri vėliau bus pateikta nacionalinėje mokymosi platformoje (NDLA, angl. National Digital Learning Arena).[14]

Aukštosiose mokyklose siūlomos tiek Skaitmeninio saugumo kultūros vienerių metų trukmės programa, tiek kibernetinio saugumo bakalauro programos. Kibernetinio saugumo dalykas taip pat įtrauktas į kelias duomenų mokslų ir informatikos magistrantūros programas. Yra įvairių specifinių kibernetinio saugumo studijų, tokių kaip taikomosios kompiuterių ir informacinių technologijų, kibernetinio saugumo bakalauro, skaitmeninės kriminalistikos bakalauro, skaitmeninės infrastruktūros ir kibernetinio saugumo, skaitmeninio saugumo kultūros ir patirtimi grindžiamos informacijos saugumo magistro studijos. Taip pat yra studijų, į kurias įtrauktas kibernetinis saugumas, kaip saugumo (angl. HSE, Health, Safety, and Environment) kultūra ir vadovavimas, savivaldybių pasirengimo ekstremalioms situacijoms koordinatoriai ir valdybos darbas praktikoje bei metinės krizių valdymo studijos.

[11] https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhetskompetanse/id2627189/
[12] https://www.mn.uio.no/ifi/studier/masteroppgaver/informasjonssikkerhet/lering-av-cybersikkerhet-i-yrkesfag.html
[13] https://www.duo.uio.no/bitstream/handle/10852/96151/5/Master_thesis_mariwilh.pdf
[14] https://ndla.no/

Lenkijoje pastaraisiais metais padaugėjo kibernetinių tyrimų. Universitetuose atidaroma vis daugiau kibernetinių kursų, kartu daugėja ir profesinio mokymo kursų. Pastaraisiais metais Lenkijoje išaugo kibernetinių profesijų paklausa, taip pat padidėjo Lenkijos visuomenės informuotumas apie kibernetinį saugumą, o tai skatina įmones įdarbinti kibernetinius ekspertus ir apsaugoti informaciją.

Lenkijoje, kaip ir daugumoje Europos šalių, akademinis laipsnis laikomas privalomu, todėl pabaigusiems studijas kibernetiniai kursai dažnai siūlomi kaip papildomos studijos. Dauguma tokių studijų yra ilgesnės trukmės, bet teorinio pobūdžio. Yra kibernetinių kursų, kurie yra trumpi, tačiau dauguma jų orientuoti į praktinį mokymąsi. Didelis iššūkis kibernetinės srities studentui yra tai, kad dauguma profesinio mokymo įstaigų neturi savo finansavimo, tad reikia ieškoti finansinio sprendimo, todėl ši galimybė ne visada tinka besidomintiesiems.

Nors kibernetinis saugumas turėtų būti visų veiklos sričių prioritetas, Rumunijos profesinio rengimo ir mokymo sistema dar nėra pasirengusi užtikrinti paruošti kompetentingus studentus šioje srityje. Išanalizavus licėjaus technologinės srities žemesnės pakopos bet kurios profesinio mokymo srities mokymo programą, techninės kultūros mokyklinėje programoje nenumatyti mokymosi rezultatų elementai apie kibernetinį saugumą. Kai kurias konkrečias šios srities kompetencijas galima rasti bendrųjų žinių programoje, informacinių ir komunikacinių technologijų disciplinoje, 9 klasės mokymo programoje:

1. Saugumo priemonių aprašymas ir taikymas naudojantis internetu:

- Išmanus interneto naudojimas,
- Duomenų perdavimo šifravimo svarba,
- Skaitmeninio parašo naudojimas,
- Apsaugos nuo virusų būdai.

2. Pokalbių paslaugos naudojimas:

- Bendradarbiavimo programų, skirtų vaizdo konferencijoms, pristatymas,
- IRC tinklo taisyklių pristatymas,

Aukštesniojo lygio vidurinėje mokykloje, 11 klasėje, tik profesinio mokymo srityje „Elektroninė automatika“, skirtoje „Telekomunikacijų technikas“, „Kompiuterių operatorius technikas“, „Telematikos operatorius technikas“ specializacijoms, siūlomas tam tikras turinys apie saugumo programų diegimą. 12-oje klasėje tik kompiuterių techniko specializacijoje į specializuotą modulį įtrauktas toks turinys kaip:

- Pagrindiniai kompiuterių sistemų ir kompiuterių tinklų saugumo principai,
- Tinklo saugumo politikos kūrimas,
- Tinklų saugumo grėsmės,
- Naršymo internete apsauga,
- Virusai ir saugumo programos.

Kalbant apie aukštąjį mokslą, Transilvanijos Brašovo universitetas demonstruoja didelį dėmesį kibernetinio saugumo švietimui, siūlydamas išsamią kibernetinio saugumo magistrantūros programą, vykdomą tik anglų kalba. Universiteto siekis puoselėti šios svarbios srities žinias akivaizdus nagrinėjant šių studijų mokymo programą.

Ši Transilvanijos universiteto magistrantūros programa studentams suteikia galimybę įgyti visapusišką kibernetinio saugumo išsilavinimą tarptautinėje akademinėje aplinkoje. Patikimos mokymo programos ir dėstymo anglų kalba derinys leidžia absolventams sėkmingai dirbti dinamiškoje ir sudėtingoje kibernetinio saugumo srityje.

Babes-Bolyai universitetas Klužo-Napokoje Matematikos ir informatikos fakultete nuo 2023-2024 akademinių metų inicijavo kibernetinio saugumo anglų kalba magistrantūros programą, kuria siekiama parengti būsimus šios srities specialistus. Priėmimo į šias studijas metu pritraukta daugiau studentų nei tikėtasi. Daugiau nei 40 į programą priimtų studentų, tarp jų ir iš užsienio, taps kibernetinio saugumo srities specialistais. Studentai netgi gali rinktis akademinius metus studijuoti kituose garsiuose Europos universitetuose.

Matematikos ir informatikos fakulteto magistrantūros programoje „Interneto technologijos“ (anglų kalba) pirmojo kurso antrajame semestre siūlomas kriptografijos ir sistemų saugumo kursas, kuriame studentai supažindinami su kibernetinio saugumo sritimi ir konkrečiais duomenų šifravimo metodais. Be to, magistrantūros programoje „Šiuolaikinės technologijos programinės įrangos sistemų inžinerijoje“ pirmajame antrųjų metų semestre siūlomas pasirenkamasis kursas „IT sistemų saugumas“. Abu minėti kursai leidžia magistrantams įgyti žinių ir patirties kibernetinio saugumo srityje ir susipažinti su šiuolaikinių sistemų šifravimo ir saugumo iššūkiais.

Bukarešto universiteto Matematikos ir informatikos fakulteto magistrantūros programoje „Saugumas ir taikomoji logika“ (anglų kalba) siūlomi kriptografijos ir sistemų saugumo kursai. Studentai gali įgyti žinių operacinių sistemų saugumo, kriptografijos, tinklo saugumo ir kibernetinio saugumo srityse.

Ispanijoje dauguma kibernetinio saugumo studijų yra aukštojo mokslo lygmens (bakalauro ir magistro studijos). Ispanijos nacionalinio kibernetinio saugumo instituto surinktais duomenimis, Ispanijoje yra:

- 87 kibernetinio saugumo magistro laipsnį suteikiančių programos, kurias siūlo valstybiniai ir privatūs universitetai bei kitos aukštojo mokslo įstaigos;
- 4 specializacijos, daugiausia kompiuterių kriminalistikos specializacijos;
- 3 universitetinį laipsnį suteikiančios programos, kurias siūlo privatus sektorius.

Ispanijos profesinio mokymo įstaigose yra apie 60 mokymo kursų. Visi jie reglamentuojami pagal tą pačią mokymo programą, kurią 2020 m. gegužės mėn. patvirtino Švietimo ministerija 2020 m. balandžio 7 d. Karališkuoju dekretu 479/2020, kuriuo nustatomas kibernetinio saugumo informacinių technologijų aplinkoje specializacijos kryptis.

Nepaisant vykdomų programų, pripažįstama, kad reikia dėti daugiau pastangų. Ispanija įgyvendino įvairius planus, įskaitant Nacionalinį skaitmeninių įgūdžių planą, 2021-2025 m. mažų ir vidutinio dydžio įmonių skaitmeninimo planą ir Ispanijos skaitmeninį 2025 m. planą, kuriuose daugiausia dėmesio skiriama naujų talentų kūrimui, kad būtų užtikrintas didėjantis skaitmeninių įgūdžių, ypač kibernetinio saugumo srityje, poreikis.

Turkijoje kibernetinio saugumo poreikis sparčiai išaugo ir tapo labai svarbus tiek pačioje šalyje, tiek visame pasaulyje, ypač pastaraisiais metais. Kartu su technologine raida tuo pačiu tempu keitėsi ir kibernetinė rizika bei grėsmės, kurios tampa sudėtingesnės. Kibernetinė rizika ir grėsmės pasiekė tokį lygį, kad gali sukelti daug platesnio masto ir neigiamų padarinių nei fizinės atakos. Kadangi tokie sektoriai kaip finansų, elektroninių ryšių, energetikos, transporto ir aviacijos teikia paslaugas saugioje skaitmeninėje aplinkoje, nacionalinio kibernetinio saugumo užtikrinimas tapo vienu svarbiausių mūsų šalies prioritetų. Atsižvelgiant į tai, tyrimais ir toliau siekiama skleisti kibernetinio saugumo mokymus profesinio mokymo ir aukštojo mokslo įstaigose, atsižvelgiant į šio sektoriaus poreikius, ir plėtoti bei turtinti mokymo turinį.

Profesiniam lavinimui kibernetinio saugumo pagrindų kursą sudaro: programavimo pagrindai, sistemų saugumas, tinklų technologijos, saugus programinės įrangos kūrimas, įsiskverbimo testavimas ir reagavimas į kibernetinius incidentus, kompiuterinė kriminalistika ir kt.

Aukštojo mokslo srityje siūloma „Kibernetinio saugumo analitiko ir operatoriaus“ asocijuotojo laipsnio programa kibernetinio saugumo profesinėse mokyklose, kriminalistinės kompiuterių inžinerijos bakalauro programa universitetuose ir atitinkamos magistrantūros programos universitetuose.

Be to, universitetų tęstinio mokymo centrai, savivaldybių viešojo švietimo centrai, oficialios institucijos, tokios kaip TÜBİTAK (angl. Scientific and Technological Research Council of Türkiye), TSE (angl. Turkish standards institute) ir privačios švietimo įstaigos taip pat rengia mokymus apie kibernetinį saugumą.

2.1.2. KIBERNETINIO SAUGUMO IŠŠŪKIAI IR POREIKIAI PRAMONĖJE

Remiantis išsamia literatūros apžvalga, įvardijami kibernetinio saugumo iššūkiai, su kuriais susiduria mažos ir vidutinio dydžio įmonės (MVĮ) projekto šalyse partnerėse. Besikeičiančioje kibernetinio saugumo aplinkoje Lietuvos MVĮ susiduria su daugybe kibernetinio saugumo iššūkių. Kadangi šių įmonių veikla vis labiau priklauso nuo skaitmeninių technologijų, jos tampa labiau pažeidžiamos įvairių kibernetinių grėsmių, todėl, norint veiksmingai valdyti šias grėsmes, būtina visapusiškai suprasti ir laikytis strateginio požiūrio.

2022 m. tyrime Bukauskas ir kt.[15] išskyrė organizacijų tipus pagal jų kibernetinio saugumo brandą ir kompetencijų poreikius. Mažos įmonės, anot tyrimo, prilygsta pavieniams asmenims visuomenėje, nes pagrindinis skaitmeninės darbo vietos saugumo parametras yra kibernetinės higienos

[15] Bukauskas, L., Brilingaitė, A., Lepaitė, D., Juozapavičius, A., Ikamas, K., 2022. ‘Projekto Kibernetinio saugumo kompetencijų žemėlapio kūrimas ataskaita’, Vilniaus universitetas Informatikos institutas. Available at: https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf [Accessed 12 January 2024]. DOI: https://doi.org/10.15388/CIBERSEK.2022.

lygis, kuriam įtakos turi bendras kibernetinio saugumo grėsmių supratimas. Šiame lygyje kibernetinis saugumas koordinuojamas įmonės viduje, todėl galimi verslo procesų saugumo pažeidimai. Vidutinio dydžio verslo įmonėse kibernetinio saugumo valdymas ir reguliavimas taip pat silpnai koordinuojamas. Reagavimas į incidentus ar kitą kibernetinio saugumo veiklą įmonėje taip pat nėra akcentuojamas. Atsižvelgdami į tai, kad smulkaus verslo įmonės Lietuvoje sudaro 97 proc. visų įmonių, Bukauskas ir kt. (2022) daro išvadą, kad yra didelis IT specialistų, kurie teiktų IT paslaugas, konsultuotų vartotojus ir, kurių darbo funkcijos apimtų pagrindinių kibernetinio saugumo principų užtikrinimą, poreikis. Šiame tyrime taip pat pabrėžiama, kad pastebimas grėsmių žvalgybos ir mokslinių tyrimų trūkumas, taip pat matomas kibernetinio saugumo specialistų poreikis saugumo inžinerijos ir sistemų gyvavimo ciklo.

Prieš kelerius metus įgyvendinant „Kurk Lietuvai“ programą, bendradarbiaujant su Krašto apsaugos ministerija, surengtos viešosios konsultacijos dėl mažų ir vidutinio dydžio įmonių informuotumo kibernetinio saugumo srityje didinimo[16]. Įgyvendinant šią inciatyvą prieita prie išvados, kad akivaizdu, jog Lietuvos mažųjų ir vidutinių įmonių informuotumo apie kibernetinį saugumą lygis nėra aukštas ir, kad smulkiojo verslo įmonės nepasiekė tinkamo kibernetinio atsparumo lygio dėl nepakankamo skaitmeninės rizikos supratimo. Be to, iniciatyvoje pažymėta, kad daugiau nei pusė (57 proc.) įmonių vadovų teigė, kad jiems trūksta arba jie nėra tikri, ar turi pakankamai žinių kibernetinio saugumo sprendimams pasirinkti, o daugiau nei trys ketvirtadaliai darbuotojų sutiko, kad jiems trūksta lengvai suprantamos informacijos.

Lyginant Bukausko ir kt. (2022) ir ankstesnės iniciatyvos „Kurk Lietuvai“ (2019) rezultatus, akivaizdu, kad Lietuvos mažosiose ir vidutinio dydžio įmonėse (MVĮ) kibernetinio saugumo pažanga yra nedidelė. Abiejuose tyrimuose pabrėžiama, kad šiose įmonėse nuolat trūksta pagrindinių kibernetinio saugumo žinių ir pasirengimo. Nepaisant didėjančios priklausomybės nuo skaitmeninių technologijų, MVĮ ir toliau pasižymi pažeidžiamumu dėl nepakankamo kibernetinio atsparumo ir bendro skaitmeninių rizikų nesupratimo. Šis nuolatinis iššūkis rodo, kad būtina skubiai gerinti mažų ir vidutinio dydžio organizacijų (kurios sudaro didžiąją dalį Lietuvos verslo aplinkos) informuotumą apie kibernetinį saugumą ir mokymus.

Suomijos ekonominių tyrimų instituto ETLA (Elinkeinoelämän tutkimuslaitos) atliktas tyrimas parodė, kad per dvejus metus duomenų apsaugos pažeidimų skaičius Suomijos įmonėse, įskaitant MVĮ, padvigubėjo. Suomijos įmonės 2019 m. pranešė apie duomenų saugumo pažeidimus tris kartus dažniau nei Europos vidurkis, o dauguma incidentų buvo susiję su sukčiavimu, sukčiavimo atakomis, duomenų apsaugos pažeidimais, kenkėjiškomis programomis ir pažeidžiamumu. Šiame tyrime taip pat pabrėžiama, kad kvalifikuotų kibernetinio saugumo specialistų trūkumas yra pagrindinis Suomijos MVĮ iššūkis[17].

Suomijos nacionalinis kibernetinio saugumo centras (NCSC-FI)[18] yra Suomijos vyriausybės vadovaujama iniciatyva. Centras veikia kaip Suomijos transporto ir ryšių agentūros (Traficom, kuri yra vyriausybinė agentūra, atsakinga už Suomijos ryšių ir transporto sektorių reguliavimą) dalis. Jie

[16] Create for Lithuania and Ministry of National Defense, 2019. SVV Kibernetinio Saugumo Apklausos Apžvalga. [online] Available at: http://kurklt.lt/wp-content/uploads/2019/12/SVV-kibernetinio-saugumo-apklausos-ap%C5%BEvalga-Kurk-Lietuvai.pdf

[17] https://www.etla.fi/en/publications/kyberuhat-yleistyvat-miten-suomen-yritykset-parjaavat/

[18] https://www.kyberturvallisuuskeskus.fi/en

teikia informaciją apie dabartinę kibernetinio saugumo būklę ir siūlo gaires bei priemones, skirtas tiek asmenims, tiek organizacijoms, kad jos galėtų pagerinti savo kibernetinio saugumo praktiką. Centras taip pat dalyvauja nacionalinėse kibernetinio saugumo iniciatyvose, pavyzdžiui, įspėjimuose apie pažeidžiamumą, ir skatina informuotumą bei pasirengimą kibernetinėms grėsmėms.

Jų kassavaitinėse apžvalgose galima susipažinti su kokiais iššūkiais susiduria MVĮ. Suomijos MVĮ, kaip ir daugelis kitų, susiduria su tomis pačiomis saugumo problemomis, kurias aprašė ETLA institucija, nes yra daugelio sukčiavimo ir apgaulingų pranešimų taikinys. Tarp jų – bandymai apsimesti teisėtomis tarnybomis, pavyzdžiui, Suomi.fi, siekiant apgaulės būdu išvilioti prisijungimo duomenis ar kitą jautrią informaciją. MVĮ finansiniai ištekliai gali riboti galimybes diegti modernius kibernetinio saugumo sprendimus, skirtus apsisaugoti nuo kibernetinių grėsmių. Kita vertus, jau net ir toms MVĮ, kurios įsidiegusios saugumo priemones, kyla sunkumų, siekiant neatsilikti nuo kylančių kibernetinio saugumo grėsmių.

Siekiant išsiaiškinti kibernetinio saugumo padėtį Belgijos mažose ir vidutinio dydžio įmonėse, buvo atliktas išsami analizė, kurios metu buvo sudėtinga gauti išsamių duomenų ar šaltinių, kuriuose būtų nagrinėjamas šis itin svarbus klausimas. Dėl tokio informacijos trūkumo sunku sukurti veiksmingas strategijas ir sprendimus, kurie padėtų MVĮ apsaugoti savo skaitmeninį turtą nuo kibernetinių grėsmių.

Kadangi „Women4Cyber“ fondas turi didelį tinklą, tyrėjams pavyko susisiekti su profesionalais, kurie aktyviai dirba kibernetinio saugumo srityje Belgijoje. Šios ekspertės pateikė tyrimui svarbių įžvalgų ir perspektyvų, kurios padėjo suprasti įvairius iššūkius, su kuriais susiduria MVĮ kibernetinio saugumo srityje. Įžvalgų pateikė Iva Taševa, gerai žinoma Belgijos fondo „Women4Cyber“ narė, kuri pasidalijo savo patirtimi ir žiniomis apie iššūkius, su kuriais MVĮ susiduria bandydamos apsaugoti savo skaitmeninę infrastruktūrą nuo kibernetinių grėsmių.

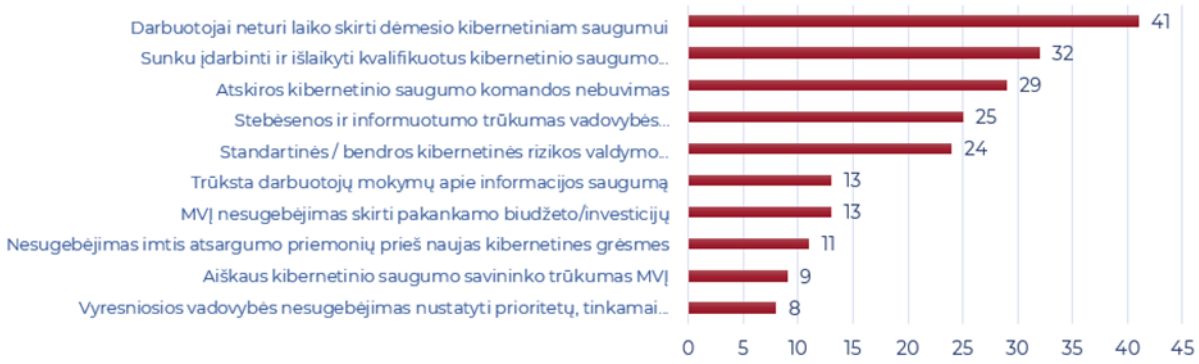
MVĮ susiduria su keliomis kibernetinio saugumo problemomis, pavyzdžiui, sunkumais gaunant ad-hoc pagalbą, nepakankamu darbuotojų mokymu apie tapatybės ir prieigos valdymą ir ribotu debesijos paslaugų vaidmenų ir pareigų supratimu. Be to, MVĮ turi ribotą prieigą prie įperkamų pažeidžiamumo nuskaitymo sprendimų ir stebėsenos priemonių, todėl yra labiau pažeidžiamos kibernetinių grėsmių. MVĮ susiduria su tapatybės vagystėmis ir sukčiavimu, o sukčiavimas ir sukčiai kelia nuolatinę riziką. Siekdamos spręsti šias problemas, MVĮ turi imtis aktyvių priemonių, įgyvendinti patikimus saugumo protokolus ir visapusiškai šviesti darbuotojus, kad sustiprintų jų įgūdžius ir apsisaugotų nuo galimų pažeidimų ir finansinių nuostolių.

Kibernetinis saugumas tapo vienu svarbiausių Ispanijos įmonių, įskaitant mažas ir vidutinio dydžio įmones, prioritetų. Didėjant nuotolinio darbo ir internetinių užsiėmimų skaičiui, plačiai naudojamos nuotolinio darbo vietos funkcijos, debesų kompiuterija ir bendradarbiavimo priemonės, be kita ko, didėja rizika ir kompiuterinių atakų skaičius. Nacionalinio kriptologijos centro (CCN-CERT) ataskaitoje nuotolinio darbo ir technologijų naudojimo didėjimas siejamas su šios rizikos padidėjimu. Dažniausios atakos, nuo kurių nukentėjo įmonės, yra išpirkos reikalaujančios programos ir atakos prieš nuotolinės prieigos sistemas. Dėl padidėjusių kibernetinių grėsmių įmonės padidino kibernetinio saugumo komandoms priskirtų žmonių skaičių – tiek vidinių, tiek išorinių.

Tačiau nepaisant to, įmonės vis dar apie 50 proc. šių funkcijų paveda atlikti išorės paslaugų teikėjams.

