Ataskaita
Lietuvos kibernetinio saugumo kompetencijų žemėlapis

2022 m. rugpjūčio mėn. 5 d.

Linas Bukauskas, Agnė Brilingaitė, Kęstutis Ikamas,

Aušrius Juozapavičius, Daiva Lepaitė

Lietuvos mokslo taryba

Vilniaus universitetas

Mokslinį tyrimą finansavo
Lietuvos mokslo taryba
Reikminių tyrimų projektas
Nacionalinio kibernetinio saugumo kompetencijų žemėlapio kūrimas / CIBERSEK
Projekto finansavimo sutartis Nr. S-REP-21-2
Projektą įgyvendino Vilniaus universitetas ir Generolo Jono Žemaičio Lietuvos karo akademija

KIBERNETINIO SAUGUMO LABORATORIJA
INFORMATIKOS INSTITUTAS
VILNIAUS UNIVERSITETAS
DIDLAUKIO 47, LT-08303
VILNIUS
+370 5 219 5002
LINAS.BUKAUSKAS@MIF.VU.LT

TYRIMO AUTORIAI IR ATASKAITOS RENGĖJAI:
DR. LINAS BUKAUSKAS (TYRIMO VADOVAS)
DR. AGNĖ BRILINGAITĖ
DR. KĘSTUTIS IKAMAS
PROF. DR. AUŠRIUS JUOZAPAVIČIUS
DR. DAIVA LEPAITĖ

Ačiū prisidėjusiems prie ataskaitos rengimo:
RIMANTĖ ANDRIJAUSKAITĖ

HTTPS://DOI.ORG/10.15388/CIBERSEK.2022

Pirmo viešinimo data: 2022 rugpjūčio mėn. 5 d.
Taisymo/papildymo data: 2022 m. gruodžio 12 d.
© Linas Bukauskas, Agnė Brilingaitė, Daiva Lepaitė, Vilniaus universitetas, 2022
© Kęstutis Ikamas, Aušrius Juozapavičius, Generolo Jono Žemaičio Lietuvos karo akademija, 2022
© Vilniaus universitetas, 2022