Be to, 21 % Ispanijos įmonių vis dar neturi saugumo operacijų centrų (SOC) incidentams apdoroti. Kalbant apie kibernetinio saugumo mokymą verslo aplinkoje, Deloitte tyrime pabrėžiama, kad 2022 m., palyginti su 2021 m. duomenimis, analizuojamų įmonių darbuotojų kibernetinio saugumo mokymų internetu valandų skaičius išaugo beveik 30 proc. Tačiau beveik 50 proc. įmonių Ispanijoje neturi jokių kibernetinio saugumo sertifikatų, o tai yra akivaizdus iššūkis ateičiai.

Vis dėlto didžiausias iššūkis, su kuriuo susiduria Ispanijos įmonės, tebėra talentingų kibernetinio saugumo specialistų trūkumas. Remiantis ObservaCiber parengta ataskaita „Kibernetinio saugumo talentų Ispanijoje analizė ir diagnozė“, 2021 m. Ispanijoje trūko 24 119 darbuotojų. Apskaičiuota, kad 2024 m. Ispanijai reikės daugiau kaip 83 000 specialistų, taigi darbuotojų trūkumas padidės iki 57,5 proc.
Silpniausia grandis, dėl kurios MVĮ susiduria su kibernetinio saugumo problemomis, yra žmogiškasis veiksnys. Didžiausias iššūkis MVĮ yra tai, kad už kibernetinį saugumą atsakingi darbuotojai negali skirti pakankamai laiko kibernetinio saugumo sričiai, nes jie yra atsakingi už daugiau nei vieną sritį. Su tuo susijęs atskiros kibernetinio saugumo grupės nebuvimas Turkijoje užima trečią vietą MVĮ patiriamų kibernetinio saugumo valdymo sunkumų sąraše. MVĮ susiduria su problemomis įdarbinant ir išlaikant kvalifikuotus kibernetinio saugumo darbuotojus.



1 pav. MVĮ iššūkiai – Turkijos tyrimas.

Rumunijoje internetinė aplinka suteikia verslo galimybių ir ryšių, kurie gali padėti MVĮ vystytis, tačiau joje esama ir daug rizikos.

Duomenų saugumo pažeidimų tyrimo ataskaitoje teigiama, kad mažos ir vidutinio dydžio įmonės (MVĮ) patyrė 16 312 saugumo incidentų, iš kurių 5 199 buvo patvirtinti kaip duomenų saugumo pažeidimai.

Analizuojant Verozon ir Duomenų saugumo pažeidimų tyrimo ataskaitas pastebimi svarbūs aspektai:

- MVĮ ir korporacijų atakų paviršiai yra panašūs, kadangi organizacijos naudoja debesų programinę įrangą.
- Neteisėtas įsiskverbimas į sistemą, socialinės inžinerijos metodai ir pagrindinės žiniatinklio programų atakos sudaro 92 % visų MVĮ užregistruotų pažeidimų atakų tipų (korporacijų atveju – 85 %). Nesankcionuotas įsiskverbimas į sistemą – sudėtingos atakos, kurių metu naudojamos kenkėjiškos programos ir (arba) įsilaužimai. Išpirkos reikalaujanti programinė įranga sudaro 24 % atvejų (duomenys pavagiami prieš juos užšifruojant).
- Išorės užpuolikai kelia didžiausią grėsmę, sukeliančią 83 % dabartinių saugumo pažeidimų, o MVĮ atakų atveju šis skaičius siekia 94 %. 94 % grėsmių dalyvių yra išoriniai, palyginti su 89 % didelių organizacijų atveju, o 98 % pažeidimų atvejų finansinė motyvacija, palyginti su 97 % korporacijų atveju.
- Finansinė motyvacija yra pirmoje vietoje 95 % visų atvejų, o MVĮ atakų atveju šis procentas padidėja iki 98 %. Tik 1 % motyvuoja šnipinėjimas.
- Darbuotojai yra silpnoji saugumo grandis – 74 % visų atvejų (prastas informuotumas apie kibernetines grėsmes). Pagrindinis įsilaužimo būdas gali būti susijęs su pavogtų prisijungimo duomenų naudojimu – 49 % ir „phishing“ – 12 % arba kitais metodais, pavyzdžiui, netinkama konfigūracija arba klaidingas neskelbtinų duomenų siuntimas.
- Kompromituojantys verslo elektroniniai laiškai – auka apgaule įtikinama pervesti dideles pinigų sumas į užpuolikų sąskaitas.

Norvegijoje daugelis mažų ir vidutinio dydžio įmonių (MVĮ) nepakankamai gerai supranta su tuo susijusią riziką, todėl atsiranda potencialių pažeidžiamumų. Pastebimas veiksmingo darbuotojų mokymo kibernetinio saugumo klausimais trūkumas, todėl žmogiškosios klaidos yra dažnas rizikos veiksnys. MVĮ, ypač tos, kurios nurodo turinčios ribotus išteklius, dažnai susiduria su sunkumais investuodamos į pažangias kibernetinio saugumo priemones ir kvalifikuotus darbuotojus. Joms taip pat reikia orientuotis sudėtinguose duomenų apsaugos įstatymuose, todėl užtikrinti atitiktį reikalavimams saugant jautrią informaciją tampa dar sudėtingiau. Jų pažeidžiamumą dar labiau parodo padažnėjusios „phishing“ atakos ir socialinė inžinerija, taip pat nepakankamas tinklo saugumas ir vidinių grėsmių rizika. Šių rizikų valdymas yra labai svarbus, tačiau MVĮ dažnai susiduria su iššūkiais, susijusiais su veiksmingu rizikos vertinimu ir valdymu. Be to, priklausomybė nuo trečiųjų šalių tiekėjų sukuria dar vieną sudėtingumo lygmenį, dėl kurio MVĮ gali kilti papildomų kibernetinio saugumo grėsmių.

2.2. MOTERYS KIBERNETINIO SAUGUMO SRITYJE

Šio tyrimo metu analizuota moterų mokymo ir palaikymo poreikius, esamą kibernetinio saugumo srityje dirbančių moterų kvalifikaciją ir kompetenciją bei rekomendacijas, kaip įtraukti daugiau moterų darbuotojų į kibernetinio saugumo sritį.

„Microsoft“ atliko apklausą, pagal kurią 35 Europos šalyse mažiau nei 1 iš 5 informatikos mokslus baigusių absolventų buvo moterys. Susidomėjimas gamtos mokslais, technologijomis, inžinerija ir matematika (STEM dalykais) sumažėja per anksti. Iš tiesų EBPO Tarptautinio mokinių vertinimo programos (PISA) duomenimis, berniukai daug dažniau nei mergaitės įsivaizduoja save kaip IRT specialistus, mokslininkus ar inžinierius.

Vertinant moterų dalį tarp dirbančių IRT specialistų, 2020 m. 27 ES valstybėse narėse tik 18,5 %. visų IRT specialistų buvo moterys. Didžiausia moterų dalis buvo Bulgarijoje – 28,2 %, Graikijoje – 26,6 % ir Rumunijoje – 26,2 % (žr. 5 diagramą („Women go tech“, 2021 m.)). Šiaurės ir Baltijos regiono šalys taip pat dažniausiai buvo netoli sąrašo pabaigos, išskyrus Norvegiją, kuri buvo labiau ties šalių reitingo viduriu. (Women go tech, 2021).

Lietuvos Respublikos statistikos departamento duomenimis, 2022 m. ketvirtąjį ketvirtį informacijos ir ryšių kategorijoje dirbo 29,4 tūkst. vyrų ir 21,5 tūkst. moterų. 2023 m. pirmąjį ketvirtį – 34,6 tūkst. vyrų ir 20,7 tūkst. moterų. Antrąjį 2023 m. ketvirtį – 36,8 tūkst. vyrų ir 14,8 tūkst. moterų, o trečiąjį 2023 m. ketvirtį – 34,5 tūkst. vyrų ir 18,0 tūkst. moterų. Nuo 2023 m. pirmojo ketvirčio iki antrojo ketvirčio pastebimas moterų darbuotojų skaičiaus sumažėjimas, o 2023 m. trečiąjį ketvirtį – padidėjimas (Rodiklių Duomenų Bazė - Oficialiosios Statistikos Portalas, n.d.).

Kadangi kibernetinio saugumo srityje Europoje ir pasaulyje dirba iki 11 % moterų[19,20], Lietuvoje buvo atlikta apklausa, kuria siekta išsiaiškinti visuomenės nuomonę apie moterų perspektyvas šioje srityje. Apklausoje 44,4 % didmiesčių respondentų atsakė, kad moterų kibernetinio saugumo srityje turėtų būti nuo 30 iki 60 %. Didžiausia dalis respondentų atsakė, kad moterys turėtų sudaryti nuo 30 iki 60 proc. specialistų (35,2 proc.). Analizuojant atsakymus pagal lytį ir amžiaus grupes, matyti, kad moterys, ypač jaunesnės (iki 25 m. ir 25-45 m.), dažniausiai mano, kad moterų turėtų būti maždaug pusė. Jauni vyrai (iki 25 m.) mano, kad moterų turėtų būti iki 30 %. Matyti, kad pačios moterys linkusios matyti daug didesnį moterų skaičių kibernetinio saugumo srityje, nei šiuo metu yra rinkoje. Tai gera žinia, nes moterų pritraukimas į šią sritį padėtų ne tik spręsti specialistų trūkumo problemą, bet ir padidintų pačių įmonių saugumą. (Bukauskas et al., 2022).

Suomijoje, kaip ir daugelyje Europos šalių, vyrauja bendras supratimas apie lyčių disbalansą kibernetinio saugumo ir apskritai IT srityje. Iniciatyvų ir pastangų remti moteris kibernetinio

[19] ENISA. Diversity in Cybersecurity. techreport. 2021. https://ecsc.eu/about/diversity-flyer-online.pdf

[20] Women4Cyber Lietuva. Moterys griauna mitus apie kibernetinį saugumą: Lietuvoje be darbo neliks. 2021. https://www.15min.lt/verslas/naujiena/mokslas-it/moterys-lietuvoje-griauna-mitus-apie-kibernetini-sauguma-nauju-tikslu-reikia-siekti-naudojant-naujus-metodus-1290-1515246

saugumo srityje ir skatinti jų dalyvavimą sprendžiant kibernetinio saugumo iššūkius padaugėjo. Daugumą jų remia ne pelno siekiančios organizacijos.

Kibernetinio saugumo srityje buvo įgyvendinta keletas iniciatyvų, skirtų švietimo ir karjeros galimybėms, mokymo programoms ir tinklų kūrimo renginiams plėtoti. Strategija taip pat grindžiama pavyzdžių skatinimu, atkreipiant dėmesį į sėkmingą moterų karjeros kelią kibernetinio saugumo srityje ir dalijantis jų istorijomis, siekiant įkvėpti daugiau moterų siekti karjeros šioje srityje. „Women4Cyber“ strategijoje ir išvardytose iniciatyvose pabrėžiama įvairovės ir įtraukties svarba, siekiant ne tik spręsti lyčių nelygybės disbalanso problemą, bet ir prisidėti prie bendro kibernetinio saugumo sektoriaus stiprumo ir atsparumo. Viešosios ir privačios institucijos taip pat remia šią strategiją, įtraukdamos šį lyčių lygybės aspektą kaip vieną iš svarbiausių prioritetų į visas savo iniciatyvas.

Women4Cyber Finland (W4CFI)

2021 m. rugpjūtį įsteigta W4CFI yra ne pelno siekianti organizacija, kurios tikslas – didinti Suomijos kibernetinio saugumo pramonėje dirbančių moterų skaičių. Ji yra didesnės ES masto iniciatyvos „Women4Cyber“ dalis ir daugiausia dėmesio skiria įvairesnei ir įtraukesnei pramonei Suomijoje remti. W4CFI dalyvauja įvairioje veikloje, įskaitant rekomendacijų teikimą, keitimąsi žiniomis ir informuotumo didinimą, siekiant didinti ir remti moterų įsitraukimą į kibernetinio saugumo sritį.[21]

Suomijos transporto ir ryšių ministerijos ir Aalto universiteto projektas

Suomijos transporto ir ryšių ministerija, bendradarbiaudama su Aalto universitetu, rengia švietimo priemonių paketą, kuriuo siekiama, kad kibernetinis saugumas taptų pilietiniu įgūdžiu visoje Europos Sąjungoje. Šia iniciatyva pabrėžiama didėjanti kibernetinio saugumo svarba kasdieniame gyvenime ir visų piliečių, įskaitant moteris, informuotumo ir įgūdžių poreikis. Joje pabrėžiamas švietimo įstaigų vaidmuo teikiant prieinamą kibernetinio saugumo švietimą ir mokymą, kuris yra labai svarbus siekiant suteikti moterims daugiau galimybių šioje srityje. Suomija skatina kibernetinio saugumo įgūdžių ugdymą ES.[22]

„Mimmit koodaa“ (Women Code) judėjimas

Įgyvendinant iniciatyvą „Mimmit koodaa“ siūlomi seminarai, mokymai, tinklų kūrimo galimybės, internetiniai seminarai ir karjeros parama. Daugiausia dėmesio skiriama stereotipams paneigti ir paskatinti daugiau moterų rinktis karjerą technologijų srityje, įskaitant kibernetinio saugumo sritį. Ši organizacija siekia sudaryti sąlygas moterims patekti į kibernetinio saugumo sritį ir joje tobulėti.[23]

[21] Women4Cyber Finland
[22] Digital Skills and Jobs Platform
[23] Mimmit koodaa

Remiantis „Agoria“ 2022 m. paskelbtu pirmuoju socialiniu ir ekonominiu tyrimu apie kibernetinio saugumo sektorių Belgijoje, moterys sudaro 19 % visų darbuotojų. Koordinuojant Belgijos ekonomikos ministerijai (FPS Belgium), kompetentingi Belgijos politikos dalyviai parengė penkerių metų moterų skaitmeninėje srityje planą, pavadintą „Moterys skaitmeninėje srityje – nacionalinė ir tarpsektorinė 2021-2026 m. strategija“.

Į penkerių metų planą įtraukta bendra ir tarpsektorinė strategija, grindžiama penkiais strateginiais tikslais, naudingais kovojant su prietarais ir šalinant struktūrines kliūtis, trukdančias moterims dalyvauti skaitmeninėje ekonomikoje:

1. Užtikrinti, kad daugiau moterų baigtų studijas skaitmeniniame sektoriuje;
2. Skatinti visas moteris dalyvauti skaitmeninėje darbo rinkoje ir (arba) skaitmeniniame sektoriuje;
3. Gerinti moterų išlaikymą skaitmeniniame sektoriuje;
4. Kurti naujus įvaizdžius, skatinančius moterų vaidmenį šioje srityje (ekrane ir už jo ribų);
5. Mažinti lyčių atotrūkį tarp konkrečių tikslinių grupių.[24]

Briuselyje įsikūręs „Women4Cyber“ fondas organizuoja ir remia įvairią veiklą, skirtą moterims, dirbančioms ar pradedančioms karjerą kibernetinio saugumo srityje Belgijoje ir Europoje. Belgijoje „Women4Cyber“ fondas remia Belgijos nacionalinį skyrių (Women4Cyber Belgium) ir bendradarbiauja su juo vykdant šias veiklas. Belgijos nacionaliniame skyriuje yra apie 20 aktyvių narių, dirbančių su šiomis iniciatyvomis. Skyriaus organizuojama veikla, renginiai ir programos, pavyzdžiui, „Women4Cyber“ narių tinklo susitikimai ir renginiai (virtualūs ir kontaktiniai), pavyzdžiui, „virtuali kava“, į kuriuos „Women4Cyber“ Belgijos skyrius kviečia įvairių su kibernetiniu ir informaciniu saugumu susijusių sričių ekspertus; internetiniai seminarai ir informacinės sesijos; mentorystės programos, kuriomis siekiama padėti moterims tobulinti įgūdžius ir siekti karjeros kibernetinio saugumo srityje visais lygmenimis; projektai ir renginiai bendradarbiaujant su Belgijos kibernetinio saugumo koalicija (pavyzdžiui, International Women’s Day 2023); stipendijų, skirtų su kibernetiniu saugumu susijusioms švietimo programoms, pavyzdžiui, Solvay Briuselio ekonomikos ir vadybos mokyklos organizuojamoms programoms, skatinimas.

Norvegijoje, siekiant sukurti atsparią ir įvairią darbo jėgą labai svarbu spręsti lyčių atotrūkio kibernetinio saugumo srityje problemą. Moterų dalis IT srityje sudaro tik 29 %. Šis mažas skaičius labai susijęs su tuo, kiek moterų vidurinėje mokykloje renkasi matematikos ir technikos dalykus.

Mokymo ir palaikymo poreikiai bei rekomendacijos moterų įtraukimui

Siekiant spręsti moterų įtraukimo į kibernetinio saugumo sritį klausimą, reikia specialiai pritaikytų kibernetinio saugumo programų, kurios būtų skirtos skatinti moterų didesnį įsitraukimą. Šiose programose techniniai aspektai turėtų būti suderinti su organizaciniais ir žmogiškaisiais kibernetinio saugumo klausimais. Šioje srityje yra kelios techninės kvalifikacijos kėlimo programos, tuo tarpu tipiškiausių moterų profesijų (pedagoginių – sveikatos priežiūros profesijų) kvalifikacijos kėlimo programų nėra, todėl trumpesnių su šiomis profesijomis susijusių kibernetinio saugumo mokymo programų parengimas galėtų pasiekti daugiau moterų. Tam

[24] https://www.bedigitaltogether.be/wp-content/uploads/2022/03/52786_9_WiD-Strategy-EN-2021.pdf

pritaria ir šio sektoriaus atstovai, kurie teigė, kad įvairovė gali suteikti unikalių požiūrių į kibernetinio saugumo iššūkius. Didinti moterų informuotumą apie kibernetinio saugumo vidaus karjerą būtų galima organizuojant praktinius užsiėmimus (angl. workshops), seminarus ir tikslines informavimo programas mokyklose ir universitetuose, kurios galėtų įkvėpti daugiau moterų pradėti dirbti šioje srityje.

Kitas būdas, kurį siūlo daugelis iš 50 geriausių Norvegijos technologijų srities moterų 2022 m., – kurti mentorystės programas ir tinklų kūrimo galimybes kibernetinio saugumo srityje dirbančioms moterims, kad joms būtų suteiktos svarbios rekomendacijos ir palaikymas, padedantys lengviau integruotis ir tobulėti šioje srityje.

Pačiame kibernetinio saugumo sektoriuje siūloma, kad organizacijos įgyvendintų įtraukią įdarbinimo praktiką ir politiką, kurių pagalba aktyviai skatinamas moterų įdarbinimas ir išlaikymas kibernetinio saugumo srityje. 32 % moterų, atliekančių techninius vaidmenis, darbe dažnai būna „vienintelė moteris kambaryje“, teigiama „McKinsey“ ataskaitoje „Moterys darbo vietoje 2022“ (Women in the Workplace 2022 m.).

Galiausiai, skatinant moteris užimti vadovaujančias pozicijas kibernetinio saugumo srityje, jos gali tapti sektinu pavyzdžiu ir įkvėpti kitas moteris siekti panašių tikslų, pavyzdžiui, Mia Landsem**.**

Rumunijoje kibernetinis saugumas tebėra vienas dinamiškiausių ir įdomiausių technologijų sektorių. Tačiau šiame sektoriuje reikia sisteminių pokyčių, susijusių su moterų atstovavimu ir atlygiu joms. Nepaisant padidėjusio susidomėjimo kibernetinio saugumo sritimi, lyčių skirtumai išlieka. Moterims vis dar labai menkai atstovaujama, o daugumoje darbo vietų vyrauja vyrai. Kibernetinio saugumo ateičiai įtakos turi gebėjimas pritraukti, išlaikyti ir skatinti daugiau kibernetinio saugumo specialistų, įskaitant daugiau moterų.

Buvo atlikta daugybė tyrimų, siekiant parodyti, kaip menkai vertinamos moterys visame pasaulyje, taip pat siekiant, kad visi suprastų moterų svarbą visose srityse, ypač kibernetinio saugumo srityje. Itin dideli lyčių skirtumai tarp kibernetinio saugumo darbuotojų rodo, kad ir kitos veikiančios jėgos yra visiškai nelygiavertės. Moterys sudaro 39% visų darbo rinkos darbuotojų. Remiantis „Cyber Venture duomenimis“, 38% dirba STEM srityje, iš jų tik 25% kibernetinio saugumo srityje.

Identifikuojamos įvairios kliūtys, trukdančios moterims dirbti kibernetinio saugumo srityje. Atlikto tyrimo (ISC)2 duomenimis, ne pelno siekiančios organizacijos, kurios daugiausia dėmesio skiria kibernetinio saugumo mokymams ir sertifikavimui, dauguma šioje srityje dirbusių moterų nurodo diskriminaciją dėl lyties. Didžioji dalis moterų (87 %) nurodė patyrusios nesąmoningą diskriminaciją, o 19 % teigė patyrusios atvirą diskriminaciją. Moterys taip pat nurodė nepaaiškinamą uždelsimą siekti karjeros (53 %) ir perdėtą reagavimą į klaidas (29 %).

Diskriminacija taip pat pasireiškia kompensacijų skirtumais. (ISC)2 tyrimai rodo, kad 32 % kibernetinio saugumo srityje dirbančių vyrų uždirba vidutiniškai nuo 50 000 iki 100 000 JAV dolerių per metus, o tik 18 % kibernetinio saugumo srityje dirbančių moterų gauna tokias pat pajamas. O 25 % vyrų ir 20 % moterų uždirba nuo 100 000 iki 500 000 JAV dolerių per metus.

Yra svarių argumentų, kodėl reikia didinti moterų kibernetinio saugumo srityje skaičių, pavyzdžiui, įvairovės, naujovių, emocinės empatijos ir nešališko požiūrio, kurie yra vertingi ir naudingi įgūdžiai kibernetinio saugumo srityje.

„Women in Cybersecurity“ valdybos narys Jay Koehler pateikė dar vieną įžvalgą: „Moterys pasitraukia, nes tai yra „berniukų klubas“, o priklausymo jausmas yra menkas.“ Šią problemą galima spręsti įsipareigojant ir prisiimant atsakomybę už psichologinio saugumo užtikrinimą ir palankią darbo vietą lyčių požiūriu, taip pat kuriant moterų tinklus.

Yra vilties, kad kibernetinis saugumas nebebus „vyrų dominuojančia profesija“, o joje dirbs talentingi įvairių lyčių ir išsilavinimo žmonės.

Literatūros apie moterų įsitraukimą kibernetinio saugumo sritį Ispanijoje nėra daug. Dauguma esamos literatūros rodo ryškų lyčių disbalansą plačioje mokslo bendruomenėje, įskaitant STEM disciplinas, ir pastebimai mažėjantį moterų patekimą į aukštesnius karjeros etapus, paprastai vadinamą „nesandaraus vamzdžio reiškiniu“ (angl. pipeline phenomenon). Kalbant apie aukštąjį mokslą, lyčių atotrūkis vis dar ryškus – tik 18 % šių dalykų studijas baigusių asmenų yra moterys. Moterų, dirbančių MVĮ su mokslo tyrimais ir plėtra (I+D, isp. Investigación y Desarrollo) susijusiose pareigose, vis dar labai mažai – Nacionalinio statistikos instituto duomenimis, jų skaičius nesiekia net 30 %. Kalbant apie Ispanijos aukštųjų mokyklų kibernetinio saugumo srityje dirbančias moteris tyrėjas, labai nedaugelyje iš jų darbuotojai yra subalansuoti pagal lytį. Iš 31 aukštosios mokyklos, kurias peržiūrėjo Fundación Alternativas, 11-oje iš jų mokslinių tyrimų grupėse nedalyvauja nė viena moteris ir tik 5-iose iš jų darbo jėga yra labiau egalitarinė (demonstruoja lygesnę darbo jėgą).