Turinys

Turinys 6

Anotacija 7

Synopsis 8

Įvadas 9

Apibrėžtys ir trumpiniai 13

1 Tyrimo kontekstas 15

1.1 Teisės aktai ir kiti formalūs dokumentai 15

1.2 Profesinių bendruomenių rekomendacijos 16

1.3 Kvalifikacijų lygiai ir sandara 17

1.4 Formalusis ir neformalusis ugdymas 18

1.5 Mokslo grupės ir atliekami tyrimai 22

1.6 Organizacijos veikiančios KS lauke Lietuvoje **23**

1.7 Tarptautiniai projektai, iniciatyvos ir užsienio šalių geroji praktika **23**

1.7.1 Projektai ir gerosios patirtys 23

1.7.2 Kibernetiniai šauktiniai 25

2 Tyrimas 27

2.1 Kompetencijų taksonomijos **28**

2.2 Tyrimo dizainas ir rezultatų patikimumas **32**

3 Tyrimo rezultatai 37

3.1 Omnibus: Visuomenės požiūrio į kibernetinį saugumą tyrimas **37**

3.1.1 Gauti rezultatai 38

3.1.2 Išvados 45

3.2 Organizacijų vadovų tyrimas **47**

3.2.1 Gauti rezultatai 47

3.2.2 Išvados 51

3.3 Žvalgomasis kibernetinio saugumo ir IT specialistų tyrimas **53**

3.3.1 Gauti rezultatai 53

3.3.2 Išvados 56

3.4 Ekspertinių interviu tyrimas **58**

3.4.1 Gauti rezultatai 58

3.4.2 Išvados 61

3.5 Fokus grupių tyrimas **64**

3.5.1 Gauti rezultatai 64

3.5.2 Išvados 68

3.6 Darbo skelbimų tyrimas 69

3.6.1 Gauti rezultatai 70

3.6.2 Išvados 81

4 Kompetencijų žemėlapis 83

4.1 KS kompetencijų poreikis pagal organizacijos tipą 83

4.2 Veiklomis paremtas kompetencijų žemėlapis 85

4.3 Lietuvos kompetencijų poreikio žemėlapis 89

4.4 KS karjeros kelias 91

5 Išvados 93

6 Rekomendacijos 97

Literatūros sąrašas 99

Knygos ir jų skyriai 99

Straipsnių rinkinių dalys 100

Žurnaliniai straipsniai 100

Tarptautinių renginių leidiniai 102

Techninės ataskaitos 103

Žiniatinklio ištekliai 103

A Priedai 107

A.1 Omnibus: Visuomenės požiūrio į kibernetinį saugumą apklausa 107

A.1.1 KSS Klausimyno dalis 107

A.2 Organizacijų vadovų tyrimas **112**

A.2.1 Klausimynas 112

A.2.2 The questionnaire 118

A.2.3 Aprašomoji informacija 124

A.3 KS specialistų apklausa **129**

A.3.1 Klausimynas 129

A.3.2 Questionire 136

A.3.3 Respondentų pageidavimai KS specialistų rengimui 142

A.4 Pusiau struktūrizuoti ekspertų interviu **143**

A.4.1 Interviu nr. 1 143

A.4.2 Interviu nr. 2 145

A.4.3 Interviu nr. 3 150

A.4.4 Interviu nr. 4 153

A.4.5 Interviu nr. 5 155

A.5 Fokus grupės dialogo gairės **159**

Anotacija

Sparčiai tobulėjant technologijoms, paslaugoms persikeliant į elektroninę erdvę, šalies ekonominiam ir politiniam stabilumui grėsmę kelia didėjantis kibernetinių incidentų kiekis, kuriems spręsti reikalingi kibernetinio saugumo specialistai. Įprastai kibernetinio saugumo darbo rinkoje dominuoja IT išsilavinimą ar kvalifikaciją turintys darbuotojai. Lietuvoje, kaip ir visame pasaulyje, didėja tokių specialistų poreikis, bet jį sunku patenkinti, nes esamų darbo vietų kvalifikaciniai reikalavimai apima technologines žinias bei integruoja kitų disciplinų ir bendrųjų kompetencijų poreikį. Esant tokiai situacijai, šalys nacionaliniu lygmeniu privalo turėti strategiją, numatančią darbuotojų pritraukimą į šį sektorių ir jų rengimą bei kvalifikacijos tobulinimą, atsižvelgiant į kintančią saugumo padėtį. Tarptautinė praktika rodo, kad į sektorių būtina pritraukti ir suteikti reikalingas kompetencijas ne tik technologinių, bet ir kitų sričių specialistams.

Šio projekto tikslas – paruošti pirmąjį nacionalinį kibernetinio saugumo kompetencijų žemėlapį ir pateikti rekomendacijas specialistų pritraukimui į kibernetinio saugumo sektorių bei jų kompetencijų ugdymo gaires. Projekto vykdymo metu atlikta šio lauko kompetencijų poreikio analizė pasaulyje, tirtas specialistų poreikis Lietuvoje, apklausiant srities profesionalus, krašto apsaugos sistemos, viešojo ir privataus sektoriaus įmonių vadovus ir ekspertus, nustatytas esamas karjeros kelias, analizuoti darbo skelbimai, išskirtos darbo rolės ir surastos sąsajos su moksliniuose darbuose bei kitų šalių nacionalinėse ataskaitose pateiktomis įžvalgomis bei kompetencijų ugdymo rekomendacijomis. Darbo rezultatai surinkti duomenų bazėje, ekspertinės tyrimo rezultatų įžvalgose bei rekomendacijose suinteresuotoms šalims, o taip pat paruoštas mokslinis straipsnis, siekiant viešinti gautus rezultatus.

Synopsis

The rapid advancement of technologies and transfer of services to cyberspace inevitably leads to an increased number of cyber incidents raising a threat to national economic and political stability. Cybersecurity (CS) specialists tasked with the prevention of these incidents usually have IT education. Demand for these specialists grows in Lithuania the same way as in other countries. However, it is not easy to satisfy it because the CS job requires specific technological knowledge from several overlapping areas as well as an extensive collection of general competencies. Therefore, a country must have a national-level strategy of recruitment and coordinated education of the specialists to meet future workforce demands. Experience of other countries shows a need to attract non-technological specialists to the area.

This project aims to prepare the first Lithuanian cyber competence map together with recommendations on how to attract specialists to the CS sector and how to advance their competencies. During the project, we explored the demand for CS specialists in Lithuania and the world, surveyed the opinions of CS professionals, management and specialists from private and public sector organizations, including national defence sector. Also, we determined the career path of the specialists, analyzed job offers, distinguished work roles, and gathered findings and recommendations from scientific research papers and similar reports of other countries. The results of the project include a publicly available database of collected data, expert findings of the research and recommendations for stakeholders, and a submitted scientific article to promote the results.

Įvadas

Projekto tikslas – ištirti Lietuvos kibernetinio saugumo (KS) specialistų kompetencijų poreikį, paruošti nacionalinį KS kompetencijų žemėlapį bei pateikti rekomendacijas kompetencijų ugdymui ir naujų darbuotojų pritraukimui į sritį sprendžiant specialistų trūkumą.

Uždaviniai:

1. Atlikti KS lauko tyrimą, vykdant įmonių vadovų ir specialistų apklausas keliuose aktualiuose sektoriuose – krašto apsaugos sistemos, informacinių technologijų, privataus, viešojo valdymo bei kituose sektoriuose, kuriuose yra KS kompetencijų poreikis, o taip pat ištirti viešoje erdvėje žiniatinklyje skelbiamus darbo pasiūlymus KS specialistams.
2. Išanalizuoti pasaulyje egzistuojančius KS kompetencijų modelius, rekomendacijas ir kitas gaires iš susijusių ar persidengiančių sričių, pavyzdžiui, IRT, kurie aktualūs specialisto ugdymo procese (profesinis mokymas, aukštasis išsilavinimas) bei persikvalifikuojant ir mokantis visą gyvenimą.
3. Susieti lauko tyrimo rezultatus su egzistuojančių modelių analizės tyrimais, paruošti bendrųjų ir dalykinių kompetencijų žemėlapį išskiriant kompetencijų ir darbo rolių specifiką.
4. Remiantis gautais rezultatais, mokslinių KS bei ugdymo srities darbų pateiktomis įžvalgomis ir suformuotu kompetencijų žemėlapiu, pateikti mokslo, ugdymo įstaigoms, verslo įmonėms ir viešojo valdymo institucijoms KS kompetencijų ugdymo ir specialistų pritraukimo rekomendacijas.

Pasaulyje egzistuojantys KS kompetencijų modeliai dažnai orientuoti į JAV rinką ir nepritaikomi siauresnei saugumo sričiai, todėl šiame projekte bus atliktas lauko tyrimas, įvertinta kitų šalių patirtis ir sukurta pirma nacionalinė KS kompetencijų sąranga su rekomendacijomis sprendžiant srities specialistų trūkumą. Kibernetinėje erdvėje yra daug neapibrėžtumų, persidengia kelios mokslo sritys, technologijos kinta greitai, todėl projekte reikės kūrybiškų sprendimų adaptuojant kitų šalių patirtį pagal tyrimais nustatytą Lietuvos specifiką ir formuojant KS specialistų ugdymo gaires įvairioms (skirtingoms) suinteresuotoms pusėms.

Aktualumas

2020 m. Lietuvos elektroninė sveikatos informacinė sistema neveikė visą savaitę, kilo problemų jungiantis prie kai kurių bankų – ir tai net nebuvo kibernetinės atakos pasekmė, o gamtos sąlygų padarinys. Ateityje priklausomybė nuo skaitmeninio pasaulio tik augs, todėl į kibernetinį saugumą reikia žiūrėti kaip į valstybės duomenų valdymo ir ekonominio gyvenimo tvarumo klausimą. Izraelis sugebėjo šią problemą transformuoti į ekonominį pranašumą pasinaudodamas tinkama specialistų pritraukimo ir ugdymo strategija [58]. Kitos šalys taip pat stengiasi suvaldyti problemą. Suomiai pozicionuoja save kaip mažą šalį su stipriu IRT sektoriumi ir pabrėžia, kad KS ekspertų trūkumas