Reaguojant į šiuos iššūkius, mokymo ir paramos poreikių analizėje nustatytos pagrindinės tobulintinos sritys.

- Turėtų būti parengtos iniciatyvos, skatinančios daugiau moterų studijuoti doktorantūroje ir užtikrinančios tolygų atstovavimą visoje švietimo sistemoje.
- Itin svarbu spręsti karjeros šališkumo problemą, o mentorystės programos gali atlikti esminį vaidmenį padedant moterims susidoroti su kibernetinio saugumo srities iššūkiais.
- Be to, rekomenduojama bendradarbiauti su privačiomis pramonės organizacijomis, siekiant ištirti karjeros kelius ir skatinti moterų dalyvavimą kibernetinio saugumo srityje privačiose pramonės šakose.
- Įvertinus kvalifikaciją ir kompetencijas, pabrėžiama svarba pritaikytų mokymo programų, kuriose akcentuojami konkretūs kibernetinio saugumo įgūdžiai ir kompetencijos.

2.3. ESCO PROFESIJŲ ANALIZĖ

Esamą ESCO (Europos įgūdžių (gebėjimų), kvalifikacijų ir profesijų klasifikatorius) klasifikaciją aiškiname pagal nustatytus mokymosi rezultatus, įskaitant žinias, įgūdžius ir kompetencijas.

Šios analizės tikslas yra:

- išanalizuoti esamas ESCO profesijas, susijusias su kibernetiniu saugumu;
- nustatytus mokymosi rezultatus susieti su ESCO profesijomis pagal žinias, įgūdžius, kompetencijas ir kt.

Kiekvienai profesijai nustatytas kompetencijų, įgūdžių ir žinių rinkinys. Toliau pateikiami kompetencijų, įgūdžių, žinių apibrėžimai ir pavyzdžiai.

Kompetencija reiškia asmens gebėjimą efektyviai atlikti konkrečią užduotį ar darbą. Ji apima žinių, įgūdžių ir elgsenos derinį, taikomą siekiant pagerinti veiklos rezultatus. Pavyzdys: projektų valdymo kompetencija – tai organizacinių įgūdžių, projektų valdymo procesų išmanymo ir gebėjimo veiksmingai bendrauti su komandos nariais derinys.

Įgūdžiai – tai specifiniai gebėjimai ar įgūdžiai (įgyjami praktikos, mokymų ar patirties būdu), leidžiantys asmeniui atlikti užduotis. Pavyzdys: įsiskverbimo testavimo įgūdžiai, gebėjimas naudotis kibernetinio saugumo priemonėmis ir programine įranga, programavimo įgūdžiai, gebėjimas analizuoti grėsmes ir reaguoti į jas realiuoju laiku.

Žinios – tai faktai, informacija ir supratimas, įgyti per išsilavinimą ar patirtį. Jos apima teorinį faktų ir principų, susijusių su tam tikra sritimi, supratimą. Pavyzdys: išmanymas, kaip vykdomos įvairių tipų kibernetinės atakos (pvz., „phishing“, išpirkos reikalaujančios programos, DDoS atakos), arba įvairių šifravimo metodų išmanymas ir susipažinimas su naujausiomis kibernetinio saugumo tendencijomis ir pokyčiais.

Ši analizė skirstoma į 2 etapus.

1 etapas: ESCO profesijų peržiūra ir atranka

ESCO portale buvo atliekama analizė, siekiant atskirti su kibernetiniu saugumu susijusias profesijas ir kitame skirsnyje dokumentuoti kiekvieną profesiją, ypatingą dėmesį skiriant išvardytiems įgūdžiams, kompetencijoms, žinioms.

ESCO profesijos pavadinimas	Žinios	Įgūdžiai	Kompetencijos
3512.3 – IRT saugumo technikas	• IRT tinklų kūrimas • įrangos atakų vektoriai • kovos su kibernetinėmis atakomis priemonės • operacinių sistemų IRT viešieji pirkimai • tinklo įranga • žiniatinklio programa • grėsmės saugumui	• kritiškai spręsti problemas • analizuoti IRT sistemą • užtikrinti tinkamą dokumentų valdymą • atlikti programinės įrangos testavimus ir nustatyti IRT sistemos trūkumus	• integruoti sistemos komponentus • teikti techninę dokumentaciją • spręsti IRT sistemos problemas • naudoti prieigos kontrolės programinę įrangą

2529.1 – vyriausiasis IRT saugumo pareigūnas – apima asmenis, atliekančius įmonės saugumo funkcijas	• IRT tinklo saugumo rizika • IRT saugumo teisės aktai • IRT saugumo standartai • atakos vektoriai • audito metodai • kovos su kibernetinėmis atakomis priemonės • kibernetinis saugumas • duomenų apsauga • sprendimų palaikymo sistemos (angl. decison support system) • informacijos konfidencialumas • informacijos saugumo strategija • vidaus rizikos valdymo politika • organizacinis atsparumas	• mokyti apie duomenų konfidencialumą • užtikrinti, kad būtų laikomasi organizacijos IRT standartų • užtikrinti atitiktį teisiniams reikalavimams • užtikrinti tarpžinybinį bendradarbiavimą • užtikrinti informacijos privatumą • nustatyti IRT saugumo riziką • įgyvendinti IRT rizikos valdymą • įgyvendinti IRT saugos politiką • įgyvendinti įmonių valdymą	• vadovauti atkūrimo po incidento pratyboms • vykdyti veiklos tęstinumo planą • valdyti IT saugumo reikalavimus • valdyti atkūrimo po incidento planus • stebėti pokyčius kompetencijos srityje • stebėti technologijų tendencijas • naudotis sprendimų palaikymo sistema (angl. decison support system)
2529.2 – skaitmeninės kriminalistikos ekspertas – iš kompiuterių ir kitų tipų duomenų laikmenų išgauna ir analizuoja informaciją; tiria skaitmenines laikmenas, kurios galėjo būti užmaskuotos/paslėptos, užšifruotos ar pažeistos, teismo ekspertizės būdu, siekdamas nustatyti, išsaugoti, atkurti, analizuoti ir pateikti faktus bei nuomones apie skaitmeninę informaciją	• IRT tinklo saugumo rizika • IRT saugumo standartai • kompiuterinė kriminalistika • kovos su kibernetinėmis atakomis priemonės • informacijos konfidencialumas • įsiskverbimo testavimo įrankis • užklausų kalbos • išteklių aprašymo sistemos užklausų kalba	• taikyti atvirkštinę inžineriją • parengti informacijos saugumo strategiją • mokyti apie duomenų konfidencialumą • rinkti duomenis teismo ekspertizės tikslais • nustatyti IRT saugumo riziką • nustatyti IRT sistemos trūkumus • įdiegti IRT tinklo diagnostikos priemones • teikti IRT konsultacijas • apsaugoti jautrią klientų informaciją • naudoti scenarijų programavimą • naudoti programinę įrangą duomenų apsaugai • atlikti IRT saugumo testavimą	• valdyti IT saugumo reikalavimus • tvarkyti duomenis teisiniais klausimais • atlikti skaitmeninių prietaisų kriminalistinę ekspertizę
2529.3 – įterptųjų sistemų saugumo inžinierius – įterptųjų sistemų saugumo inžinieriai daugiausia dėmesio skiria prijungtiems įrenginiams ir juos palaikantiems tinklams, o ne organizaciniam saugumui, kaip IRT saugumo inžinieriai	• IRT tinklo saugumo rizika • IRT saugumo standartai • daiktų internetas • kompiuterių programavimas • kovos su kibernetinėmis atakomis priemonės • įterptinės sistemos • informacijos saugumo strategija • programinės įrangos anomalijos	• analizuoti IRT sistemą • sukurti srauto diagramą • apibrėžti saugumo politiką • kurti IRT įrenginio tvarkyklę (angl. driver) • kurti programinės įrangos prototipą • atlikti programinės įrangos testus • nustatyti IRT saugumo riziką • nustatyti IRT sistemos trūkumus	• sekti naujausius informacinių sistemų sprendimus • valdyti IT saugumo atitikties reikalavimus • stebėti sistemos veikimą • atlikti rizikos analizę • pateikti testavimo rezultatus, naudojant programinės įrangos projektavimo šablonus • naudoti programinės įrangos bibliotekas • naudotis kompiuterizuotomis programinės įrangos inžinerijos priemonėmis

		• aiškinti techninius tekstus • teikti IRT konsultacijas • atlikti IRT saugumo testavimą • teikti techninę dokumentaciją	• apibrėžti techninius reikalavimus
2529.4 – etiškas įsilaužėlis – atlieka saugumo pažeidžiamumo vertinimą ir įsiskverbimo testus pagal pramonėje pripažintus metodus ir protokolus; analizuoja sistemas, ieškodamas galimų pažeidžiamumų, kurie gali atsirasti dėl netinkamos sistemos konfigūracijos, aparatinės ar programinės įrangos trūkumų arba veiklos trūkumų	• atakos vektoriai • kompiuterinė kriminalistika • kovos su kibernetinėmis atakomis priemonės • etika • teisiniai reikalavimai IRT produktams • įsiskverbimo testavimo įrankis • programinės įrangos anomalijos • įrankiai IRT testų automatizavimui • žiniatinklio programų saugumo grėsmės	• atlikti IRT saugumo testavimą • teikti techninę dokumentaciją • kurti kodo išnaudojimo būdus • atlikti IRT auditą • atlikti programinės įrangos testus • nustatyti IRT saugumo riziką • nustatyti IRT sistemos trūkumus	• kritiškai spręsti problemas • analizuoti organizacijos kontekstą • stebėti sistemos veikimą
2529.5 – IRT atsparumo vadybininkas - tiria, planuoja ir kuria modelius, politiką, metodus, būdus ir priemones, kuriomis didinamas organizacijos kibernetinis saugumas, atsparumas ir atkūrimas po nelaimių	• IRT atkūrimo metodai • kibernetinio saugumo užtikrinimas • rizikos valdymo politika • organizacinis atsparumas • geriausia sistemos atsarginių kopijų kūrimo praktika	• parengti nenumatytų atvejų planus ekstremalioms situacijoms • parengti informacijos saugumo strategiją • atlikti IRT auditą • nustatyti IRT saugumo riziką • įdiegti IRT atkūrimo sistemą • įgyvendinti IRT rizikos valdymą	• analizuoti verslo procesus • analizuoti organizacijos aplinką • laikytis teisinių reguliavimų • vadovauti avarijų (incidentų) padarinių likvidavimo pratyboms • valdyti IT saugumo atitikties reikalavimus • valdyti atkūrimo po nelaimės planus • valdyti sistemos saugumą • atlikti IRT saugumo testavimą
2529.6 – IRT saugumo administratorius – planuoja ir įgyvendina saugumo priemones, skirtas informacijai ir duomenims apsaugoti nuo neteisėtos prieigos, tyčinių išpuolių, vagysčių ir sugadinimo	• IRT tinklo saugumo rizika • daiktų internetas • kovos su kibernetinėmis atakomis priemonės • duomenų bazių kūrimo įrankiai • interneto valdymas • mobiliųjų įrenginių valdymas • operacinės sistemos • organizacinis atsparumas • kokybės užtikrinimo metodikos • geriausia sistemos atsarginių kopijų kūrimo praktika	• nustatyti IRT sistemos trūkumus • interpretuoti techninius tekstus • prižiūrėti IRT tapatybės valdymą • palaikyti duomenų bazės saugumą	• taikyti įmonės politiką • rūpintis IRT sistemų kokybe • užtikrinti tinkamą dokumentų valdymą • valdyti IRT duomenų architektūrą • valdyti IT saugumo reikalavimus • atlikti IRT trikčių šalinimą • spręsti IRT sistemos problemas
2529.7 – IRT saugumo inžinierius – pataria ir įgyvendina sprendimus, kaip kontroliuoti prieigą prie duomenų ir programų, užtikrina organizacijos misijos ir verslo procesų apsaugą	• IRT saugumo teisės aktai • IRT saugumo standartai • atakos vektoriai • verslo analizė • kovos su kibernetinėmis atakomis priemonės • kibernetinis saugumas • naujausios technologijos • informacijos architektūra • informacijos saugumo strategija • operacinės sistemos • organizacinis atsparumas	• parengti informacijos saugumo strategiją • mokyti apie duomenų konfidencialumą • užtikrinti informacijos saugumą • atlikti IRT auditą • atlikti programinės įrangos testus	• apibrėžti duomenų kokybės kriterijus • apibrėžti techninius reikalavimus • tvarkyti užduočių įrašus • sekti naujausius informacinių sistemų sprendimus • valdyti IT saugumo atitikties reikalavimus. • valdyti atkūrimo po nelaimės planus

	• rizikos valdymas • nestruktūrizuoti duomenis	• nustatyti IRT saugumo riziką • nustatyti IRT sistemos trūkumus • įgyvendinti IRT rizikos valdymą • teikti IRT konsultacijas • analizuoti IRT sistemą. • apibrėžti saugumo politiką	• stebėti sistemos veikimą • atlikti duomenų analizę • atlikti rizikos analizę • pranešti apie testavimų rezultatus šalinti trikdžius • tikrinti oficialias IRT specifikacijas
2529.8 – IRT saugumo vadybininkas – siūlo ir įgyvendina būtinus saugumo atnaujinimus; konsultuoja, palaiko, informuoja, rengia mokymus ir informuoja apie saugumą bei imasi tiesioginių veiksmų visame tinkle ar sistemoje arba jų dalyje	• IRT problemų valdymo metodai • IRT projektų valdymas • IRT kokybės politika • IRT saugumo standartai • IRT sistemos naudotojo reikalavimai • daiktų internetas • atakos vektoriai • kompiuterinė kriminalistika • informacijos saugumo strategija • vidaus rizikos valdymo politika • interneto valdymas • teisiniai reikalavimai IRT produktams	• apibrėžti saugumo politiką • parengti informacijos saugumo strategiją • parengti IRT saugumo prevencijos planą • įgyvendinti IRT rizikos valdymą	• vadovauti avarijų padarinių likvidavimo pratyboms • prižiūrėti IRT tapatybės valdymą • valdyti IT saugumo reikalavimus • valdyti atkūrimo po nelaimės (incidento) planus • spręsti IRT sistemos problemas
2529.9 – žinių inžinierius – integruoja susistemintas žinias kompiuterinėse sistemose (žinių bazėse), kad būtų galima spręsti sudėtingas problemas, kurioms spręsti paprastai reikia aukšto lygio žmogiškųjų žinių arba dirbtinio intelekto metodų	• verslo žvalgyba • verslo procesų modeliavimas • duomenų bazių kūrimo įrankiai • informacijos išgavimas • informacijos struktūra natūralios kalbos apdorojimas • dirbtinio intelekto principai • išteklių aprašymo sistemos užklausų kalba • sistemų kūrimo gyvavimo ciklas • sistemų teorija • užduočių algoritmavimas • žiniatinklio programavimas	• naudoti konkrečiai programai skirtą sąsają • naudoti duomenų bazes • naudoti ženklinimo (angl. markup) kalbas	• analizuoti verslo reikalavimus • taikyti IRT sistemų teoriją • įvertinti IRT žinias • kurti semantinius medžius • apibrėžti techninius reikalavimus • valdyti IRT semantinę integraciją • valdyti verslo žinias • valdyti duomenų bazę

2 etapas: ESCO profesijos ir mokymosi rezultatų nustatymas

Remdamiesi ankstesne lentele, išanalizavome dokumentuose nurodytas profesijas ir nustatėme su kiekvienu vaidmeniu susijusius mokymosi rezultatus. Naudodamiesi ESCO sistema, šiuos rezultatus suskirstėme į žinias, įgūdžius ir kompetencijas.

Mokymosi rezultatai – tai aiškus ir konkretus teiginys, apibūdinantis, ką besimokantysis turėtų išmokti ir gebėti atlikti pasibaigus mokymams. Šis teiginys apima žinias, įgūdžius ir nuostatas. ESCO profesijų klasifikatoriaus skirsnyje Informacijos ir ryšių technologijų specialistai yra suskirstyti į du poskyrius: Programinės įrangos ir taikomųjų programų kūrėjai ir analitikai bei Duomenų bazių ir tinklų specialistai. Pastarąjį sudaro keturios grupės: Duomenų bazių ir tinklų specialistai, Sistemų administratoriai, Kompiuterių tinklų specialistai ir Duomenų bazių ir tinklų specialistai, neklasifikuojami kitur. Visos lentelėje pateiktos kibernetinio saugumo profesijos buvo rastos šioje vienetų grupėje. Pavyzdžiui, šiai grupei priklauso informacinių ir ryšių technologijų saugumo specialistai.

Tokiais atvejais užduotys būtų šios.

(a) parengti planus, kaip apsaugoti kompiuterines bylas nuo atsitiktinio ar neleistino pakeitimo, sunaikinimo ar atskleidimo ir patenkinti skubius duomenų tvarkymo poreikius;
(b) naudotojų mokymas ir sąmoningumo apie saugumą skatinimas, siekiant užtikrinti sistemos saugumą ir pagerinti serverio bei tinklo efektyvumą;
(c) konsultuotis su naudotojais, kad būtų aptarti tokie klausimai, kaip prieigos prie kompiuterinių duomenų poreikiai, saugumo pažeidimai ir programavimo pakeitimai;
(d) stebėti dabartinius pranešimus apie kompiuterių virusus, kad būtų galima nustatyti, kada atnaujinti apsaugos nuo virusų sistemas;
(e) keisti kompiuterių saugumo failus, kad būtų įdiegta nauja programinė įranga, ištaisytos klaidos arba pakeistas asmens prieigos statusas;
(f) stebėti duomenų failų naudojimą ir reguliuoti prieigą, kad būtų apsaugota kompiuterių failuose esanti informacija;
(g) atlikti rizikos vertinimą ir duomenų tvarkymo sistemos testus, kad užtikrintų duomenų tvarkymo veiklos ir saugumo priemonių veikimą;
(h) šifruoti duomenų perdavimą ir statyti ugniasienes, kad būtų apsaugota perduodama konfidenciali informacija ir, kad nebūtų perduodama sugadinta skaitmeninė informacija.

Kiekvienos profesijos mokymosi rezultatų aprašymas:

Profesija	Mokymosi rezultatai
IRT saugumo technikas (3512.3)	• Pademonstruoti išsamų supratimą apie IRT tinklus, įrangos atakų vektorius, kibernetinių atakų atsakomąsias priemones ir operacines sistemas • kritiškai analizuoti ir nustatyti IRT sistemų pažeidžiamumą, kad būtų padidintas sistemos saugumas • įgyvendinti ir valdyti patikimas dokumentų valdymo strategijas, atitinkančias IRT saugumo protokolus • rengti ir vykdyti išsamius programinės įrangos testavimo planus, skirtus programinės įrangos pažeidžiamoms vietoms nustatyti ir ištaisyti • integruoti sistemos komponentus ir naudoti prieigos kontrolės programinę įrangą saugioms ir veiksmingoms IRT sistemoms kurti
Vyriausiasis IRT saugumo pareigūnas (2529.1)	• suprasti ir analizuoti IRT tinklo saugumo riziką, teisės aktus ir standartus, kad būtų apsaugota organizacijos informacija. • rengti ir įgyvendinti informacijos saugumo strategijas ir vidaus rizikos valdymo politiką • vadovauti atkūrimo po nelaimės pratyboms ir prižiūrėti veiklos tęstinumo planus • šviesti darbuotojus duomenų konfidencialumo klausimais ir užtikrinti bendradarbiavimą tarp padalinių, kad būtų sustiprinta saugumo praktika

Skaitmeninės kriminalistikos ekspertas (2529.2)	• analizuoti ir testuoti įterptųjų sistemų saugumą, ypač daiktų interneto (IoT) aplinkoje • kurti ir vykdyti programinės įrangos prototipus ir bandymus bei naudotis kompiuterinėmis programinės įrangos inžinerijos priemonėmis • valdyti IT saugumo reikalavimų laikymąsi, atlikti rizikos analizę ir sistemos veikimo stebėseną • apibrėžti ir įgyvendinti įterptinių sistemų saugumo politiką ir techninius reikalavimus
Įterptųjų sistemų saugumo inžinierius (2529.3)	• analizuoti ir testuoti įterptųjų sistemų saugumą, ypač daiktų interneto (IoT) aplinkoje • kurti ir vykdyti programinės įrangos prototipus ir bandymus bei naudotis kompiuterinėmis programinės įrangos inžinerijos priemonėmis • valdyti IT saugumo reikalavimus, atlikti rizikos analizę ir sistemos veikimo stebėseną • apibrėžti ir įgyvendinti įterptinių sistemų saugumo politiką ir techninius reikalavimus
Etiškas įsilaužėlis (2529.4)	• atlikti saugumo pažeidžiamumo vertinimą ir įsiskverbimo testavimą naudojant pramonėje pripažintus metodus • nustatyti ir išnaudoti galimas sistemų pažeidžiamumo vietas, kad būtų patobulintos saugumo priemonės • kurti kodo saugumo spragų išnaudojimo galimybes ir atlikti IRT auditą, kad užtikrinti sistemos vientisumą • analizuoti organizacijos kontekstą, kad būtų galima veiksmingai pritaikyti saugumo strategijas
IRT atsparumo vadybininkas (2529.5)	• rengti ir įgyvendinti nenumatytų atvejų planus ir informacijos saugumo strategijas ekstremaliųjų situacijų scenarijams • įdiegti ir valdyti IRT atkūrimo sistemas ir rizikos valdymo procesus • vadovauti avarinio atkūrimo pratyboms ir valdyti sistemos saugumą krizių metu • analizuoti verslo procesus, kad padidinti organizacijos atsparumą ir atitiktį teisinėms nuostatoms
IRT saugumo administratorius (2529.6)	• planuoti ir įgyvendinti saugumo priemones duomenims apsaugoti ir IRT tapatybės sistemoms valdyti • palaikyti duomenų bazės saugumą ir užtikrinti sistemos vientisumą bei atsparumą • spręsti IRT sistemos problemas ir atlikti trikdžių šalinimo bei kokybės užtikrinimo metodikas • tvarkyti duomenų architektūrą ir laikytis organizacinės duomenų apsaugos politikos

IRT saugumo inžinierius (2529.7)	• konsultuoti ir įgyvendinti sprendimus, kaip kontroliuoti prieigą prie duomenų ir apsaugoti verslo procesus • analizuoti IRT sistemas ir apibrėžti saugumo politiką bei duomenų kokybės kriterijus • atlikti duomenų analizę ir rizikos analizę, valdyti IT saugumo reikalavimus ir atkūrimo po nelaimės planus • nuolat atnaujinti informaciją apie naujas technologijas ir informacinių sistemų sprendimus
IRT saugumo vadybininkas (2529.8)	• siūlyti ir įgyvendinti saugumo atnaujinimus bei valdyti IRT saugumą įvairiuose projektuose • vadovauti avarijų padarinių likvidavimo pratyboms ir parengti IRT saugumo prevencijos planus • prižiūrėti ir valdyti IRT tapatybės valdymo sistemas ir spręsti sudėtingas sistemos problemas • kurti ir įgyvendinti informacijos saugumo strategijas ir valdyti atkūrimo po nelaimės planus
Žinių inžinierius (2529.9)	• Integruoti struktūrizuotas žinias į kompiuterines sistemas naudojant pažangias priemones, pavyzdžiui, RDF užklausų kalbą ir žiniatinklio programavimą • valdyti semantinės integracijos ir duomenų bazių sistemas, siekiant pagerinti verslo žinių valdymą • analizuoti verslo reikalavimus ir taikyti IRT sistemų teoriją, kad būtų sukurtos veiksmingos žinių bazės • sukurti semantinius medžius ir įvertinti IRT žinias, kad būtų galima spręsti sudėtingas problemas naudojant dirbtinio intelekto metodus

3. ANALIZĖ IR IŠVADOS

3.1. EMPIRINIO TYRIMO ANALIZĖ

Profesinio mokymo ir aukštojo mokslo institucijų apklausos analizė

Apklausoje „MVĮ kibernetinio saugumo pokyčių agentų poreikių nustatymas“ pateikiami įvairūs klausimai, skirti kibernetinio saugumo mokymui profesinio rengimo ir aukštojo mokslo institucijų kontekste. Rinkome duomenis apie kibernetinio saugumo mokymuose įtrauktas temas, mokymo metodus, lyčių įtrauktį ir respondentų demografinius duomenis.