daro didelį poveikį visai šaliai, organizacijoms ir individams, o prieiga prie talentingų žmonių tampa labai svarbi [55]. Atlikę apklausas, interviu, išanalizavę tyrimų duomenis, mokslininkai siūlo metrikas, leidžiančias pakelti KS lygmenį ugdant kompetencijas nacionaliniu mastu. Analogiškai australai [29] tyrė darbo skelbimus ir vykdė apklausas, o po to išskyrė kompetencijų rinkinius pagal Australijos specifiką, kad šalies aukštosios mokyklos galėtų pasinaudoti šiais rezultatais būsimų specialistų ugdymui. Kai kuriuos užsienio šalių sprendimų elementus galima būtų pritaikyti Lietuvai.

Lietuvoje atlikti KS specialistų trūkumo tyrimą ir sukurti kompetencijų žemėlapį galima remiantis tais pačiais principais, kurie buvo naudojami pasaulyje žinomų sąrangų sudarymui, tačiau pritaikant Lietuvos dydžiui ir specifikai, t.y. reikalinga įvertinti rinkos poreikius, prognozes, specialistų pasirenkamą ugdymo planą, atlikti aplinkos ir analogų pasaulyje analizę.

Vienas iš žymiausių KS kompetencijų modelis, naudojamų kaip atspirties taškas ugdant KS specialistus, yra NIST NICE, sukurtas JAV nacionalinio standartizacijos instituto [49]. Šiame modelyje išskirtos kategorijos, specializacijos, pareigybės organizacijoje, o naudojama žinių-įgūdžių-gebėjimų (angl. knowledge, skills, and abilities, KSA) kompetencijų sąranga leidžia susieti roles su KSA elementais. Šios iniciatyvos idėja buvo paruošti gaires vyriausybei, mokslo bendruomenei ir verslo sektoriui, kad ruošdami KS specialistus koordinuotų veiksmus pritraukdami naują darbo jėgą. Šiuo metu rengiami šio modelio atnaujinimai [51], pabrėžiant, kad užduotys (angl. tasks) sudaro darbo procesą (angl. work), kurį reikia aprašyti detaliai, kai ieškoma darbuotojo konkretiems procesams. Technologijos ir informacija sparčiai kinta, o su šiomis sritimis susiję specialistai tampa mokymosi visą gyvenimą dalyviais. Modelyje taip pat įvedama per pastaruosius dvidešimt metų ugdymo sistemos lygmenyse mokymo(si) procesuose įsivyravusi [67] kompetencijos sąvoka, apimanti reikalingas žinias, gebėjimus ir asmenines savybes bei nuostatas. Besimokantysis ar ieškantis darbo gali susieti darbą su savo gebėjimais. Verta ištirti, kiek ši sąranga bei kiti populiarūs kompetencijų modeliai, pvz., ACM (Joint Task Force on Cybersecurity Education, 2018), tinka Lietuvos darbo rinkai. Įvairiuose sektoriuose kuriami kompetencijų modeliai kibernetiniam saugumui [65] bei skaitmenizuotų kompetencijos modelių kritinės apžvalgos [52] suteikia solidų mokslinį pagrindą pagrįsti šį modelį atsižvelgiant į Lietuvos kontekstą.

Parrish ir kt. [50] pabrėžia, kad KS yra meta-disciplina, bet dažniausiai siejama su inžinerija ir kompiuterių mokslais (angl. computing). Lietuvoje taip pat įprastai kibernetinio saugumo specialistais tampa IT specialistai [48], bet paties IT sektoriaus darbo vietos nėra užpildytos, IRT specialistų (absolventų) skaičius lyginant su kitomis šalimis didėja lėčiau (Nacionalinė švietimo agentūra, 2020), moterys nelinkusios rinktis IRT srities savo profesijai, nors pastebimas stojančiųjų moterų skaičiaus padidėjimas (Simaškaitė, 2019). KS kaip su IT susijusi sritis laikoma itin paklausia ir perspektyvia, todėl Lietuvoje būtina nacionaliniu lygmeniu formuoti strategiją kaip pritraukti kuo daugiau specialistų. Tarptautiniai tyrimai ((ISC)^2, 2020) rodo, kad yra poreikis aktyviai ir masiškai pritraukti specialistus į sektorių. Tyrimo metu nustatyta, kad Z karta turi ne tokį pozityvų požiūrį į KS sritį, todėl gali būti papildomų iššūkių pritraukiant jaunuosius talentus.

Technologinių žinių nepakanka sprendžiant KS incidentus, nes sėkmingą gynybą lemia ne tik technologinis pasirengimas, bet ir gebėjimas išvengti žmogiškųjų klaidų [14]. Reikia nepamiršti ir aukštųjų mokyklų absolventų, kurie turi netechnologinį pagrindinį laipsnį (angl. major degree)m tačiau kurių įgytos kompetencijos gali būti reikšmingos KS sektoriui [35]. Kai kurios specialistų rolės NIST NICE modelyje apibrėžtos ne taip griežtai kaip kitos ir pakliūna į netechnologinę ar daugiadisciplinę sritį. Tokiu būdu atveriamos galimybės pritraukti žmones be IT išsilavinimo taip subalansuojant KS darbo jėgą. Pavyzdžiui, verslo mokyklos gali ruošti KS specialistus, pasirinkusios tinkamus modelius - mažiau ar daugiau technologinius [32]. KS specialistams ir apskritai personalui reikalingi KS mokymai keliant jų kvalifikaciją, ugdant praktinius gebėjimus. Dėl to darbuotojų sertifikavimas ir mokymas tampa sudėtingas, nes dalyvių lygis yra nuo žemo iki eksperto [30], todėl turi būti tinkamai suprojektuoti mokymo modeliai [5].

Apibendrinant galima teigti, kad atlikus egzistuojančių pasaulyje kompetencijų žemėlapių (tokių kaip NIST, ACM) analizę, surinkus ilgo laikotarpio darbo skelbimus, apklausus įmonių vadovus ir specialistus, atlikus KS studijų programų apžvalgą (pvz., SPARTA Project, 2020) ir KS sertifikavimo programų analizę, bus nustatytas KS specialistų Lietuvoje trūkumas ir ateities kompetencijų poreikis, parinktos tiesioginės ir netiesioginės jo metrikos, išsiaiškintos jo priežastys ir atitinkamai pasiūlytos priemonės šiai problemai spręsti.

Apibrėžtys ir trumpiniai

ACM	- angl. Association for Computing Machinery
DB	- Duomenų bazė
ESCO	- angl. European Skills, Competences, Qualifications and Occupations
EQANIE	- angl. European Quality Assurance Network for Informatics Education
IRT	- Informacijos ir ryšio technologijos
IT	- Informacinės technologijos
KS	- Kibernetinis saugumas
KSS	- Kibernetinio saugumo specialistas
LKA	- Generolo Jono Žemaičio Lietuvos karo akademija
NIST	- angl. National institute of standards
PLT	- Profesinio lauko tyrimas
VU	- Vilniaus universitetas
VU KSL	- Vilniaus universiteto kibernetinio saugumo laboratorija

1. Tyrimo kontekstas

Šioje dalyje pateiktas tyrimo kontekstas, kuris nustato ir daro įtaką tyrimo eigos gairėms. Kontekstas paremtas tarptautiniais ir nacionaliniais teisės aktais, apibrėžta kvalifikacijų sandaros sąranga, nacionaliniais bei tarptautinės profesinės bendruomenės studijų krypčių aprašais ir gerąja kitų šalių praktika.