Šio tyrimo tikslas – išanalizuoti respondentų atsakymus ir išsiaiškinti dabartinę kibernetinio saugumo mokymų padėtį, taikomas metodikas ir požiūrį į šios srities įtrauktį bei veiksmingumą.

Atsakymų analizė bus grindžiama tokia pagrindine struktūra:

- Demografiniai duomenys
- Mokymo programa, mokymo poreikiai ir mokymosi pageidavimai
- Kompetencijos reikalavimai ir būsimi įgūdžiai
- Su lytimi susijusios įžvalgos

Demografiniai duomenys:

Apklausos respondentų pasiskirstymas pagal lytį tarp profesinio mokymo įstaigų ir aukštųjų mokyklų yra toks:

Iš viso respondentų pagal institucijos tipą

Institucijos tipas	Atsakymai	Moteris	Vyras	Nenurodyta
Aukštojo mokslo institucijos	104	28	73	3
Profesinis rengimas ir mokymas	86	36	48	2
Iš viso	**190**	**64**	**121**	**5**

Nors tiek aukštojo mokslo, tiek profesinio mokymo įstaigose lyčių pusiausvyra yra nevienoda, profesinio mokymo įstaigose šis skirtumas yra mažesnis. Siekdami susidaryti aiškesnį vaizdą apie lyčių atstovavimą, palyginti su bendru kiekvienos institucijos atsakymų skaičiumi, ir pakoreguoti rezultatus, susijusius su atsakymų skaičiaus paklaida, apskaičiavome kiekvienos lyties procentinę dalį abiejų tipų institucijose.

Respondentų pasiskirstymas pagal institucijos tipą

Institucijos tipas	Moteris %	Vyras %	Nenurodyta %	Viso
Aukštojo mokslo institucijos	27	70	3	**100%**
Profesinis rengimas ir mokymas	42	56	2	**100%**

Analizė, pakoreguota atsižvelgiant į atsakymų paklaidą, patvirtina, kad nors abiejų tipų įstaigose yra daugiau vyrų respondentų, atotrūkis tarp vyrų ir moterų atstovavimo profesinio mokymo įstaigose išlieka mažesnis. Priežastys gali būti įvairios (pavyzdžiui, kultūriniai, struktūriniai ar politiniai veiksniai, darantys įtaką lyčių įvairovei kibernetinio saugumo švietimo srityje šių tipų institucijose). Didesnis moterų respondenčių procentas profesinio mokymo įstaigose rodo galimas sritis, kuriose reikėtų toliau tirti praktiką, padedančią palaikyti labiau lyčių įtrauktį skatinančią aplinką profesiniame mokyme, palyginti su aukštuoju mokslu.

Mokymo programa, mokymo poreikiai ir mokymosi pageidavimai

Temos, įtrauktos į aukštųjų mokyklų ir profesinio mokymo įstaigų rengiamus kibernetinio saugumo mokymus

Tema	Atsakymai	Aukštojo mokslo institucijos	Profesinis rengimas ir mokymas
Kibernetinio saugumo pagrindai	151	90	61
Tinklo saugumas	123	72	51
Grėsmių analizė ir valdymas	99	65	34
Kriptografija	92	57	35
Reagavimas į incidentus	82	49	33
Rizikos valdymas	77	43	34
Kibernetinio saugumo įstatymai ir politika	73	42	31
Pažangūs grėsmių mažinimo metodai	54	33	21

Tyrimo respondentai nurodo, kad pamatinės žinios ir įgūdžiai bei tinklo saugumas yra prioritetas. Grėsmių analizė ir valdymas, kriptografija ir reagavimas į incidentus rodo, kad mokymuose išsamiai aptariamos kibernetinio saugumo grėsmės. Rizikos valdymas ir kibernetinio saugumo įstatymai ir politika, nepaisant suvokiamą poreikį visapusiškai suprasti teisinį kontekstą ir veiksmingą rizikos valdymą, ne visada pasirenkamas. Įdomu pastebėti, kad į mokymus mažiau įtraukiama pažangių grėsmių mažinimo metodų.

Kad rezultatai būtų gauti be iškraipymo, kurį lemia respondentų iš kiekvieno tipo institucijų (aukštųjų mokyklų ir profesinio mokymo įstaigų) skaičius, duomenys buvo normalizuoti pagal bendrą kiekvieno tipo institucijų atsakymų skaičių. Šis metodas leidžia pamatyti, kokia dalis institucijų įtraukia kiekvieną temą į savo kibernetinio saugumo mokymo programas.

Temos	Aukštojo mokslo institucijų dalis	Profesinio rengimo mokymo dalis
Kibernetinio saugumo pagrindai	15.76%	15.48%
Tinklo saugumas	12.61%	12.94%
Grėsmių analizė ir valdymas	11.38%	8.63%
Kriptografija	9.98%	8.88%
Reagavimas į incidentus	8.58%	8.38%

Temos	Aukštojo mokslo institucijų dalis	Profesinio rengimo mokymo dalis
Rizikos valdymas	7.53%	8.63%
Kibernetinio saugumo įstatymai ir politika	7.36%	7.87%
Pažangūs grėsmių mažinimo metodai	5.78%	5.33%

Įdomu tai, kad yra panašių prioritetų su nedideliais skirtumais. Tiek aukštosios mokyklos, tiek profesinio mokymo įstaigos daug dėmesio skiria „Kibernetinio saugumo pagrindams“ ir „Tinklo saugumui“. Tai rodo, kad šios temos pripažįstamos kaip itin svarbūs kibernetinio saugumo mokymo komponentai. Proporcijos yra labai panašios: „Kibernetinio saugumo pagrindai“ šiek tiek labiau akcentuojami aukštosiose mokyklose, palyginti su profesinio mokymo įstaigomis, o „Tinklų saugumas“ pasižymi panašia tendencija, tačiau atotrūkis yra mažesnis.

Pastebimi ryškūs skirtumai, kai dėmesys skiriamas labiau specializuotoms temoms, pavyzdžiui, „Grėsmių analizė ir valdymas“, „Kriptografija“ ir „Pažangūs grėsmių mažinimo metodai“. Aukštosios mokyklos šioms temoms paprastai skiria šiek tiek didesnę mokymo programų dalį, palyginti su profesinio mokymo įstaigomis. Tai galima paaiškinti tuo, kad aukštosios mokyklos daugiausia dėmesio skiria išsamesniam, teoriškai pagrįstam kibernetinio saugumo supratimui, kuris dažnai apima platesnį specializuotų temų spektrą. Kita vertus, profesinio mokymo įstaigos, nors vis dar apimančios platų temų spektrą, gali teikti pirmenybę praktiniam taikymui ir tiesioginiam pasirengimui darbui.

Mokymo metodai

Mokymo metodai	Aukštojo mokslo institucijų dalis	Profesinio rengimo mokymo dalis
Atvejų tyrimai	60.91%	39.09%
Grupiniai projektai	58.95%	41.05%
Praktiniai darbai	59.02%	40.98%
Paskaitos	56.97%	43.03%
Apversta klasė	34.78%	65.22%
Virtualios simuliacijos	51.35%	48.65%

Atvejo analizės, grupiniai projektai, praktiniai darbai, paskaitų metodai plačiai taikomi abiejų tipų institucijose, tačiau pirmenybė teikiama aukštosiose mokyklose, o ne profesinio mokymo įstaigose. Kalbant apie apverstos klasės metodą, jis labiau paplitęs profesinio mokymo įstaigose (65,22 %) nei aukštosiose mokyklose (34,78 %), o tai rodo polinkį į interaktyvų mokymosi modelį profesiniame mokyme. Naudojant apverstos klasės metodą pirmenybė teikiama aktyviam mokymuisi ir studijuojančių įsitraukimui, o tai gerai dera su profesiniam mokymui būdingu praktiniu ir įgūdžiais grindžiamu metodu.

Mokymo metodų veiksmingumas

Mokymo metodai	Kiekis
Praktiniai užsiėmimai	141
Asmeniniai seminarai	134
Interaktyvios simuliacijos	104
Internetiniai kursai	100
Vaizdo pamokos	73
Nuotoliniai seminarai	68

Šioje apžvalgoje išryškėja pageidaujamų mokymo metodų įvairovė, tačiau aiškiai pabrėžiamas praktinis, interaktyvus ir lankstus mokymasis. Labai vertinami praktiniai užsiėmimai ir asmeniniai seminarai, nes jie suteikia interaktyvios ir praktinės mokymosi patirties. Interaktyvios simuliacijos ir internetiniai kursai taip pat buvo nemažai paminėti, o tai rodo prieinamų mokymosi būdų svarbą.

Iššūkiai, su kuriais susiduria mokymo institucijos

Paklausus apie pagrindinius iššūkius, su kuriais susiduria mokymo institucijos, toliau pateikiama dažniausiai pasikartojančių temų santrauka:

- **Dalyvių įgūdžių ir patirties įvairovė**: Dėstytojai susiduria su sunkumais dėl skirtingo dalyvių išsilavinimo ir patirties lygio. Sudėtinga mokymus pritaikyti visai grupei ir užtikrinti, kad užsiėmimai būtų naudingi tiek techniniams, tiek ne techniniams asmenims.
- **Kursų medžiagos atnaujinimas**: dėl sparčios kibernetinio saugumo grėsmių raidos reikia nuolat atnaujinti mokymo medžiagą ir mokymo metodus, kad būtų užtikrintas aktualumas.
- **Išteklių apribojimai**: dažnai instruktoriai susiduria su ribotais finansiniais ištekliais, kvalifikuoto personalo trūkumu, pasenusia mokomąja medžiaga ir nepakankama efektyviam mokymui reikalinga technine ir programine įranga.
- **Praktinio mokymo apribojimai**: yra didelis iššūkis suteikti praktinės patirties. Apribojimai – nepakankama laboratorijų įranga, realaus pasaulio modeliavimo galimybių trūkumas ir sunkumai kuriant tikroviškus kibernetinių atakų scenarijus praktikai.
- **Galimybė naudotis naujausiomis priemonėmis ir technologijomis**: suteikti studentams prieigą prie naujausių kibernetinio saugumo priemonių ir technologijų, kad jie galėtų mokytis praktiškai, dažnai būna sudėtinga, o tai labai svarbu praktiniam supratimui.
- **Pramonės ir švietimo derinimas**: suderinti poreikį mokyti teorinių pagrindų ir praktinių įgūdžių, atitinkančių pramonės poreikius, yra iššūkis. Taip pat būtina parengti studijuojančius darbo rinkai, kad jie įgytų tinkamų įgūdžių.
- **Mokymo programa ir švietimo struktūra**: reikia parengti išsamias, tarpdisciplinines mokymo programas, apimančias visus kibernetinio saugumo aspektus. Be to, kibernetinio saugumo įtraukimas į mokymo programas, ypač vidurinių mokyklų lygmeniu, tebėra didelis iššūkis.
- **Dėstytojų gebėjimai ir tobulėjimas**: Užtikrinti, kad instruktoriai turėtų naujausių žinių ir gebėtų veiksmingai perteikti sudėtingas sąvokas, yra labai svarbu, tačiau sudėtinga.
- **Studentų įsitraukimas ir motyvacija**: studijuojančių dėmesio išlaikymas ir motyvacija aktyviai dalyvauti mokymosi procese yra sudėtinga, ypač kai reikia perteikti sudėtingą ir kartais sausą techninį turinį.
  Kalbos ir lokalizavimo klausimai: kibernetinio saugumo ištekliai ne visada gali būti prieinami studentų gimtąja kalba, todėl mokymas ne angliškai kalbančiuose regionuose tampa dar sudėtingesnis.

Suderinimas su konkrečiais MVĮ poreikiais

Atsakymas	Kiekis
Neutralus	82
Suderinta	67
Šiek tiek nesuderinta	19
Labai suderinta	17
Nesuderinta	5

Dauguma atsakymų rodo neutralų požiūrį, o tai reiškia, kad šį aspektą galima tobulinti. Nemažai respondentų savo programas įvertino kaip suderintas, o labai nedaug instruktorių mano, kad jų programos yra labai suderintos arba nesuderintos su pramonės poreikiais. Atsakymai apatinėje skalės dalyje (nesuderinta ir šiek tiek nesuderinta) atspindi susirūpinimą arba iššūkius, susijusius su visišku švietimo turinio suderinimu su besikeičiančiu kibernetinio saugumo pobūdžiu pramonėje. Toks atsakymų pasiskirstymas rodo, kad iššūkis užtikrinti kibernetinio saugumo mokymą, pritaikytą prie pramonės tendencijų ir reikalavimų, tebėra aktualus. Jis pabrėžia projekto CyberAgent aktualumą, kuriuo siekiama užtikrinti nuolatinį mokymo programų atnaujinimą, partnerystę su pramonės atstovais ir praktinio mokymo galimybes, kad kibernetinio saugumo mokymo programos būtų geriau suderintos su kibernetinio saugumo pramonės poreikiais.

Konkrečios MVĮ skirtos temos

Tema / įgūdžiai	Kiekis
Kibernetinio saugumo pagrindai MVĮ	91
Duomenų apsauga ir privatumas MVĮ	75
Į programą neįtraukta jokia konkreti MVĮ tema ar įgūdžiai	64
Reagavimas į incidentus MVĮ	58
Rizikos vertinimas ir valdymas MVĮ kontekste	53
Kibernetinio saugumo politikos rengimas MVĮ	46

Didelis dėmesys skiriamas pagrindiniams kibernetinio saugumo principams ir duomenų apsaugai. Dažniausiai minimos temos „Kibernetinio saugumo pagrindai MVĮ“ ir „Duomenų apsauga ir privatumas MVĮ“ rodo, kad dėstytojai teikia pirmenybę tam, kad MVĮ įgytų žinių, kaip apsaugoti savo duomenis ir suprasti pagrindines kibernetinio saugumo sąvokas. „Į programą neįtraukta MVĮ skirta tema ar įgūdžiai“ tema rodo, kad kai kuriose kibernetinio saugumo mokymo programose esama spragų, susijusių su MVĮ pritaikytu turiniu. Tai rodo, kad itin svarbu tobulinti kibernetinio saugumo mokymus, ypač atsižvelgiant į iššūkius ir grėsmes, su kuriomis susiduria MVĮ.

MVĮ dažnai turi ribotus išteklius ir gali neturėti galimybės naudotis specializuotomis kibernetinio saugumo žiniomis, todėl yra ypač pažeidžiamos kibernetinių grėsmių. Tai, kad kibernetinio saugumo mokymo programose nėra MVĮ skirto turinio, rodo, kad šios programos gali nevisiškai tenkinti skirtingus MVĮ poreikius, todėl gali būti, kad jų pasirengimas ir atsparumas kibernetinėms atakoms yra nepakankamas. Norint pašalinti šią spragą, reikia integruoti temas ir įgūdžius, specialiai pritaikytus MVĮ kibernetinio saugumo poreikiams tenkinti, pavyzdžiui, mažesnių įmonių veiklai pritaikytą rizikos vertinimą, ekonomiškai efektyvią kibernetinio saugumo praktiką ir veiksmingos kibernetinio saugumo politikos rengimo ribotais ištekliais strategijas.

MVĮ darbuotojų įgūdžių trūkumas

Įgūdis/tema	Skaičius
Grėsmių aptikimas ir reagavimas	103
Debesijos saugumo patirtis	87
Reagavimas į incidentus ir atkūrimas	69
Duomenų privatumas ir apsauga	67
Rizikos valdymas ir analizė	63
Besivystančios technologijos	58
Tinklo saugumas	41
Atitikties ir reguliavimo žinios	36

Tyrimo respondentai nurodo, kad darbuotojai stokoja įgūdžių pagrindinėse srityse, iš kurių dažniausiai minima grėsmių aptikimo ir reagavimo į jas sritis. Tai rodo, kad svarbu rengti studentus atpažinti kibernetinio saugumo grėsmes ir į jas reaguoti, nes tai yra esminis šios srities įgūdžių elementas. Debesijos saugumo žinios užima antrą vietą, tai rodo, kad darbuotojai priklauso nuo debesijos technologijų ir, kad jiems reikia specializuotų žinių, kaip užtikrinti debesijos aplinkos saugumą. Taip pat vertinamas reagavimas į incidentus ir gebėjimas atstatyti, duomenų privatumas ir apsauga bei rizikos valdymas ir analizė. Manoma, kad atsižvelgiant į atsirandančias technologijas, poreikis nuolat sekti naujausius šios srities pažangos rezultatus nėra deficitinė sritis. Tas pats taikoma ir tinklo saugumui, kuris yra pamatinė sritis, įtraukta į daugumą kibernetinio saugumo mokymo programų. Tai rodo, kad mokymai šioje srityje yra veiksmingi.

Grėsmės

Tema	Skaičius
Dirbtinio intelekto valdomos kibernetinės atakos	117
Išpirkos reikalaujančių programų atakos	96
Sukčiavimas ir socialinė inžinerija	87
Debesijos saugumo pažeidimai	82
Daiktų interneto pažeidžiamumai	75
„Deepfake“ grėsmės	51
Vidinės grėsmės	25

Tyrimo respondentai nurodo, kad dažniausiai minima nauja kibernetinio saugumo grėsmė yra dirbtinio intelekto valdomos kibernetinės atakos, o tai rodo susirūpinimą dėl dirbtinio intelekto valdomų kibernetinių grėsmių sudėtingumo ir kompleksiškumo. Išpirkos reikalaujančios programinės įrangos atakos ir sukčiavimo bei socialinės inžinerijos atakos taip pat užėmė aukštą vietą, o tai rodo, kad šie atakų vektoriai yra aktualūs MVĮ. Debesijos saugumo pažeidimai ir daiktų interneto pažeidžiamumai rodo susirūpinimą, susijusį su debesijos paslaugų saugumu ir besiplečiančiu daiktų internetu, ir atspindi iššūkius, kylančius MVĮ saugant įvairias ir paskirstytas technologines ekosistemas. Giluminės klastotės (angl. Deepfake threats) ir vidinės grėsmės (angl. Insider threats) nelaikomos dideliais grėsmių vektoriais. Mokymo programos, apimančios 5 svarbiausias temas, gali geriau paruošti studentus ir MVĮ darbuotojus kovai su kylančiomis grėsmėmis.

Naujos tendencijos

Sritis	Skaičius
Dirbtinis intelektas ir mašininis mokymasis kibernetinėje saugoje	160
Skaitmeninė tapatybė ir privatumas	96
Etinis įsilaužimas ir gynybiniai įgūdžiai	82
Kvantinės kompiuterijos grėsmės	67
Decentralizuotos saugumo sistemos (pvz., blokų grandinė)	52
Dėmesys minkštiesiems įgūdžiams ir tarpdisciplininiam mokymui	47

Kibernetinio saugumo srityje daugiausia dėmesio skiriama dirbtiniam intelektui ir mašininiam mokymuisi, nes tai rodo šių technologijų svarbą stiprinant kibernetinio saugumo priemones ir šių sričių specialistų poreikį. Skaitmeninė tapatybė ir privatumas – dar vienas svarbus aspektas, pabrėžiantis skaitmeninės tapatybės apsaugos ir privatumo užtikrinimo svarbą. Etinio įsilaužimo ir gynybinių įgūdžių pakankamai aukšti balai rodo praktiškų, praktinių įgūdžių, kurie leistų specialistams nustatyti pažeidžiamumą ir veiksmingai apsisaugoti nuo atakų, poreikį. Kvantinės kompiuterijos grėsmės, decentralizuotos saugumo sistemos, pavyzdžiui, blokų grandinės technologija, ir minkštieji įgūdžiai bei tarpdisciplininis mokymas nebuvo laikomi naujomis tendencijomis. Atsakymų pasiskirstymas rodo kibernetinio saugumo srities įvairovę ir tai, kaip svarbu rengti specialistus, turinčius įvairių įgūdžių ir žinių, kad jie galėtų spręsti dabartinius ir būsimus iššūkius. Tačiau sąrašo viršuje yra dirbtinio intelekto tema.

Lyčių lygybė

Moterų procentinė dalis	Atsakymų skaičius
Mažiau nei 10%	57
10% - 25%	79
26% - 50%	43
51% - 75%	8
Daugiau nei 75%	3

Kibernetinio saugumo mokymo programose dalyvaujančių moterų procentinė dalis atskleidžia lyčių įvairovės skirtumus – daugumoje atsakymų nurodoma, kad moterų yra mažai. Išsamiau, 79 atsakymuose moterų dalyvavimas sudarė nuo 10 % iki 25 %, o 57 atsakymuose nurodyta, kad jis yra mažesnis nei 10 %. Kai kuriose programose siūlomas vidutinis lyčių įvairovės lygis – 43 respondentai įvertino, kad moterų dalyvavimo lygis yra nuo 26 % iki 50 %. Tačiau programos, kuriose dalyvauja daug moterų, yra ypač retos – tai rodo vos 8 respondentai, nurodę nuo 51 % iki 75 %, ir minimalus skaičius – 3 respondentai, įvertinę daugiau nei 75 %. Šie duomenys pabrėžia, kad kibernetinio saugumo mokymo programose sunku pasiekti lyčių įvairovę, išryškindami didelį moterų dalyvavimo atotrūkį daugumoje pateiktų programų.