1.1. Teisės aktai ir kiti formalūs dokumentai

Europos kibernetinio saugumo centrų ekspertiniame apibrėžimų ir taksonomijos leidinyje [47] pateikiama pakankamai išsami KS srityje naudojamų dokumentų bei apibrėžimų analizė, įskaitant tarptautinių profesinių bendruomenių (IEEE, ACM) klasifikatorius, ISO/ISEC standartus ir ES direktyvas. Šis dokumentas suteikia pagrindą EU lygyje nubrėžti bendras daugiasritines darbinių rolių apibrėžtis, nustatyti pirmines Europos lygiu taikomas kompetencijų sąrangas. ES ir nacionalinis reguliavimas nulemia dalies profesinių rolių standartizavimą atsakomybių požiūriu. Pavyzdžiui, Bendrasis duomenų apsaugos reglamentas (BDAR) [63] darė įtaką duomenų apsaugos pareigūno (DAP) pareigybės įvedimui Lietuvos valdžios institucijoms ir organizacijoms, kurios dideliu mastu tvarko asmens duomenis – BDAR nusako DAP ekspertinių žinių lygį, profesines savybes, funkcijas ir pan.

ENISA organizacija šiuo metu atnaujina Europos kibernetinio saugumo kompetencijų sąrangą (angl. European Cybersecurity Skills Framework, ECSF) [24], užtikrinančią kompetencijų perkeliamumą tarp šalių bei vieningą specialisto rolių bei atsakomybių klasifikavimą. Dokumento rengime dalyvauja ir Lietuvos atstovas iš L3CE centro [41]. ENISA ECSF v0.5 juodraštinėje versijoje išskirtos 12 kibernetinio saugumo specialistų rolės. Kiekvienai iš jų pateikti alternatyvūs pavadinimai, reikalingos

žinios, gebėjimai, atsakomybės ir pan. Rolių sąrašas pateiktas 1.1 lentelėje. *Pastaba: dokumento juodraštis paviešintas 2022 m pavasarį, o galutinį dokumentą planuojama paskelbti 2022 m. rudenį.*

1.1 lentelė. ENISA rolės (parengta pagal [24])

Nr.	Rolės pavadinimas anglų kalba	Rolės vertimas
E1.	chief information security officer (CISO)	vyr. informacijos saugos vadovas
E2.	incident responder	aktyvios pagalbos teikėjas
E3.	legal, policy and compliance officer	teisės, politikos ir atitikties pareigūnas
E4.	threat intelligence specialist	grėsmių žvalgybos pareigūnas
E5.	architect	architektas
E6.	auditor	auditorius
E7.	educator	ugdytojas
E8.	implementer	įgyvendintojas
E9.	researcher	mokslininkas
E10.	risk manager	rizikos valdytojas
E11.	digital forensics investigator	skaitmeninių nusikaltimų tyrėjas
E12.	penetration tester	pažeidžiamumų testuotojas

JAV Nacionalinis standartų ir technologijų institutas (angl. National Institute of Standards and Technology, NIST) sukūrė ir tobulina kompetencijų sąrangą KSS ugdymui (angl. National Initiative for Cybersecurity Education, NIST NICE) [49, 51]. NIST NICE remiasi darbo vietos role, su ja susijusiomis užduotimis (angl. tasks) ir kompetencijomis, žiniomis ir įgūdžiais, reikalingais užduotims atlikti. Šiame modelyje apibrėžta didelė aibė specializuotų rolių, turinčių dedikuotas funkcijas ir gana siaurą specializaciją. Autoriai pabrėžia, kad rolės gali būti sukuriamos, kad tiktų unikalioms situacijoms ir atitiktų kontekstą, bet esamos rolės neturėtų būti perrašomos, siekiant išlaikyti rolių aprašo vientisumą. Vienas iš šio modelio palaikymo tikslų yra vieninga komunikacija tarp skirtingų suinteresuotų šalių, kalbant apie naujos darbo jėgos parengimą ir planavimą.

> Tarptautinėmis kompetencijų sąrangomis siekiama užtikrinti vieningą komunikaciją tarp suinteresuotų šalių – darbuotojų, darbdavių bei ugdytojų.