Lyčių lygybės iniciatyvos

Atsakymas	Atsakymų skaičius
Taip	30
Ne	160

Tyrimo respondentai nurodo, kad didžioji dauguma respondentų (iš viso 160) netaiko konkrečių iniciatyvų ar strategijų, skirtų skatinti moterų dalyvavimą kibernetinio saugumo mokymuose. Tik 30 respondentų patvirtino, kad tokios priemonės yra įgyvendinamos. Tai rodo, kad, nors yra tam tikras sąmoningumas ir pastangos didinti moterų dalyvavimą kibernetinio saugumo mokymuose pasitelkiant tikslines iniciatyvas, dauguma programų galbūt vis dar neteikia pirmenybės arba neįgyvendina konkrečių strategijų, skirtų lyčių įvairovei užtikrinti. Šis tikslinių iniciatyvų trūkumas gali lemti mažą moterų dalyvavimo procentą, kaip pažymėta atsakymuose į ankstesnį klausimą.

Įtraukiantys lyčių lygybę mokymai

Atsakymas	Atsakymų skaičius
Taip	47
Ne	44
Nežinau	72
Man neaktualu	27

Rezultatai rodo, kad respondentų nuomonės dėl į lyčių lygybę orientuotų kibernetinio saugumo mokymo modulių prieinamumo išsiskyrė. Didžiausia grupė, kurią sudarė 72 respondentai, išreiškė abejonių („Nežinau”), o tai rodo, kad nėra aiškaus sutarimo ar žinių apie į lyčių lygybę įtrauktos medžiagos buvimą. Beveik po lygiai pasiskirstė tie, kurie mano, kad yra pakankamai į lyčių lygybę orientuotų modulių (47 atsakymai), ir tie, kurie mano, kad jų nėra (44 atsakymai). Be to, 27 respondentai manė, kad klausimas nėra susijęs su jų patirtimi ar kontekstu.

Šis pasiskirstymas atspindi vykstančias diskusijas ir skirtingą požiūrį į kibernetinio saugumo mokymo turinio įtraukimą. Didelis neaiškios nuomonės atsakymų skaičius rodo, kad kibernetinio saugumo švietimo ir mokymo ekosistemoje galimai trūksta informuotumo apie lyčių aspektą įtraukiančius mokymo išteklius arba jų prieinamumo.

Kliūtys lyčių įtraukčiai

Kliūtis	Skaičius
Stereotipai arba kultūrinės normos	107
Nepakankamas informuotumas apie kibernetinio saugumo galimybes	86
Mentorystės ar sektinų pavyzdžių trūkumas	74
Darbo ir asmeninio gyvenimo pusiausvyros iššūkiai	60
Suvokiamas lyčių šališkumas pramonėje	58

Didžiausios kliūtys, trukdančios moterims dalyvauti kibernetinio saugumo srityje, apklausos dalyvių nuomone, yra stereotipai arba kultūrinės normos (107 paminėjimai) ir nepakankamas informavimas apie galimybes kibernetinio saugumo srityje (86 paminėjimai). Šios dvi priežastys rodo, kad visuomenės suvokimas ir nepakankama informacija apie karjeros galimybes labai trukdo moterims patekti į kibernetinio saugumo sritį. Mentorystės ar sektinų pavyzdžių trūkumas ir darbo, ir asmeninio gyvenimo derinimo problemos taip pat yra esminės kliūtys, pabrėžiančios palaikymo tinklų ir lanksčios darbo aplinkos svarbą skatinant moterų dalyvavimą. Be to, pastebimas lyčių šališkumas šioje srityje rodo, kad reikia kultūrinių ir sisteminių pokyčių šioje srityje, kad ji taptų palankesnė ir teisingesnė moterims.

Speciali įvairovės ir įtraukties skatinimo programa

Atsakymas	Atsakymų skaičius
Taip	44
Ne	85
Nežinau	61

Tyrimo respondentai nurodo, kad nemaža dalis apklaustų institucijų (85 atsakymai) neturi konkrečios politikos ar programų, skirtų moterų įvairovei ir įtraukčiai kibernetinio saugumo mokymuose skatinti. Tuo tarpu 44 respondentai nurodė, kad jų institucijos įgyvendina tokias iniciatyvas, taip pabrėžiant požiūrį į lyčių įvairovės šioje srityje sprendimą. Tačiau nemažai respondentų, 61, nėra tikri, ar jų institucijos turi tokią politiką ar programas, o tai rodo, kad galimai trūksta komunikacijos ar informuotumo apie esamas įvairovės ir įtraukties pastangas. Be to, šie nevienareikšmiai atsakymai rodo, kad nors kai kurios institucijos imasi veiksmų, siekdamos įtraukti į kibernetinio saugumo mokymus, vis dar išlieka didelis atotrūkis tiek įgyvendinant įvairovės programas, tiek informuojant dėstytojus, darbuotojus ir studentus apie tokias iniciatyvas.

Pasiūlymai dėl patobulinimų

Pasiūlymas	Skaičius
Didesnis sėkmingų kibernetinio saugumo specialistų moterų matomumas	95
Daugiau moterų kibernetinio saugumo instruktorių ar mokymo personalo	89
Siūlyti stipendijas arba paskatas	81
Mentorystės galimybės	49
Mokymo turinys, kuriame išvengiama lyčių šališkumo	33
Reguliariai atnaujinama politiką, kad palaikyti įtrauktį	31
Į lyčių aspektą įtraukiantys atvejo tyrimai ir scenarijai	24
Pritaikytos mokymo programos	21
Daugiau tik moterims skirtų mokymų	18

Išanalizavus atsakymus, susijusius su pasiūlymais, kaip kibernetinio saugumo mokymą padaryti labiau įtraukiantį lyčių aspektą, paaiškėjo, kad vieningai sutariama dėl kelių pagrindinių strategijų svarbos. Daugiausia pritarimo sulaukęs pasiūlymas, paminėtas 95 kartus, yra didesnis sėkmingų kibernetinio saugumo specialisčių moterų pastebimumas. Tai pabrėžia, kad vaidmenų modeliai ir sektinos asmenybės atlieka itin svarbų vaidmenį įkvepiant moteris siekti karjeros kibernetinio saugumo srityje. Nuo jų nedaug atsilieka (89 paminėjimai) raginimas, kad kibernetinio saugumo dėstytojų ar mokymų darbuotojų moterų būtų daugiau, taip pabrėžiant atstovavimo švietimo darbuotojams poreikį. Stipendijų ar paskatų siūlymas (81 paminėjimas) įvardijamas kaip labai svarbus, kad ši sritis taptų finansiškai prieinamesnė ir patrauklesnė moterims. Mentorystės galimybės, kurias pažymėjo 49 respondentai, pabrėžia patyrusių šios srities specialistų patarimų ir paramos svarbą. Mokymų turinio, kuriame būtų išvengta lyčių šališkumo, poreikis ir reguliariai atnaujinama politika, kuria remiama įtrauktis, rodo, kad būtina koreguoti mokymo programas ir politiką, atspindinčią ir skatinančią įvairovę.

MVĮ tyrimo analizė

Demografiniai duomenys

Į apklausą atsakė visos partnerių šalys. Daugiausia respondentų yra Rumunijoje (28), po to – Norvegijoje (23), Lietuvoje, Ispanijoje ir Belgijoje - po 21 respondentą. Suomija ir Turkija taip pat turi nemažai atsakymų – po 20, nuo jų nedaug atsilieka Lenkija (19 respondentų).

Įmonės sektorius

Įmonės sektorius	Skaičius
IT	18
Švietimas	6
Statybos	4
Konsultavimas	4
Kibernetinis saugumas	4

Duomenys rodo, kad daug respondentų atstovauja IT sektoriui – 18 respondentų nurodė, kad jų įmonė veikia šiame sektoriuje. Švietimo, statybos, konsultavimo ir kibernetinio saugumo sektoriai taip pat turi nemažai atstovų (nuo 4 iki 6). Po pirmojo penketuko sektorių, kurių atstovų skaičius yra mažesnis, yra ilgas spektras, o tai rodo, kad apklausa apima įvairias pramonės šakas.

Respondentų profilis

Pareigos bendrovėje	**Skaičius**
Vadovas	48
Vykdomasis direktorius/savininkas	35
Techninis (inžinierius/programuotojas/analitikas)	27
Kita	25
Koordinatorius/administratorius	8
Pardavimai/rinkodara	8
Specialistas/ekspertas	8
Darbuotojas	8
Konsultantas	3
Švietimas/mokymas	2
Finansai/apskaita	1
Projektų valdymas	1
Žmogiškieji ištekliai	1
Iš viso	**175**

Įvairių profesijų atstovų auditorijoje yra daug įvairių pareigų pavadinimų, taip pat daug pareigybių, tokių kaip „darbuotojas“ ir „direktorius“, kurios rodo platų respondentų spektrą, apimantį įvairius organizacinės hierarchijos lygius. Kibernetinis saugumas yra tarpdisciplininis klausimas, kuris įtraukia įvairių vaidmenų ir pareigų įmonėse turinčius asmenis.

Lytis

Apklausos respondentų pasiskirstymas pagal lytį rodo, kad daugiau yra vyrų (102) nei moterų (69), o nedidelė dalis respondentų (4) pageidavo neatskleisti savo lyties. Toks pasiskirstymas rodo, kad apklausoje atstovaujamose srityje egzistuoja lyčių skirtumas, kuris atspindi platesnes tendencijas kibernetinio saugumo ir technologijų sektoriuose, kuriuose dažnai dominuoja vyrai. Vis dėlto didelis moterų respondenčių skaičius rodo reikšmingą moterų dalyvavimą šioje srityje, o tai rodo vykstančius pokyčius sektoriaus lyčių įvairovės srityje. Nors lyčių atotrūkis akivaizdus, atsakymų įvairovė taip pat rodo, kad kibernetinio saugumo sritis pamažu keičiasi.

Lyčių pasiskirstymas pagal šalis

Šalis	Moteris	Vyras	Nenori sakyti
Belgija	10	10	1
Suomija	9	11	0
Lietuva	9	12	0
Norvegija	8	15	0
Lenkija	8	9	2
Rumunija	12	16	0
Ispanija	6	14	1
Turkija	7	13	0

Lentelėje pateikiamas lyčių pasiskirstymas įvairiose šalyse. Visose šalyse respondentų vyrų yra daugiau nei moterų, o tai atitinka anksčiau aptartą bendrą lyčių pasiskirstymą. Tačiau šis skirtumas įvairiose šalyse skiriasi: kai kuriose šalyse, pavyzdžiui, Belgijoje, respondentų vyrų ir moterų skaičius yra vienodas (po 10), o Lenkijoje vyrų (9) ir moterų (8) pasiskirstymas yra glaudesnis, be to, nedidelis skaičius respondentų pageidavo nenurodyti savo lyties (2). Tokiose šalyse, kaip Rumunija ir Norvegija, bendras respondentų skaičius yra didesnis ir jose vyrų ir moterų santykis išlieka didesnis. Toks pasiskirstymas pagal lytį ir šalis leidžia geriau suprasti apklausos respondentų demografinę sudėtį, išryškindamas tiek lyčių skirtumus, tiek geografinę kibernetinio saugumo srities įvairovę.

Įmonės dydis

Įmonės dydis	Skaičius
Iki 10 darbuotojų	64
11-50	60
51-250	51

Apklausos atsakymai rodo, kad tarp dalyvių buvo daug mažų ir vidutinių įmonių. Didžiausią grupę sudaro įmonės, kuriose dirba iki 10 darbuotojų (64 respondentai), po jų seka įmonės, kuriose dirba nuo 11 iki 50 darbuotojų (60 respondentų), o po jų – įmonės, kuriose dirba nuo 51 iki 250 darbuotojų (51 respondentas).

Tai, kad tarp respondentų vyrauja mažesnės įmonės, rodo, jog svarbu, kad kibernetinio saugumo sprendimai būtų pritaikyti atsižvelgiant į konkrečius MVĮ poreikius ir apribojimus.

Žinių lygis

Kibernetinio saugumo žinių lygis	Skaičius
Vidutinis	85
Pradedantysis	64
Pažengęs	26

Iš apklausos atsakymų matyti, kad dauguma respondentų dabartinį savo darbuotojų kibernetinio saugumo žinių lygį vertina kaip „vidutinį“ (85), toliau seka respondentai, kurie mano, kad jų lygis yra „pradedančiųjų“ (64), o mažesnė dalis respondentų mano, kad jų darbuotojai turi „pažengusiųjų“ kibernetinio saugumo lygio žinių (26).

Toks pasiskirstymas rodo, kad atstovaujamose organizacijose yra didelis kibernetinio saugumo įgūdžių augimo ir tobulinimo potencialas. Dauguma „vidutinio“ ir „pradedančiojo“ lygio darbuotojų rodo, kad būtina vykdyti nuolatines mokymo ir švietimo iniciatyvas, siekiant pagerinti šių darbuotojų kibernetinio saugumo žinių bazę. Tai rodo galimybę rengti tikslines kibernetinio saugumo mokymo programas, pritaikytas skirtingiems žinių lygiams, užtikrinant, kad pradedantys darbuotojai gerai išmanytų pagrindinius kibernetinio saugumo principus.

Nors pažengusių darbuotojų yra mažiau, tačiau tai suteikia optimizmo, nes tai rodo, kad kai kuriose organizacijose egzistuoja pamatinis kibernetinio saugumo žinių lygis.

Žinių lygis pagal įmonės dydį.

Įmonės dydis	Pažengęs	Pradedantysis	Vidutinis
Iki 10 darbuotojų	6	25	33
11-50	10	20	30
51-250	10	19	22

Lentelėje nurodyta, kaip kibernetinio saugumo žinių lygiai (pažengęs, pradedantis, vidutinio lygio) pasiskirstę skirtingo dydžio įmonėse. Mažose įmonėse (iki 10 darbuotojų) kibernetinio saugumo žinių lygis yra linkęs į „vidutinio lygio“ lygį, po jo seka „pradedančiųjų“ lygis. Tai rodo, kad nors mažosios įmonės gali turėti tam tikrų kibernetinio saugumo žinių, vis dar nemaža dalis jų yra pradedančiųjų lygio, o tai rodo, kad yra kur tobulėti ir kad reikia daugiau pamatinių mokymų. Vidutinėse įmonėse (11-50 darbuotojų) žinios pasiskirsčiusios tolygiai, šiek tiek pirmenybė teikiama „vidutinio lygio“ žinioms. Tai gali atspindėti šiek tiek didesnių organizacijų labiau struktūruotą požiūrį į kibernetinio saugumo mokymą, tačiau taip pat rodo, kad yra ir pažengusiųjų, ir pagrindų mokymosi poreikių. Didesnės MVĮ (51-250 darbuotojų) laikosi panašaus dėsningumo kaip ir vidutinės įmonės: pažengusiųjų ir pradedančiųjų lygių atstovų skaičius yra vienodas, o vidutinio lygio žinių skaičius šiek tiek mažesnis.

Visose visų dydžių įmonėse labiausiai paplitęs „vidutinio“ kibernetinio saugumo žinių lygis.

Darbuotojai, atliekantys kibernetinio saugumo užduotis

Darbuotojų skaičius	Skaičius
1-5	88
0	22
6-10	17
21+	12
11-20	5

Kibernetinio saugumo srities darbuotojų diapazonas	Skaičius
0-4	113
5-9	17
10-14	13
20-24	4
25-50	6
+100	9

Lentelėse parodytas su kibernetiniu saugumu susijusį darbą dirbančių darbuotojų skaičiaus pasiskirstymas įvairiose organizacijose. Iš jų galima susidaryti aiškesnį vaizdą, kaip kibernetinio saugumo pareigos pasiskirsto skirtingose darbuotojų skaičiaus ribose. Didžioji dauguma atsakymų patenka į 0-4 intervalą, o tai rodo, kad daug organizacijų turi labai mažas kibernetinio saugumo komandas arba net neturi nė vienos specialiai kibernetiniam saugumui skirtos komandos. Pereinant į aukštesnius intervalus, dažnumas gerokai sumažėja, o šiek tiek padidėja organizacijų, turinčių daugiau nei 100 kibernetiniam saugumui skirtų darbuotojų, skaičius. Tai paaiškinama tuo, kad šiose įmonėse darbas kibernetinio saugumo srityje yra pagrindinis jų užsiėmimas.

Kalbant detaliau, duomenys rodo, kad kibernetinio saugumo komandų dydis yra labai įvairus: dažniausiai pasitaiko vienas darbuotojas, vėliau – nė vieno kibernetiniam saugumui skirto darbuotojo, o tai rodo, kad daugelis organizacijų minimaliai turi kibernetinio saugumo darbuotojų arba visai jų neturi. Pastebima, kad didėjant komandos dydžiui dažnumas mažėja.

Pasiskirstymas rodo galimą kibernetinio saugumo darbuotojų pasiskirstymo spragą, kai nemažai mažų ir vidutinių įmonių (MVĮ) negali turėti tinkamų kibernetiniam saugumui skirtų išteklių, todėl joms kyla didesnė rizika. Didesnių komandų buvimas kai kuriose organizacijose rodo, kad tam tikruose sektoriuose ar didesnėse įmonėse pripažįstama kibernetinio saugumo svarba.

Moterys kibernetinio saugumo srityje

Kibernetinio saugumo srityje dirbančių moterų skaičius	Skaičius
0	78
1-5	57
6-10	8
11-15	4
16-20	1

Klausimo „Kiek iš šių darbuotojų yra moterų?“ rezultatai rodo, kad kibernetinio saugumo darbuotojų skaičius MVĮ labai skiriasi nuo vyrų ir moterų skaičiaus. Labiausiai stebina tai, kad dauguma įmonių, iš viso 78, nurodė, kad kibernetinio saugumo srityje nedirba nė viena moteris. Tai rodo, kad apklaustose MVĮ vyrauja nepakankamo moterų atstovavimo šioje itin svarbioje srityje problema. Pastebėta, kad didėjant kibernetinio saugumo srityje dirbančių moterų skaičiui, jų skaičius palaipsniui mažėja: 31 įmonė turi vieną moterį tokiose pareigose. Kai kuriose įmonėse, kibernetinio saugumo srityje dirba 10 ar daugiau moterų, nors tai yra teigiamas reiškinys, tačiau tai yra greičiau išimtis nei įprasta taisyklė.

Šie atvejai gali būti susiję su organizacijomis, turinčiomis didesnes kibernetinio saugumo komandas, arba tomis, kurios ypatingą dėmesį skiria lyčių įvairovei kibernetinio saugumo darbuotojų tarpe. Tai rodo, kad reikia iniciatyvų, kuriomis siekiama skatinti ir remti moteris siekti karjeros kibernetinio saugumo srityje. Didelis skaičius įmonių, kuriose nėra nė vienos moters, užimančios kibernetinio saugumo pareigas, išryškina itin svarbią vietą, kurioje reikia imtis veiksmų, kad būtų skatinama lyčių įvairovė ir įtrauktis šiame sektoriuje. Šio lyčių atotrūkio mažinimas galėtų prisidėti prie įvairesnių perspektyvų sprendžiant kibernetinio saugumo iššūkius.

Naudojimasis išorės paslaugomis

Atsakymas	Skaičius
Ne	115
Taip	60

Atsakymai atskleidžia svarbų MVĮ požiūrio į kibernetinį saugumą aspektą. Dauguma apklaustų įmonių, 115 iš 175, nurodė, kad kibernetinio saugumo darbams nesamdo išorinių paslaugų teikėjų. Tai rodo, kad didelė MVĮ dalis pirmenybę teikia kibernetinio saugumo darbams arba būtinybę juos valdyti savo viduje. Šią tendenciją gali lemti įvairūs veiksniai, pavyzdžiui, biudžeto apribojimai, suvokiama kibernetinio saugumo praktikos kontrolė arba įsitikinimas, kad esamų vidaus išteklių pakanka kibernetinio saugumo poreikiams patenkinti. Esant tokiai situacijai, Cyberagent projektas tampa labai aktualus, siekiant suteikti darbuotojui pamatinių įgūdžių ir žinių.

60 įmonių nurodė, kad kibernetinio saugumo užduotims atlikti samdo išorės paslaugų teikėjus. Tikėtina, kad ši grupė suvokia užsakomųjų paslaugų privalumus, pavyzdžiui, galimybę naudotis specializuotais įgūdžiais, nuolat susipažinti su naujausiomis kibernetinio saugumo grėsmėmis ir kovos priemonėmis arba sustiprinti savo vidinius pajėgumus. Sprendimas samdyti išorės paslaugas taip pat gali atspindėti supratimą apie kibernetinio saugumo grėsmių sudėtingumą, kurį gali būti sudėtinga suvaldyti vien savo jėgomis, ypač MVĮ, turinčioms ribotus išteklius.

Šis pasiskirstymas rodo, kad MVĮ kibernetinio saugumo strategija skiriasi, balansuojant tarp kibernetinio saugumo funkcijų vidaus valdymo ir išorės užsakomųjų paslaugų. Tai pabrėžia individualaus požiūrio į kibernetinį saugumą svarbą, pripažįstant, kad skirtingų organizacijų poreikiai, pajėgumai ir ištekliai gali būti skirtingi, o tai daro įtaką jų sprendimams, ar kreiptis išorinės paramos kibernetinio saugumo užtikrinimui.

Mokymo programų veiksmingumas

Atsakymas	Skaičius
1 (Neefektyvi)	8
2	38
3	79
4	39
5 (Labai efektyvi)	11

Atsakymai leidžia suprasti, kaip dabartinės mokymo programos veiksmingai padeda studentams pasirengti realiems kibernetinio saugumo iššūkiams MVĮ. Dauguma respondentų – 79 – dabartinių mokymo programų veiksmingumą įvertino „3“, t. y. neutraliai arba vidutiniškai vertina jų veiksmingumą. Tai rodo, kad nors šiomis programomis pasitikima, tačiau yra ir nemažai galimybių jas tobulinti. Atsakymai taip pat rodo tendenciją artėti prie apatinės skalės dalies: „2“ įvertino 38 respondentai, o tai rodo skeptišką požiūrį į šių mokymo programų veiksmingumą. Kraštutiniuose atvejuose „1“ (neefektyvi) buvo pasirinkta mažiausiai (8 balai), o „5“ (labai efektyvi) - šiek tiek daugiau (11 balų). Tai rodo, kad labai nedaug respondentų mano, jog dabartinės mokymo programos yra visiškai neveiksmingos arba labai veiksmingos rengiant studentus kibernetinio saugumo iššūkiams MVĮ. Subalansuotas „4“ atsakymų skaičius (39 skaičiai) rodo, kad nemaža dalis dalyvių mano, jog mokymo programos yra gana veiksmingos, nors ir nepasižymi reikšmingais trūkumais. Nors dabartinės mokymo programos suteikia tam tikrą pasirengimą realiems kibernetinio saugumo iššūkiams MVĮ, tačiau yra atotrūkis tarp teikiamų mokymų ir pramonės poreikių. Šį atotrūkį gali lemti keletas veiksnių, pavyzdžiui, kibernetinio saugumo grėsmių raidos tempas, praktinis įgūdžių pritaikymas arba MVĮ kylančių iššūkių specifiškumas.

3 svarbiausios kibernetinio saugumo mokymo sritys

Kategorija	Skaičius
Grėsmių aptikimas ir reagavimas	102
Rizikos valdymas ir analizė	81
Reagavimas į incidentus ir atkūrimas	72
Duomenų privatumas ir apsauga	68
Debesijos saugumo patirtis	51
Tinklo saugumas	46
Atitikties ir reguliavimo žinios	31
Besivystančios technologijos	24

Tyrimo respondentai nurodo, kad „Grėsmių aptikimas ir reagavimas“ laikoma svarbiausia kibernetinio saugumo mokymo sritimi (102 atsakymai), o tai rodo tvirtą įsitikinimą dėl jos svarbos sprendžiant realius MVĮ kibernetinio saugumo iššūkius. Po šios srities seka „Rizikos valdymas ir analizė“ ir „Reagavimas į incidentus ir jų šalinimas“ (atitinkamai 81 ir 72 balai), pabrėžiant, kad labai svarbu suprasti riziką ir gebėti veiksmingai reaguoti į incidentus. „Duomenų privatumui ir apsaugai“ taip pat skiriama daug dėmesio – tai rodo didėjančią duomenų apsaugos įstatymų svarbą ir poreikį skaitmeniniame amžiuje apsaugoti asmeninę ir jautrią informaciją. „Debesijos saugumo kompetencija“ 51 respondentas įvardijo kaip pagrindinę sritį, greičiausiai dėl vis dažniau naudojamų debesijos paslaugų ir su jomis susijusių unikalių saugumo iššūkių. Tinklo saugumas – 46 respondentai nurodė, kad tai tebėra pagrindinis rūpestis, pabrėžiantis stiprios apsaugos nuo tinklo grėsmių poreikį. „Atitikties ir reguliavimo žinios“ ir „Naujos technologijos“ laikomos ne tokiomis svarbiomis.

Kompetencijos ir žinios

Kompetencijos ir žinių sritis	Esminis (%)	Didelis poreikis (%)	Vidutinis poreikis (%)	Mažas poreikis (%)	Nereikalingas (%)
Duomenų privatumas ir apsauga	38.29	38.29	13.14	10.29	0.00*
Rizikos vertinimas ir valdymas	34.86	36.00	24.00	4.57	0.57
Reagavimas į incidentus ir atkūrimas	33.14	38.86	19.43	8.00	0.57
Komunikacijos įgūdžiai	32.57	35.43	22.29	8.00	1.71
Techninės žinios	30.29	32.00	26.29	8.57	2.86
Grėsmių žvalgyba ir stebėjimas	29.71	37.14	24.00	8.57	0.57
Politikos kūrimas ir įgyvendinimas	24.00	37.14	24.00	12.57	2.29

* „Duomenų privatumo ir apsaugos“ procentinė dalis „Nereikalinga“ nėra duomenų, todėl tai gali būti susiję su tuo, kad visi respondentai mano, jog ši sritis yra bent šiek tiek reikalinga, todėl gali būti laikoma 0 %.

Lentelėje pateikiami vidutiniai kiekvienos kompetencijos ir žinių srities balai, gauti iš apklausos atsakymų, kuriais jų svarba įvertinta skalėje nuo 1 (nebūtina) iki 5 (būtina). Šie balai leidžia kiekybiškai įvertinti, kaip respondentai teikia pirmenybę skirtingoms šios srities sritims.

Šioje lentelėje pateikiama aiški informacija apie tai, kaip respondentai vertina kiekvieną kompetenciją ir žinių sritį. Tokios sritys kaip „Duomenų privatumas ir apsauga“ bei „Rizikos vertinimas ir valdymas“ turi didžiausią procentinę dalį „esminių“ vertinimų, o tai rodo jų svarbą šioje srityje. Priešingai, „Politikos formavimas ir įgyvendinimas“ pasižymi platesniu atsakymų pasiskirstymu, o tai rodo įvairesnį šios srities svarbos suvokimą. Rezultatai rodo, kad didelis dėmesys skiriamas techninėms žinioms, informuotumui apie grėsmes ir gebėjimui reaguoti į incidentus, taip pat labai svarbus efektyvaus bendravimo ir duomenų apsaugos praktikos poreikis.

Kylančios kibernetinio saugumo grėsmės

Kylanti kibernetinio saugumo grėsmė	Dažnumas
Sukčiavimas ir socialinė inžinerija	105
Dirbtinio intelekto valdomos kibernetinės atakos	95
Išpirkos reikalaujančių programų atakos	90
Debesijos saugumo pažeidimai	60
„Deepfake“ grėsmės	57
Daiktų interneto pažeidžiamumai	44
Grėsmės iš vidaus	31

Aktualiausiomis grėsmėmis laikomos sukčiavimas ir socialinė inžinerija, taip pat daug dėmesio skiriama dirbtinio intelekto valdomoms kibernetinėms atakoms ir išpirkos reikalaujančių programų atakoms. Tai rodo, kad MVĮ gerai supranta, jog reikia saugotis ir nuo tradicinių, ir nuo naujų kibernetinių grėsmių. Taip pat pabrėžiami debesijos saugumo pažeidimai ir „deepfake“ grėsmės, atspindinčios susirūpinimą dėl debesijos paslaugų saugumo ir galimo piktnaudžiavimo dirbtiniu intelektu. Daiktų interneto pažeidžiamumai ir grėsmės iš vidaus taip pat įvardijami, nors jie laikomi ne tokiais neišvengiamais kaip kitos kategorijos. Pažymėtina, kad yra atsakymų, kuriuose nurodoma, jog kai kurie respondentai nėra tikri dėl konkrečių grėsmių arba neturi idėjų savo verslo lygmeniu, o tai rodo, kad tarp kai kurių MVĮ gali būti žinių apie konkrečias kylančias grėsmes trūkumas arba susirūpinimas dėl jų.

Kibernetinio saugumo žinių ar įgūdžių trūkumas

Kibernetinio saugumo žinių ar įgūdžių trūkumas	Dažnumas
Žemas informuotumo apie grėsmes lygis	105
Žemas kibernetinio saugumo reguliarių mokymų lygis	88
Žemas pažeidžiamumo vertinimo lygis	80
Žemas techninių įgūdžių lygis	71
Žemas politikos ir reglamentų supratimo lygis	50
Žemas minkštųjų įgūdžių lygis	37

Didžiausios darbuotojų kibernetinio saugumo žinių ar įgūdžių spragos yra susijusios su grėsmių suvokimu, reguliariais kibernetinio saugumo mokymais, pažeidžiamumo vertinimu, techniniais įgūdžiais ir politikos bei taisyklių supratimu. Šių atsakymų dažnumas rodo, kad labai reikia visapusiško kibernetinio saugumo švietimo ir mokymo, kuris būtų skirtas šioms konkrečioms sritims. Žinojimas apie grėsmes išsiskiria kaip didžiausia spraga, rodanti, kad darbuotojai gali būti nevisiškai informuoti apie kibernetinio saugumo grėsmes, galinčias paveikti jų organizaciją. Ši spraga rodo, kaip svarbu tobulinti informuotumo didinimo programas ir mokymus, kad darbuotojai galėtų veiksmingiau atpažinti galimas grėsmes. Reguliarių kibernetinio saugumo mokymų trūkumas taip pat vertinamas kaip spraga, rodanti, kad reikia ne vienkartinių mokymų, o nuolatinio švietimo ir naujausios informacijos apie naujausią kibernetinio saugumo praktiką ir grėsmes atnaujinimo.

Naujos tendencijos

Naujos kibernetinio saugumo mokymo tendencijos	**Dažnumas**
Dirbtinis intelektas ir mašininis mokymasis kibernetinėje saugoje	134
Skaitmeninė tapatybė ir privatumas	108
Etinis įsilaužimas ir gynybiniai įgūdžiai	86
Dėmesys minkštiesiems įgūdžiams ir tarpdisciplininiam mokymui	54
Kvantinės kompiuterijos grėsmės	39
Decentralizuotos saugumo sistemos (pvz., blokų grandinė)	28

Tyrimo respondentai nurodo, kad labiausiai tikėtina ateinančių penkerių metų tendencija kibernetinio saugumo srityje yra dirbtinis intelektas ir mašininis mokymasis. Tai rodo, kad vis labiau pripažįstamas pažangiųjų technologijų vaidmuo stiprinant kibernetinio saugumo apsaugą ir kuriant naujus saugumo sprendimus. Didelis šios kategorijos atsakymų dažnumas rodo, kad į mokymo programas vis dažniau reikės įtraukti dirbtinio intelekto ir mašininio mokymosi komponentus, kad kibernetinio saugumo specialistai būtų parengti ateičiai. Skaitmeninė tapatybė ir privatumas iškyla kaip antra labiausiai prognozuojama tendencija, pabrėžianti susirūpinimą dėl asmens duomenų apsaugos ir skaitmeninės tapatybės valdymo vis labiau skaitmeniniame pasaulyje. Ši tendencija rodo mokymų, apimančių privatumo įstatymų, duomenų apsaugos metodų ir tapatybės valdymo sprendimų sudėtingumą, paklausą. Trečioji pagrindinė tendencija – etiškas įsilaužimas ir gynybiniai įgūdžiai, atspindinti aktyvios gynybos strategijų svarbą kibernetinio saugumo srityje. Etinio įsilaužimo akcentavimas rodo, kad pereinama prie mokymų, kurie leidžia kibernetinio saugumo specialistams mąstyti kaip įsilaužėliams, kad jie galėtų geriau apsaugoti savo organizacijas.

Mokymo programų tinkamumas

Atsakymas	Dažnumas
Taip	81
Nežinau	65
Ne	29

Analizuojant klausimą, kuriuo buvo tiriama respondentų nuomonė apie dabartinių kibernetinio saugumo mokymo programų tinkamumą, paaiškėjo, kad dalyvių požiūris yra nevienodas. Didžioji dalis respondentų mano, kad dabartinės kibernetinio saugumo mokymo programos yra tinkamos, kaip rodo atsakymai „Taip“. Tai rodo, kad nemažai asmenų mano, jog šiuo metu siūlomi mokymai atitinka jų organizacijų poreikius arba atitinka jų lūkesčius dėl to, ką turėtų apimti kibernetinio saugumo mokymai. Tačiau nemažai respondentų atsakė „Nežinau“ dėl dabartinių mokymo programų tinkamumo, o tai rodo tam tikrą neaiškumą arba informacijos apie esamas mokymo galimybes ar jų veiksmingumą sprendžiant dabartinius kibernetinio saugumo iššūkius trūkumą. Šį neapibrėžtumą galima paaiškinti kintančiu kibernetinių grėsmių pobūdžiu ir sunkumais, susijusiais su mokymo programų atnaujinimu atsižvelgiant į naujausius pokyčius šioje srityje. Atsakymai „Ne“, nors ir sudaro mažiausią grupę, rodo aiškų susirūpinimą, kad esamų mokymo programų nepakanka dabartiniams kibernetinio saugumo poreikiams patenkinti. Ši grupė gali įžvelgti spragas mokymo programose, apimančiose naujas grėsmes, technologijas ar metodikas.

Mokymo programų įtraukimas

Atsakymas	Dažnumas
Taip	81
Nežinau	65
Ne	29

Tyrimo respondentai nurodo rodo, kad dabartinių kibernetinio saugumo mokymo programų įtraukimo į lyčių lygybę aspektas yra įvairus. Dauguma respondentų mano, kad dabartiniai mokymai yra įtraukūs ir veiksmingai tenkina visų lyčių poreikius, kaip rodo atsakymai „Taip“. Tai rodo, kad nemaža dalis kibernetinio saugumo bendruomenės mano, jog dabartinės mokymo programos padeda siekti įtraukties ir lyčių lygybės. Tačiau nemažai respondentų atsakė „Nežinau“ dėl šių programų įtraukimo, o tai rodo, kad yra nemažai neaiškumų arba trūksta informacijos apie tai, ar kibernetinio saugumo mokymai įtraukia lyčių atstovus. Šis atsakymas gali rodyti mokymo paslaugų teikėjų ir dalyvių bendravimo spragą arba rodyti, kad įtraukties pastangos gali būti ne tokios pastebimos ar paveikios, kaip norėta. Atsakymai „Ne“, sudarantys mažiausią grupę tarp respondentų, vis dėlto išryškina esminį susirūpinimą, kad dabartiniai kibernetinio saugumo mokymai nepakankamai atsižvelgia į visų lyčių poreikius. Šie atsakymai rodo, kad kibernetinio saugumo mokymo programose esama įtraukties pastangų spragų, ir rodo, kad reikia daugiau dirbti siekiant užtikrinti, kad šios programos būtų draugiškos ir pritaikytos visų lyčių asmenų poreikiams.

3.2. MOKYMŲ PAGEIDAVIMAI IR POREIKIAI

Remdamiesi tyrimo rezultatais, pateikiame nustatytų savybių ir mokymo poreikių, mokymosi prioritetų, mokymosi pageidavimų aprašymą ir kibernetinio saugumo srityje dirbančių moterų mokymų ir palaikymo poreikį.

MOKYMO POREIKIŲ NUSTATYMAS:

1 sritis – Pagrindinės žinios ir įgūdžiai

Kibernetinio saugumo mokymo prioritetas. Ypač tokios temos, kaip kibernetinio saugumo pagrindai ir tinklo saugumas. Esama didelių spragų tokiose srityse, kaip grėsmių aptikimas ir reagavimas į jas, debesijos saugumo kompetencijos, reagavimas į incidentus ir atkūrimas, duomenų privatumas ir apsauga, rizikos valdymas ir analizė. Mokymo programose reikia spręsti šių įgūdžių trūkumo problemą. Be to, labai reikia į kibernetinį saugumą orientuoto MVĮ skirto turinio.

2 sritis – Specializuotos temos

Reikia mokymų, kurie apimtų platų kibernetinio saugumo grėsmių ir atsakomųjų priemonių spektrą. Buvo išskirtos kai kurios specialios temos, pavyzdžiui, grėsmių analizė ir valdymas, kriptografija ir pažangūs grėsmių mažinimo būdai. Į mokymus turėtų būti įtrauktas turinys apie dažniausiai įvardijamas kylančias grėsmes, įskaitant dirbtinio intelekto valdomas kibernetines atakas, išpirkos reikalaujančių programų atakas, sukčiavimą ir socialinę inžineriją, debesijos saugumo pažeidimus ir daiktų interneto pažeidžiamumą.

3 sritis – Praktinis taikymas

Pirmenybė teikiama tokiems mokymo metodams, kaip praktinės laboratorinės užduotys, atvejų analizės ir grupiniai projektai, pabrėžiant praktinio, interaktyvaus ir realaus taikymo svarbą kibernetinio saugumo mokymuose.

DABARTINĖ PATIRTIS:

Kalbant apie mokymo metodus, galima pastebėti, kad taikomi įvairūs metodai, tokie kaip atvejų analizė, grupiniai projektai, praktiniai laboratoriniai darbai ir paskaitos. Dabartinėse mokymo programose derinami teoriniai ir praktiniai metodai.

Dabartinės mokymo programos apima įvairias kibernetinio saugumo temas, pirmenybė teikiama fundamentaliems dalykams. Tačiau pastebima, kad kai kuriose programose trūksta MVĮ skirto turinio.

Kalbant apie įtrauktį ir lyčių pusiausvyrą, kai kuriose programose įgyvendinamos iniciatyvos, kuriomis siekiama padidinti moterų dalyvavimą ir sukurti į lyčių lygybę orientuotą mokymo aplinką, nors atrodo, kad tokių pastangų yra mažuma.

Iššūkiai:

Pagrindiniai iššūkiai, su kuriais susiduriama kibernetinio saugumo švietimo srityje, yra šie:

- Sudėtinga pritaikyti mokymą prie įvairios patirties ir žinių lygio, nes įgūdžiai ir patirtis yra skirtingi;
- Sudėtinga išlaikyti kursų medžiagą aktualią, kad ji atitiktų sparčią kibernetinio saugumo grėsmių raidą. Reikia nuolat atnaujinti mokymo medžiagą;
- Praktinio mokymo apribojimai dėl laboratorinių patalpų, realaus pasaulio modeliavimo galimybių ir tikroviškų kibernetinių atakų scenarijų kūrimo praktikai;
- Sudėtinga išlaikyti mokinių įsitraukimą ir motyvaciją, ypač mokantis sudėtingo techninio turinio;
- Rinkos ir mokymo suderinamumas su rinkos poreikį atitinkančių teorinių pagrindų ir praktinių įgūdžių derinimu kelia iššūkių.

Pasiūlymas dėl mokymo tobulinimo:

- Mokymo pritaikymas MVĮ poreikiams: integruoti temas ir įgūdžius, specialiai pritaikytus MVĮ kibernetinio saugumo poreikiams;
- Praktinio pritaikymo gerinimas, plačiau taikant praktinius, interaktyvius mokymo metodus, siekiant pagerinti praktinius įgūdžius ir pasirengimą realiam pasauliui;
- Įtraukti naujas tendencijas, pavyzdžiui, dirbtinio intelekto ir mašininio mokymosi, skaitmeninės tapatybės ir privatumo bei etiško įsilaužimo. Dabar jos laikomos pagrindinėmis sritimis, kurioms ateityje mokymo programose reikia skirti daugiausia dėmesio;
- Įgūdžių spragų šalinimas, sutelkiant dėmesį į sritis, kuriose darbuotojams trūksta įgūdžių, pavyzdžiui, grėsmių aptikimo ir reagavimo, debesijos saugumo ir reagavimo į incidentus, kad jie būtų geriau pasirengę įveikti iššūkius ir tapti veiksmingais ir atspariais kibernetiniais agentais;
- Plėtoti lyčių įvairovės iniciatyvas, siekiant didinti moterų dalyvavimą, pasitelkiant tikslines iniciatyvas, mentorystę ir sektinus pavyzdžius.

4. MVĮ KIBERNETINIO SAUGUMO POKYČIŲ AGENTO KVALIFIKACIJA

Remdamiesi dokumentų analine ir atliktų tyrimų rezultatais, pateikiame numatomų CyberAgent žinių, įgūdžių ir kompetencijų rinkinio pavyzdį. Šiuose rezultatuose suformuluoti tikėtini dalyvių pasiekimai atitinkamų kibernetinio saugumo mokymo programų pabaigoje, užtikrinant vystymąsi nuo pagrindinių žinių ir įgūdžių, atitinkančių Europos kvalifikacijų sistemą, EKS (EQF, European Qualifications Framework) 4-5 lygį, iki pažangesnių ir į vadovavimą orientuotų gebėjimų, atitinkančių EKS 6 lygį.

CyberAgent Kvalifikacijos profilis	**Žinios**	**Įgūdžiai**	**Kompetencijos**
4-5 EKS lygis	**Kibernetinio saugumo pagrindai** - Pagrindinės kibernetinio saugumo koncepcijos - Kibernetinių grėsmių tipai (sukčiavimas, išpirkos reikalaujanti programinė įranga, DDoS atakos), atakų vektoriai - Kibernetinio saugumo svarba saugant organizacijos turtą **Kibernetinio saugumo teisinė ir duomenų sistema** - Kibernetinio saugumo teisės aktai, standartai ir atitikties reikalavimai - Informacijos saugumo strategijos ir politika - Duomenų apsauga - Rizikos valdymo politika	**Saugumas** - Nustatyti galimą kibernetinio saugumo riziką ir pažeidžiamumą - Naudoti kibernetinio saugumo priemones ir programinę įrangą siekiant apsisaugoti nuo kibernetinių grėsmių - Skatinti praktiškai taikyti pagrindinius kibernetinio saugumo metodus, saugų slaptažodžių kūrimą, saugų naršymą, el. pašto saugumą ir saugų neskelbtinų duomenų tvarkymą	**Rizikos valdymas ir jos mažinimas** - Įvertinti ir sumažinti galimas saugumo grėsmes **Veiksmingas komunikavimas kibernetinio saugumo klausimais** - Gebėjimas veiksmingai bendrauti kibernetinio saugumo klausimais - Pranešti apie grėsmes ir pažeidimus atitinkamais organizacijos komunikacijos kanalais

6 EKS lygis	**Pažangios kibernetinio saugumo koncepcijos** - Suprasti pažangius kibernetinio saugumo principus, įskaitant sudėtingas kibernetines grėsmes ir atakų vektorius - Žinoti naujausias kibernetinio saugumo grėsmių ir gynybos mechanizmų tendencijas **Kibernetinio saugumo teisės aktai ir jų laikymasis** - Žinios apie nacionalinis ir tarptautinius kibernetinio saugumo teisės aktus, standartus, atitikties reikalavimus ir kitus su konkrečia pramonės šaka susijusius reikalavimus	**Pažangus rizikos vertinimas ir valdymas** - Gebėjimas atlikti išsamų rizikos vertinimas - Naudoti pažangias metodikas ir įrankius - Sukurti ir įgyvendinti veiksmingas rizikos valdymo strategijas nustatytai rizikai mažinti **Patirtis saugumo architektūros ir tinklo apsaugos srityje** - Projektuoti, diegti ir vertinti saugias tinklo architektūras, įskaitant ugniasienių, įsilaužimo aptikimo sistemų (IDS) ir įsilaužimo prevencijos sistemų (IPS) naudojimą **Reagavimas į incidentus ir atkūrimas po jų** - Gebėjimas pasirengti kibernetinio saugumo incidentams, reaguoti į juos ir atsigauti po jų - Parengti atkūrimo ir veiklos tęstinumo planus	**Planavimas ir politikos rengimas** - Gebėjimas kurti ir įgyvendinti strateginę kibernetinio saugumo politiką ir sistemas, suderintas su organizacijos tikslais ir atitikties įsipareigojimais **Vadovavimas kibernetinio saugumo iniciatyvoms** - Vadovavimas kibernetinio saugumo projektams ir komandos bei jų valdymas, įskaitant gebėjimą įkvėpti ir vadovauti darbuotojams įgyvendinant kibernetinio saugumo strategijas **Sprendimų priėmimas** - Priimti etiškus sprendimus, susijusiu su kibernetinio saugumo praktika

4-5 EKS lygyje, galimi mokymosi rezultatai galėtų būti tokie:

- Besimokantieji sužinos pagrindines kibernetinio saugumo sąvokas, įskaitant pagrindinius terminus, kibernetinių grėsmių tipus, pavyzdžiui, sukčiavimo, išpirkos reikalaujančios programinės įrangos ir DDoS atakas, ir šių atakų vektorius.
- Besimokantieji gebės nustatyti galimus kibernetinio saugumo pavojus ir pažeidžiamumus, naudotis atitinkamomis priemonėmis ir programine įranga šiems pavojams mažinti ir įgyvendinti pagrindines kibernetinio saugumo praktikas, tokias kaip saugus slaptažodžių kūrimas ir saugus naršymas.
- Besimokantieji įgis žinių apie kibernetinio saugumo teisės aktus, standartus ir atitikties reikalavimus, taip pat apie informacijos saugumo ir rizikos valdymo strategijas ir politiką organizacijoje.
- Besimokantieji įgis kompetenciją veiksmingai vertinti ir mažinti galimas saugumo grėsmes, aiškiai ir veiksmingai pranešti apie kibernetinio saugumo problemas organizacijoje, įskaitant pranešimus apie grėsmes ir pažeidimus atitinkamais kanalais.

6 EKS lygyje, galimi mokymosi rezultatai galėtų būti tokie:

- Besimokantieji įgis pažangų kibernetinio saugumo principų supratimą, įskaitant gebėjimą atpažinti sudėtingas kibernetines grėsmes ir atakų vektorius, taip pat bus informuoti apie naujausias kibernetinio saugumo tendencijas.
- Besimokantieji įgis išsamių žinių apie nacionalinius ir tarptautinius kibernetinio saugumo teisės aktus, standartus ir atitikties reikalavimus, pritaikydami šį supratimą prie konkrečių savo pramonės šakos poreikių.
- Besimokantieji gebės atlikti išsamų rizikos vertinimą, naudodami pažangias metodikas ir priemones, ir parengti veiksmingas rizikos valdymo strategijas šiai rizikai mažinti.
- Besimokantieji projektuos, įgyvendins ir vertins saugias tinklo architektūras, įskaitant svariausių saugumo technologijų, tokių kaip ugniasienės, IDS ir IPS, naudojimą.
- Besimokantieji gebės planuoti ir įgyvendinti reagavimo į incidentus ir atkūrimo strategijas, užtikrindami organizacijos atsparumą taikant veiksmingus atkūrimo ir veiklos tęstinumo planus.
- Besimokantieji demonstruos lyderystę kibernetinio saugumo srityje, kurdami strateginę politiką, vadovaudami kibernetinio saugumo projektams ir komandos bei priimdami pagrįstus ir etiškus sprendimus esant poreikiui.

5. PRIEDAI

5.1. A PRIEDAS: APŽVELGTOS LITERATŪROS SĄRAŠAS

Profesinio mokymo ir aukštojo mokslo institucijų kibernetinio saugumo švietimo apžvalga

1. https://ccb.belgium.be/en/ict-security-education-belgium
2. https://acdn.be/enewsv7/upload/whitepaper/CybersecurityReport.pdf
3. https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf
4. https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?country[]=fin
5. http://www.anc.edu.ro/standarde-pregatire-profesionala/
6. http://217.73.164.21/index.php/articles/curriculum/c556+592/
7. http://217.73.164.21/index.php/articles/c560/
8. https://www.agerpres.ro/english/2023/09/19/first-master-s-program-in-romania-in-cyber-security-accredited-by-eit-digital-at-ubb-cluj-napoca--1171675
9. https://dnsc.ro/invatamant/vezi/5
10. https://www.linkedin.com/posts/eit-digital_ubb-cluj-joins-eit-digital-adding-cybersecurity-activity-7031990099756081152-Sr77/?originalSubdomain=si
11. https://www.unitbv.ro/documente/curriculum-syllabus/Master/Plan%20inv/MI_master_TIN_2017_2018_PI.pdf
12. https://mateinfo.unitbv.ro/images/2023/planuri_inv/Plan_inv_2023_2025_Tehnologii_moderne_in_ingineria_sistemelor_soft.pdf
13. https://drive.google.com/drive/folders/1h9aC1xwobVtGN4gNukWMvDPXICf62FgF
14. Analysis and Diagnosis of Cybersecurity Talent in Spain, March 2022, Observaciber, https://www.observaciber.es/
15. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf
16. Panorama actual de la Ciberseguridad en España, Google https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf
17. Catálogos de formación en ciberseguridad, INCIBE, 2023 https://www.incibe.es/incibe/formacion/catalogos-formacion-ciberseguridad
18. Plan Nacional de competencias digitales https://portal.mineco.gob.es/es-es/digitalizacionIA/Paginas/plan-nacional-competencias-digitales.aspx
19. Plan España Digital 2025 https://avancedigital.mineco.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx
20. Plan de Digitalización de PYMES 2021-2025 https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_digitalizacion_pymes.pdf
21. Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4963

Kibernetinio saugumo iššūkiai ir pramonės poreikiai

1. El estado de la ciberseguridad en España, Deloitte, 2022 **https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html**
2. Ferreirós Orihuel, Inés (coord.). IV Informe sobre la Ciencia y Tecnología en España: Situar a España e el mapa geopolítico de la I+D+i. Fundación Alternativas: 187-206 (2023) **https://digital.csic.es/handle/10261/310469**
3. El reto de la ciberseguridad en España: un país vulnerable, Telefónica **https://www.telefonica.com/es/sala-comunicacion/blog/un-pais-vulnerable-el-reto-de-la-ciberseguridad-en-espana/**
4. Los retos de la ciberseguridad para las empresas españolas, Byte ti, 11 de enero de 2024 **https://revistabyte.es/tema-de-portada-byte-ti/retos-de-la-ciberseguridad/**
5. La falta de profesionales acentúa la amenaza de los ciberataques, el Periódico de España, 7 de Marzo de 2023 **https://www.epe.es/es/tecnologia/20230307/falta-profesionales-acentua-amenaza-ciberataques-84230209**
6. Analysis and Diagnosis of Cybersecurity Talent in Spain, March 2022, Observaciber, **https://www.observaciber.es/**

7. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación **https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf**
8. Panorama actual de la Ciberseguridad en España **https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf**
9. Plan España Digital 2025 **https://avancedigital.mineco.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx**
10. **Plan de Digitalización de PYMES 2021-2025 https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_digitalizacion_pymes.pdf**
11. **https://esco.ec.europa.eu/sites/default/files/ethical%20hacker.pdf**
12. **http://data.europa.eu/esco/occupation/276ba420-ef09-4a0e-b215-2c2e2f80ad28**
13. **https://nsm.no/fagomrader/digital-sikkerhet/**
14. **https://www.bdo.no/nb-no/nyheter/2023/na-jakter-hackerne-de-sma-selskapene**
15. **https://www.evelon.no/artikler/trussellandskapet-i-europa**
16. **https://norsis.no/sikkerhetskultur2023/sammendrag/**
17. **https://serit.no/hva-er-god-datasikkerhet-i-bedriften/**
18. **https://www.duo.uio.no/bitstream/handle/10852/96151/5/Master_thesis_mariwilh.pdf**

Moterys kibernetinio saugumo srityje

1. Microsoft. (2017, March). Why Europe's girls aren't studying STEM. Microsoft News. Retrieved January 20, 2024, from **https://news.microsoft.com/uploads/2017/03/ms_stem_whitepaper.pdf**
2. Women go tech. (2021, September). ICT workforce in Europe and its gender challenge after Covid-19. Women Go Tech. Retrieved January 20, 2024, from **https://womengotech.com/app/uploads/2021/09/ICT-workforce-in-Europe-and-its-gender-challenge.pdf**
3. Rodiklių duomenų bazė - Oficialiosios statistikos portalas. (n.d.) 1. **https://osp.stat.gov.lt/statistiniu-rodikliu-analize#/**
4. Bukauskas, Brilingaite, Ikamas, Juozapavicius, & Lepaite. (2022, August 5). Ataskaita Lietuvos kibernetinio saugumo kompetenciju¸ žemelapis. Vilnius University. Retrieved January 20, 2024, from **https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf**
5. **https://www.digi.no/artikler/debatt-flere-tech-jenter-ma-til-for-a-finne-morgendagens-losninger/535073**
6. **https://odanettverk.no/2022/03/08/dette-er-norges-50-fremste-tech-kvinner-2022/**
7. **https://e24.no/naeringsliv/i/k6Goma/etterlyser-flere-kvinner-til-cybersikkerhet**
8. **https://www.ssb.no/befolkning/artikler-og-publikasjoner/kvinner-velger-fortsatt-kvinneyrker**
9. **https://live.worldbank.org/en/event/2023/women-business-law-2023**
10. **https://wbl.worldbank.org/en/data/exploreeconomies/romania/2023**
11. **https://eige.europa.eu/gender-equality-index/2022/country/RO**
12. **https://cybernews.com/editorial/cyber-women-grim-statistics-big-opportunities/**
13. **https://www.weforum.org/agenda/2022/09/cybersecurity-women-stem/**
14. https://www.bcg.com/publications/2022/empowering-women-to-work-in-cybersecurity-is-a-win-winFerreirós Orihuel, Inés (coord.). IV Informe sobre la Ciencia y Tecnología en España: Situar a España e el mapa geopolítico de la I+D+i. Fundación Alternativas: 187-206 (2023) **https://fundacionalternativas.org/publicaciones/iv-informe-sobre-la-ciencia-y-la-tecnologia-en-espana/**
15. Mujeres empleadas en ciencia y tecnología (reparto por sectores). España, UE-27 y UE-28. Serie 2019-2021. **https://www.ine.es/jaxi/Tabla.htm?path=/t00/mujeres_hombres/tablas_1/l0/&file=c02002.px&L=0**
16. La mujer en la ciencia española, en datos y gráficos, EpData, 7 de marzo de 2023 **https://www.epdata.es/datos/mujer-ciencia-espanola-datos-estadisticas/298**
17. Analysis and Diagnosis of Cybersecurity Talent in Spain, March 2022, Observaciber, **https://www.incibe.es/ed2026/talento-hacker/publicaciones/diagnostico-talento-ciberseguridad**
18. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación **https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf**
19. Panorama actual de la Ciberseguridad en España, Google **https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf**

5.2. B PRIEDAS: APKLAUSOS KLAUSIMYNAS

Profesinio mokymo ir aukštojo mokslo klausimynas

Ši apklausa skirta išsiaiškinti dabartinę kibernetinio saugumo mokymų būklę ir būsimus poreikius bei padėti parengti veiksmingą kibernetinio saugumo mokymo programą, pritaikytą mažųjų ir vidutinių įmonių (MVĮ) kibernetinio saugumo problemoms spręsti.

Apklausa suskirstyta į 4 dalis:

- Demografiniai duomenys
- Mokymo programa, mokymo poreikiai ir mokymosi pageidavimai
- Kompetencijos reikalavimai ir būsimi įgūdžiai
- Su lytimi susijusios įžvalgos

Apklausai užpildyti prireiks maždaug 8 minučių.

DEMOGRAFIJA

Kokia yra jūsų šalis?
▫ Lietuva
▫ Belgija
▫ Norvegija
▫ Turkija
▫ Suomija
▫ Rumunija
▫ Ispanija
▫ Lenkija

Kokioje mokyklinėje įstaigoje šiuo metu dėstote?
▫ profesinio mokymo institucija
▫ aukštojo mokslo institucija

Kokia jūsų lytis?
▫ Vyras
▫ Moteris
▫ Nenoriu nurodyti

Kiek metų dalyvaujate kibernetinio saugumo mokymuose?
▫ Mažiau nei 1 metai
▫ 1-5 metai
▫ 6-10 metų
▫ Daugiau nei 10 metų

MOKYMO PROGRAMA, MOKYMO POREIKIAI IR MOKYMOSI PAGEIDAVIMAI

Kurios iš šių temų yra įtrauktos į jūsų kibernetinio saugumo mokymo programą? (Pasirinkite visus, kurios tinka)
▫ Kibernetinio saugumo pagrindai
▫ Grėsmių analizė ir valdymas

▫ Pažangūs grėsmių mažinimo būdai
▫ Kriptografija
▫ Tinklo saugumas
▫ Kibernetinio saugumo įstatymai ir politika
▫ Rizikos valdymas
▫ Reagavimas į incidentus
▫ Kita: _____

Kokius mokymo metodus pirmiausia taikote kibernetinio saugumo mokymuose? (Pasirinkite visus, kurie tinka)

▫ Paskaitos
▫ Praktinės laboratorijos
▫ Atvejo analizės
▫ Grupiniai projektai
▫ Internetinės simuliacijos
▫ Apversta klasė
Kita: _____

Kokie mokymosi formatai būtų veiksmingiausi kibernetinio saugumo mokymams? (Pažymėkite visus taikytinus variantus)

▫ Kontaktiniai seminarai
▫ Internetiniai kursai
▫ Internetiniai seminarai
▫ Interaktyvios simuliacijos
▫ Vaizdo pamokos
▫ Praktiniai užsiėmimai
▫ Kita: _____

Su kokiais didžiausiais iššūkiais susiduriate rengdami veiksmingus kibernetinio saugumo mokymus?

Atviras klausimas

Kaip manote, kiek efektyviai, vertinant skalėje nuo 1 iki 5, dabartinės mokymo programos parengia studentus realiems MVĮ kibernetinio saugumo iššūkiams?

▫ Labai neefektyviai
▫ Šiek tiek neefektyviai
▫ Neutralu
▫ Šiek tiek veiksminga
▫ Labai veiksminga

Kaip manote, ar dabartiniai kibernetinio saugumo mokymai atitinka konkrečius MVĮ poreikius?

1 (Neatitinka)
2 (Šiek tiek atitinka)
3 (Suderinta)
4 (Gerai suderinta)
5 (Labai suderinta)

Ar yra konkrečių temų ar įgūdžių, kuriuos įtraukiate į savo mokymus, atsižvelgiant į unikalius MVĮ kibernetinio saugumo poreikius? (Pažymėkite visus, kurie tinka)

▫ Kibernetinio saugumo pagrindai MVĮ
▫ Rizikos vertinimas ir valdymas MVĮ kontekste
▫ Reagavimas į incidentus MVĮ
▫ Duomenų apsauga ir privatumas MVĮ
▫ Kibernetinio saugumo politikos rengimas MVĮ
▫ Kita: _____

Kaip dažnai pritaikote arba adaptuojate savo kibernetinio saugumo mokymus, kad jie būtų geriau pritaikyti MVĮ?

▫ Visada
▫ Dažnai
▫ Kartais
▫ Retai
▫ Niekada

Ar gaunate grįžtamąjį ryšį arba ar palaikote ryšį su MVĮ atstovais ar specialistais, kad užtikrintumėte mokymo turinio atitiktį jų poreikiams?

▫ Taip, reguliariai
▫ Retkarčiais
▫ Retai
▫ Niekada

Remdamiesi savo patirtimi, kaip manote, kiek veiksmingi yra dabartiniai kibernetinio saugumo mokymai, kad MVĮ specialistai būtų pasirengę spręsti kibernetinio saugumo iššūkius?

▫ Labai neveiksmingi
▫ Šiek tiek neveiksmingi
▫ Neutralūs
▫ Šiek tiek veiksmingi
▫ Labai veiksmingi

Kokių turite pasiūlymų, kaip pagerinti kibernetinio saugumo mokymų MVĮ aktualumą ir veiksmingumą?

Atviras klausimas

KOMPETENCIJOS REIKALAVIMAI IR ATEITIES ĮGŪDŽIAI

Jūsų nuomone, kokių įgūdžių labiausiai trūksta dabartiniams MVĮ kibernetinio saugumo darbuotojams? (Pasirinkite ne daugiau kaip tris)?

▫ Grėsmių aptikimas ir reagavimas į jas
▫ Debesijos saugumo kompetencija
▫ Atitikties ir reguliavimo žinios
▫ Reagavimas į incidentus ir atkūrimas
▫ Rizikos valdymas ir analizė
▫ Duomenų privatumas ir apsauga
▫ Naujos technologijos
▫ Tinklo saugumas

Įvertinkite kompetencijas ir žinias, kurių reikia, skalėje nuo 1 (nereikia) iki 5 (labai reikia):

	Vertinimas				
Rizikos vertinimas ir valdymas Rizikos tipų ir poveikio supratimas.					
Techninės žinios Techniniai kibernetinio saugumo aspektai ir operacinių sistemų, tinklų ir duomenų bazių valdymo žinios.					
Reagavimas į incidentus ir atkūrimas Saugumo pažeidimų ir incidentų nustatymas, reagavimas į juos ir atsigavimas po jų.					
Politikos kūrimas ir įgyvendinimas Efektyvios saugumo politikos ir praktikos kūrimas ir įgyvendinimas.					
Grėsmių žvalgyba ir stebėsena Naujausių kibernetinio saugumo tendencijų, grėsmių ir atakų metodų stebėjimas.					
Bendravimo įgūdžiai Efektyvus bendravimas su darbuotojais, vadovybe ir galbūt klientais kibernetinio saugumo klausimais.					
Duomenų privatumas ir apsauga Duomenų privatumo principai ir kaip apsaugoti neskelbtiną informaciją.					

Ar matote kokį nors ankstesniame klausime nenurodytą svarbų įgūdžių ir žinių rinkinį, kuris gali būti labai reikalingas MVĮ?

Atviras klausimas

Kokioms naujoms kibernetinio saugumo grėsmėms, jūsų nuomone, MVĮ turi būti pasirengusios per ateinančius 5 metus? (Pasirinkite ne daugiau kaip tris)

▫ Išpirkos reikalaujančių programų atakos
▫ Daiktų interneto pažeidžiamumai
▫ Debesijos saugumo pažeidimai
▫ Dirbtinio intelekto valdomos kibernetinės atakos
▫ Vidinės grėsmės
▫ Kita: _____

Kokias 3 svarbiausias naujas kibernetinio saugumo mokymo tendencijas numatote per artimiausius 5 metus? (Pasirinkite iki 3 variantų)

▫ Dirbtinis intelektas ir mašininis mokymasis kibernetinio saugumo srityje
▫ Dėmesys minkštiesiems įgūdžiams ir tarpdisciplininiam mokymui
▫ Kvantinės kompiuterijos grėsmės
▫ Etinis įsilaužimas ir gynybiniai įgūdžiai
▫ Skaitmeninė tapatybė ir privatumas
▫ Decentralizuotos saugumo sistemos (pvz., blokų grandinė)
▫ Kita: _____

Ar yra kokių nors konkrečių mokymo metodų, priemonių ar platformų, kurios, jūsų nuomone, yra išskirtinai veiksmingos kibernetinio saugumo mokymui?

Atviras tekstas

Gal turite papildomų pastabų ar pasiūlymų, kaip pagerinti kibernetinio saugumo mokymus MVĮ?

Atviras tekstas

ĮŽVALGOS, SUSIJUSIOS SU LYTIMI

Koks apytikslis moterų procentas sudaro jūsų kibernetinio saugumo mokymo programų dalyvių skaičių?

▫ Mažiau nei 10 proc.
▫ 10% - 25%
▫ 26% - 50%
▫ 51% - 75%
▫ Daugiau nei 75 proc.

Ar yra kokių nors konkrečių iniciatyvų ar strategijų, kurias taikote siekdami paskatinti moterų dalyvavimą kibernetinio saugumo mokymuose?

▫ Taip
▫ Ne

Jei taip, nurodykite: _____

Ar manote, kad yra pakankamai į lyčių lygybę orientuotų kibernetinio saugumo mokymo modulių?

▫ Taip
▫ Ne
▫ Nežinau
▫ Man neaktualu

Kokios, jūsų patirtimi, yra pagrindinės kliūtys, trukdančios moterims dalyvauti kibernetinio saugumo mokymuose ir siekti karjeros arba tobulėti? (Pažymėkite visus, kurie tinka)

▫ Nepakankamas informuotumas apie kibernetinio saugumo galimybes
▫ Stereotipai arba kultūrinės normos
▫ mentorystės ar sektinų pavyzdžių trūkumas
▫ darbo ir asmeninio gyvenimo pusiausvyros problemos
▫ Jaučiamas lyčių šališkumas šioje srityje
▫ Kita: _____

Ar jūsų įstaiga turi specialią politiką ar programas, skirtas skatinti įvairovę ir įtrauktį, ypač moterų, kibernetinio saugumo mokymuose?

▫ Taip
▫ Ne
▫ Nežinau

Kas galėtų padėti kibernetinio saugumo mokymams labiau įtraukti lyčių lygybę? (Pasirinkite iki trijų)

▫ Daugiau moterų kibernetinio saugumo dėstytojų
▫ Siūlyti stipendijas ar paskatas
▫ Mokymo turinys, kuriame būtų išvengta lyčių šališkumo
▫ Didesnis sėkmingų kibernetinio saugumo specialisčių moterų matomumas

▫ Daugiau tik moterims skirtų mokymų
▫ Į lyčių lygybę orientuotos konkrečių atvejų studijos ir scenarijai
▫ Pritaikytos mokymo programos
▫ Mentorystės galimybės
▫ Kita: _____

MVĮ KLAUSIMYNAS

Šia apklausa siekiama nustatyti MVĮ kibernetinio saugumo pokyčių atstovų mokymo poreikius. Jūsų atsakymai padės suprasti dabartinę kibernetinio saugumo žinių ir įgūdžių padėtį įvairiose MVĮ, nustatyti kibernetinio saugumo mokymo spragas ir padidinti būsimų mokymo programų veiksmingumą.

Apklausa suskirstyta į 3 dalis:

- Demografiniai duomenys
- Mokymo poreikiai
- Įtraukimas ir moterų poreikis kibernetinio saugumo srityje.

Apklausai užpildyti prireiks maždaug 5 minučių.

DEMOGRAFIJA
Kokia yra jūsų šalis?
▫ Lietuva
▫ Belgija
▫ Norvegija
▫ Turkija
▫ Suomija
▫ Rumunija
▫ Ispanija
▫ Lenkija
Kokios yra jūsų dabartinės pareigos ir padalinys įmonėje?
Pareigos: _____
Padalinys: _____
Kokia jūsų lytis?
▫ Vyras
▫ Moteris
▫ Nenoriu nurodyti
Kiek darbuotojų dirba įmonėje?
▫ Iki 10 darbuotojų
▫ 11-50
▫ 51-250
Kaip įvertintumėte dabartinį darbuotojų kibernetinio saugumo žinių ir įgūdžių lygį?
▫ pradedančiųjų
▫ vidutinio lygio
▫ pažengę
Kiek darbuotojų atlieka darbus, susijusius su kibernetiniu saugumu?
Įrašykite skaičių: _____
Ar kibernetinio saugumo darbams atlikti samdote išorės tarnybas?
▫ Taip

▫ Ne

MOKYMO POREIKIAI

Naudodami skalę nuo 1 (neveiksminga) iki 5 (labai veiksminga), įvertinkite kaip veiksmingai, jūsų nuomone, dabartinės mokymo programos parengia studentus realiems MVĮ kibernetinio saugumo iššūkiams?

1 - Neefektyvu

5 - Labai efektyvu

Kokie, jūsų nuomone, yra pagrindiniai įgūdžių trūkumai dabartinėje MVĮ kibernetinio saugumo srityje? (Pasirinkite ne daugiau kaip tris)

▫ Grėsmių aptikimas ir reagavimas į jas
▫ Debesijos saugumo kompetencija
▫ Atitikties ir reguliavimo žinios
▫ Reagavimas į incidentus ir atkūrimas
▫ Rizikos valdymas ir analizė
▫ Duomenų privatumas ir apsauga
▫ Naujos technologijos
▫ Tinklo saugumas
▫ Kita: _____

Įvertinkite kompetencijas ir reikalingas žinias skalėje nuo 1 (nereikia) iki 5 (būtina):

	Vertinimas				
Rizikos vertinimas ir valdymas Rizikos tipų ir poveikio supratimas.					
Techninės žinios Techniniai kibernetinio saugumo aspektai ir operacinių sistemų, tinklų ir duomenų bazių valdymo žinios.					
Reagavimas į incidentus ir atkūrimas Saugumo pažeidimų ir incidentų nustatymas, reagavimas į juos ir atsigavimas po jų.					
Politikos kūrimas ir įgyvendinimas Efektyvios saugumo politikos ir praktikos kūrimas ir įgyvendinimas.					
Grėsmių žvalgyba ir stebėsena Naujausių kibernetinio saugumo tendencijų, grėsmių ir atakų metodų stebėjimas.					
Bendravimo įgūdžiai Efektyvus bendravimas su darbuotojais, vadovybe ir galbūt klientais kibernetinio saugumo klausimais.					
Duomenų privatumas ir apsauga Duomenų privatumo principai ir kaip apsaugoti neskelbtiną informaciją.					

Ar matote kokį nors svarbų įgūdžių ir žinių rinkinį, neišvardytą ankstesniame klausime, kuris gali būti labai reikalingas MVĮ?

Atviras klausimas

Kokioms naujoms kibernetinio saugumo grėsmėms, jūsų nuomone, MVĮ turi būti pasirengusios per ateinančius 5 metus? (Pasirinkite ne daugiau kaip tris)

▫ Išpirkos reikalaujančių programų atakos
▫ Daiktų interneto pažeidžiamumai
▫ Debesijos saugumo pažeidimai
▫ Dirbtinio intelekto valdomos kibernetinės atakos
▫ Vidinės grėsmės
▫ Kita: _____

Kokių konkrečių spragų (trūksta saugumo žinių ar įgūdžių), jei tokių yra, jūsų nuomone, turi dabartiniai kibernetinio saugumo darbuotojai?

▫ Žemas techninių įgūdžių lygis
▫ Žemas minkštųjų įgūdžių lygis
▫ Žemas pažeidžiamumo vertinimo lygis
▫ Žemas politikų ir reguliacijų supratimo lygis
▫ Žemas grėsmių suvokimo lygis
▫ Žemas kibernetinio saugumo reguliarių mokymų lygis
▫ Kita: _____

Kokias 3 svarbiausias naujas kibernetinio saugumo mokymų tendencijas numatote per ateinančius 5 metus? (Pasirinkite ne daugiau kaip 3 variantus)

▫ Dirbtinis intelektas ir mašininis mokymasis kibernetinio saugumo srityje
▫ Dėmesys minkštiesiems įgūdžiams ir tarpdisciplininiam mokymui
▫ Kvantinės kompiuterijos grėsmės
▫ Etinis įsilaužimas ir gynybiniai įgūdžiai
▫ Skaitmeninė tapatybė ir privatumas
▫ Decentralizuotos saugumo sistemos (pvz., blokų grandinė)
▫ Kita: _____

ĮTRAUKTIS IR MOTERŲ POREIKIAI KIBERNETINIO SAUGUMO SRITYJE

Ar manote, kad dabartiniai kibernetinio saugumo mokymai yra integraciniai ir veiksmingai tenkina visų lyčių poreikius?

▫ Taip
▫ Ne
▫ Nežinau

Jei save priskiriate prie moterų, ar susidūrėte su kokiomis nors kliūtimis ar sunkumais, kai norėjote dalyvauti kibernetinio saugumo mokymuose ir (arba) studijose?

▫ Taip
▫ Ne
▫ Nenoriu sakyti
▫ Jei taip, nurodykite: _____

Ar žinote apie kokias nors iniciatyvas ar programas savo organizacijoje, kurios konkrečiai remia ar skatina moterų dalyvavimą kibernetinio saugumo srityje?

▫ Taip
▫ Ne
▫ Nežinau

Kokio pobūdžio parama ar ištekliai paskatintų daugiau moterų jūsų organizacijoje dalyvauti kibernetinio saugumo mokymuose? (Atviras klausimas)

Atviras klausimas

Kokius patobulinimus ar naujoves siūlytumėte kibernetinio saugumo mokymų efektyvumui didinti?

Atviras klausimas

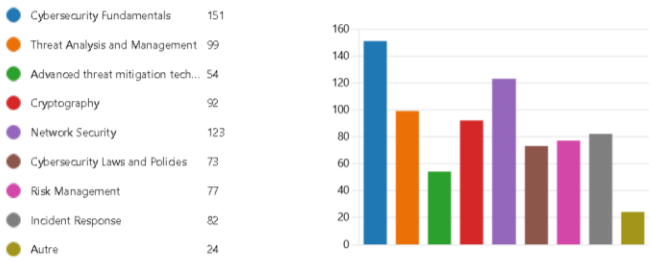
5.3. C PRIEDAS: APKLAUSOS REZULTATAI

Profesinio mokymo ir aušt̨ųjų mokymo įstaigų atstovų atsakymai

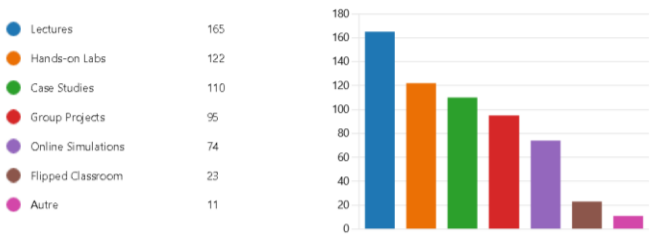
Mapping the training needs for SME Cyber Security Change Agents - VET and HEI survey

190 Responses

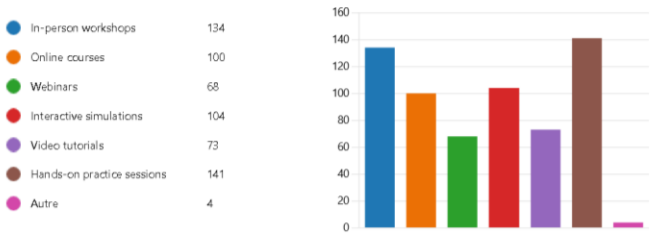
1. **Which of the following topics are included in your cybersecurity training program? (Select all that apply)**



2. **What teaching methods do you primarily use in your cybersecurity training? (Select all that apply)**



3. **What teaching method would be the most effective for cybersecurity training? (Select all that apply)**



4. **What are the biggest challenges you face in delivering effective cybersecurity training?**

190
Réponses

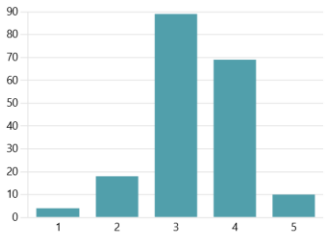
Dernières réponses
"-"
"-"
"keeping up with Technology Changes, Basic knowledge of the students, Soft...

Mettre à jour

34 répondants (**19**%) répondu **students** pour cette question.

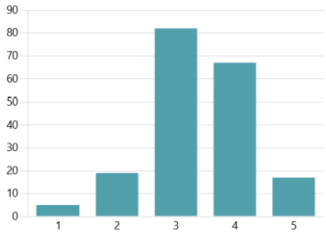
5. **On a scale of 1 (Very Ineffective) to 5 (Very Effective), how effectively do you think the current training programs prepare students for real-world SMEs cybersecurity challenges?**

3.33
Évaluation moyenne



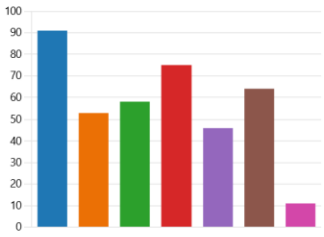
6. **On a scale of 1 (Not aligned) to 5 (Highly aligned), how well do you believe the current cybersecurity training aligns with the specific needs of SMEs?**

3.38
Évaluation moyenne



7. **Are there specific topics or skills that you include in your training to address the unique cybersecurity needs of SMEs? (Select all that apply)**

Basic Cybersecurity for SMEs	91
Risk Assessment and Managem...	53
Incident Response for SMEs	58
Data Protection and Privacy for ...	75
Cybersecurity Policy Developme...	46
No SME's specific topic or skills ...	64
Autre	11



8. **How often do you customize or adapt your cybersecurity training to better cater to SMEs?**

Always	14
Often	60
Sometimes	55
Rarely	47
Never	14

9. **Do you receive feedback or are you in contact with SME representatives or professionals to ensure the relevancy of your training content to their needs?**

Yes, regularly	43
Occasionally	64
Rarely	54
Never	29

10. **Based on your experience, how effective do you believe the current cybersecurity training is in equipping SME professionals to handle cybersecurity challenges?**

Very Ineffective	7
Somewhat Ineffective	21
Neutral	65
Somewhat Effective	88
Very Effective	9

11. **What suggestions do you have for improving the relevance and effectiveness of cybersecurity training for SMEs?**

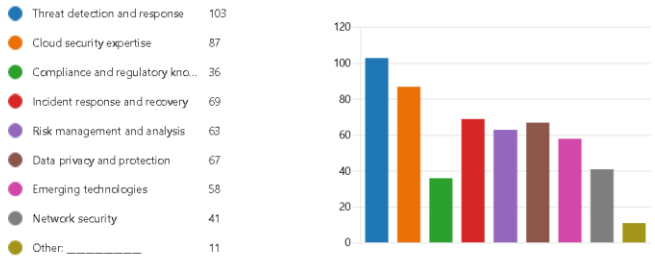
117
Réponses

Dernières réponses
"leverage external expertise, practical hands-on exercises, interactive training...

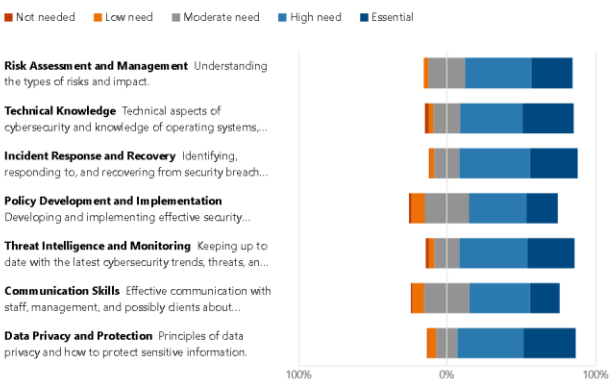
Mettre à jour

36 répondants (**31**%) répondu **trainings** pour cette question.

12. **In your opinion, what are the top skills deficits in the current SME cybersecurity workforce? (Choose up to three)**



13. **Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:**



14. **Do you see any relevant set of skills and knowledge not listed in the previous question that might be highly needed for SMEs?**

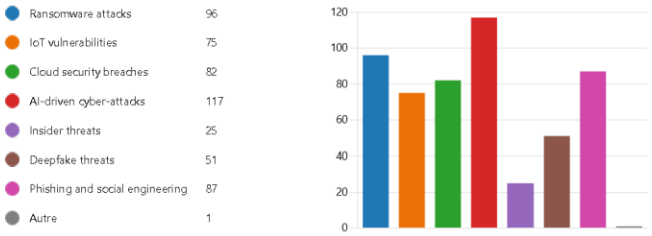
190
Réponses

Dernières réponses
"-"
"-"
"Cloud Security, AI"

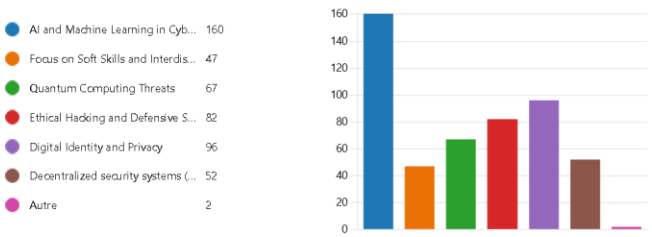
Mettre à jour

10 répondants (**5**%) répondu **skills** pour cette question.

15. **Which emerging cybersecurity threats do you believe SMEs need to be prepared for in the next 5 years? (Choose up to three)**



16. **What do you foresee as the top 3 emerging trends in cybersecurity training for the next 5 years? (Choose up to 3 options)**



17. **Are there any particular training methods, tools, or platforms that you believe are exceptionally effective for cybersecurity education?**

115
Réponses

Dernières réponses
"TryHackMe, HackTheBox"

Mettre à jour

12 répondants (**11**%) répondu **platform** pour cette question.

18. **Any additional comments or suggestions for improving cybersecurity training for SMEs?**

80
Réponses

Dernières réponses
"Uniform Course material"

Mettre à jour

9 répondants (**11**%) répondu **SMEs** pour cette question.

19. **What is the estimated percentage of women among the participants in your cybersecurity training programs?**

Less than 10%	57
10% - 25%	79
26% - 50%	43
51% - 75%	8
More than 75%	3

20. **Are there any specific initiatives or strategies you employ to encourage women's participation in cybersecurity training?**

Yes	30
No	160

21. **If you replied "Yes" to the previous question, please specify**

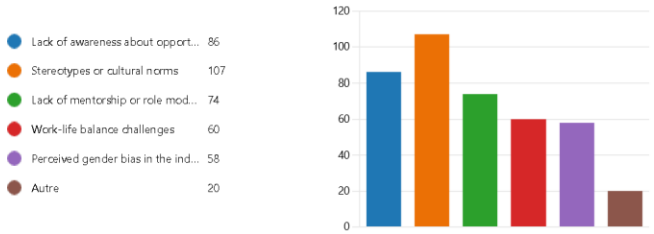
35
Réponses

Dernières réponses

13 répondants (**37**%) répondu **women** pour cette question.

22. **Do you believe there are enough gender-inclusive training modules available in cybersecurity?**

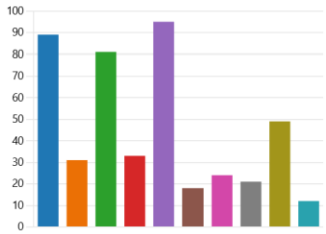
23. **In your experience, what are the primary barriers that prevent women from participating or advancing in cybersecurity training and careers? (Select all that apply)**



24. **Does your institution have specific policies or programs to promote diversity and inclusion, particularly for women, in cybersecurity training?**

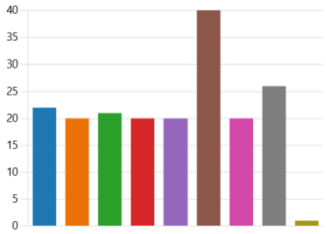
25. **What could make cybersecurity training more gender-inclusive? (Choose up to three)**

More female cybersecurity instr...	89
Regularly update policies to sup...	31
Offer scholarships or incentives	81
Training content that avoids gen...	33
Increased visibility of successful ...	95
More women-only training sessi...	18
Gender-inclusive case studies a...	24
Tailored training programs	21
Mentorship opportunities	49
Autre	12



26. **What is your country?**

Lithuania	22
Belgium	20
Norway	21
Türkiye	20
Finland	20
Romania	40
Spain	20
Poland	26
Azerbaijan	1



27. **In which school institution are you currently teaching?**

VET (Vocational Education and T...	86
HEI (Higher Education (HE) Instit...	104

28. **What is your gender?**

Male	121
Female	64
Prefer not to say	5

29. **How many years have you been involved in cybersecurity training? (Either general, specific, short and long trainings)**

Less than 1 year	21
1-5 years	85
6-10 years	53
More than 10 years	31

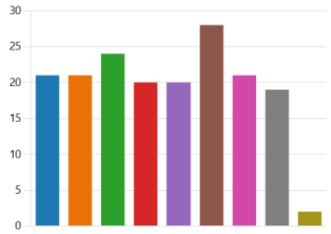
MVĮ atstovų atsakymai

Mapping the training needs for SME Cyber Security Change Agents - SMEs survey

176 Responses

1. **What is your country?**

Lithuania	21
Belgium	21
Norway	24
Türkiye	20
Finland	20
Romania	28
Spain	21
Poland	19
Azerbaijan	2



2. **What is your company sector?**

176
Réponses

Dernières réponses
"Consultancy"
"Cyber Security - Management Consultancy"
"Education, VET"

Mettre à jour

13 répondants (**7**%) répondu **education** pour cette question.

3. **What is your current position in the company?**

176
Réponses

Dernières réponses
"Team lead"
"Owner & Director"
"Teacher"

Mettre à jour

43 répondants (**25**%) répondu **Manager** pour cette question.

4. **What is your gender?**

5. **How many employees are working in the company?**

6. **How would you rate employees' current level of cybersecurity knowledge and skills?**

7. **How many employees perform work related to cybersecurity?**

176
Réponses

Dernières réponses
"3"
"2"
"3"

Mettre à jour

36 répondants (**21**%) répondu **1** pour cette question.

8. **How many of these employees are women?**

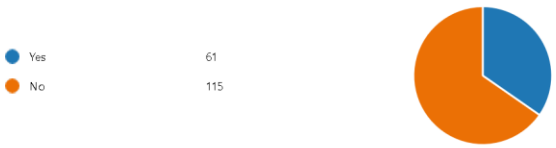
176
Réponses

Dernières réponses
"1"
"1"
"0"

Mettre à jour

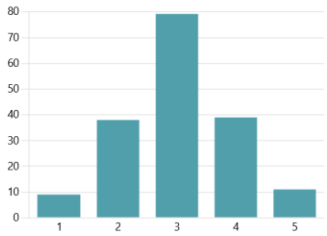
31 répondants (**18**%) répondu **1** pour cette question.

9. **Do you hire external services for cybersecurity work?**



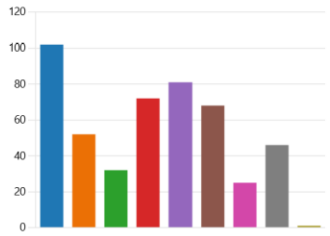
10. **On a scale of 1 (ineffective) to 5 (very effective), how effectively do you think the current training programs prepare students for real-world SMEs cybersecurity challenges?**

3.03
Évaluation moyenne

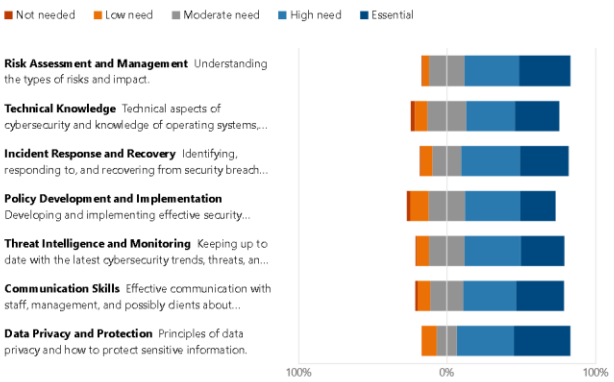


11. **In your opinion, what are the top skills deficits in the current SME cybersecurity workforce? (Choose up to three)**

Threat detection and response	102
Cloud security expertise	52
Compliance and regulatory kno...	32
Incident response and recovery	72
Risk management and analysis	81
Data privacy and protection	68
Emerging technologies	25
Network security	46
Other: _____	1



12. **Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:**



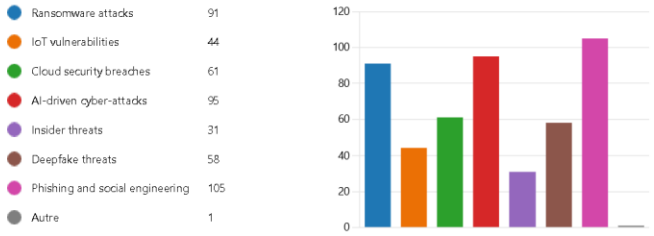
13. **Do you see any relevant set of skills and knowledge not listed in the previous question that might be highly needed for SMEs?**

175
Réponses

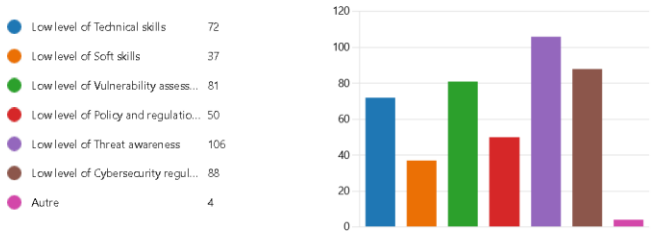
Dernières réponses
"My assumption is that Subject matter experts (SME's) in a big company are ...
"Cyber Security on all these topics arround Generative AI - which is complete...
"Not sure"

4 répondants (**2**%) répondu **skills** pour cette question.

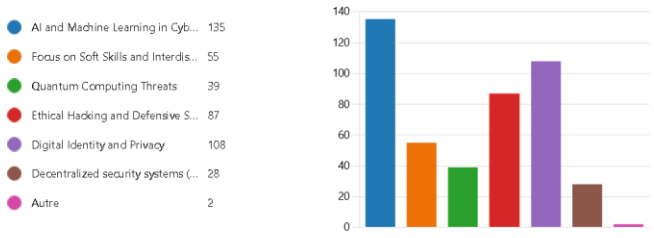
14. **Which emerging cybersecurity threats do you believe SMEs need to be prepared for in the next 5 years? (Choose up to three)**



15. **What specific gaps, if any, do you feel exist in employee's current cybersecurity knowledge or skills status? (Choose up to three)**

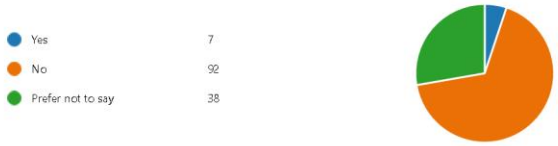


16. **What do you foresee as the top 3 emerging trends in cybersecurity training for the next 5 years? (Choose up to 3 options)**



17. **Do you feel that current cybersecurity training is inclusive and addresses the needs of all genders effectively?**

18. **If you identify as female, have you faced any barriers or challenges in accessing or participating in cybersecurity training/studies?**



19. **If you replied "Yes" to the previous question, please specify**

11
Réponses

Dernières réponses
"I feel that previous question is missing one more answer such as "I'm a male...
"I have to actively look for help and support for us females who work in the C...

Mettre à jour

3 répondants (**30**%) répondu **male** pour cette question.

20. **Are you aware of any initiatives or programs within your organization that specifically support or promote the participation of women in cybersecurity?**

21. **If you replied "Yes" to the previous question, please specify**

17
Réponses

Dernières réponses
"I am a strong female advocate for Cyber Security, Women Supporting Wom..."

8 répondants (**47**%) répondu **Women** pour cette question.

5.4. D PRIEDAS: PERŽIŪRĖTŲ ESCO PROFESIJŲ SĄRAŠAS

Nuorodos:

2529.1 https://esco.ec.europa.eu/sites/default/files/chief%20ICT%20security%20officer.pdf
2529.2 https://esco.ec.europa.eu/sites/default/files/digital%20forensics%20expert.pdf
2529.3 https://esco.ec.europa.eu/en/classification/occupation?uri=http%3A%2F%2Fdata.europa.eu%2Fesco%2Foccupation%2F1c5a896a-e010-4217-a29a-c44db26e25da
2529.4 https://esco.ec.europa.eu/sites/default/files/ethical%20hacker.pdf
2529.5 https://esco.ec.europa.eu/sites/default/files/ICT%20resilience%20manager.pdf
2529.6 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20administrator.pdf
2529.7 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20consultant.pdf
2529.8 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20manager.pdf
2529.9 https://esco.ec.europa.eu/sites/default/files/knowledge%20engineer.pdf

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