1.2. Profesinių bendruomenių rekomendacijos

Nepaisant įvairių studijų ir mokslo krypčių įtakos, pasaulyje KS laikomas informatikos dalimi. Vienas žymiausių dažniausiai referuojamų KS ugdymo standartų yra ACM/IEEE Kibernetinio saugumo mokymo programa (angl. ACM/IEEE/AIS SIGSEC/IFIP Cybersecurity Curricular Guideline) [36], apibrėžianti KS discipliną, žinių ir kompetencijų grupes, įskaitant ir į žmogaus ar organizacijos saugumą orientuotas dalis, tokias kaip - žmogaus elgsenos supratimas, tapatybių valdymas, atitiktis teisiniam reguliavimui. Lietuvoje KS nėra išskirtas studijų krypčių klasifikatoriuje [43].

Europos e-kompetencijų sąranga (angl. European e-Competence framework) [34] verslo subjektams

pritaikyta vertinti IT kvalifikacinius lygmenis ir grupuoti kompetencijas. Pavyzdžiui, informacijos saugos specialistas yra IT rolė, užtikrinanti organizacijos saugumo strategiją, o jai priklausytų tokios užduotys kaip mokymų rengimas saugumo tematika, grėsmių vertinimas ir pan. Šioje sąrangoje bazinė dimensija yra formuojama per veiksmą – planuoti, kurti, vykdyti, įgalinti, valdyti ir per jas sudėliota 41 kompetencija. Šia sąranga remiasi ir ENISA modelis.

1.3. Kvalifikacijų lygiai ir sandara

Europos kvalifikacijų sąranga (angl. European Qualification Framework, EKF) [60] švietimo sistemoje yra taikoma apibrėžti kvalifikacinius lygmenis grupuojant kompetencijas. Aukštojo mokslo ir studijų lygmenims numatytos kompetencijos atitinka 6 lygmenį (bakalauro studijos), 7 lygmenį (magistrantūros studijos) ir 8 lygmenį (doktorantūros studijos). Lygmenys yra aprašomi pagal žinių, kompetencijų, autonomijos ir atsakomybių lygmenis. Pavyzdžiui, strateginis valdymas minimas prie 7 lygmens. Lietuvos kvalifikacijų sandara yra suderinta su Europos kvalifikacijų sandara.

Aukštosios mokyklos rengia ir/arba tobulina studijų krypties programas pagal studijų krypčių aprašus [11], viešinamus Studijų kokybes vertinimo centro internetiniame puslapyje ir patvirtintus Lietuvos Respublikos Švietimo, Mokslo ir Sporto ministrės(-o). Kaip minėta 1.2 skyriuje, KS nėra išskirtas studijų krypčių klasifikatoriuje. Atliekant studijų krypčių aprašų (53) analizę ir dokumentuose ieškant su kibernetiniu saugumu susijusių žodžių, tokių kaip - kibernetinis saugumas, kibernetiniai incidentai, kibernetinė erdvė, elektroninės informacijos sauga ir pan., atitinkami raktiniai žodžiai buvo rasti tik viename studijų krypčių grupės apraše – Informatikos mokslų [10], taigi su KS siejamos kompetencijos pasidengia informatikos kryptimis. Apraše teigiama, kad *„žinių branduolį sudaro šios žinių sritys: (...), informacijos ir informacinių technologijų sauga, apimant ir kibernetinio saugumo (...) aspektus (...)”*. Apraše yra išskiriamos keturios studijų kryptys – informatikos mokslų, informatikos inžinerijos, informacijos sistemų ir programų sistemų. Trijose iš keturių krypčių yra minima kokias kibernetinio saugumo žinias turi įgyti studentas.

1. Informatikos studijų kryptis *„apima šias pagrindines teorines ir praktines žinių sritis: (...),informacijos ir informacinių technologijų sauga (...).”*
2. Informatikos inžinerijos studijų kryptis – *„gilinamasi į informatikos ir elektronikos metodų, inžinerinės veiklos principų bei technologijų taikymą kompiuterinių sistemų ir tinklų projektavimo, įgyvendinimo, palaikymo, plėtros, tikrinimo bei vertinimo veiklose, taikant (...) saugos, apimant ir kibernetinio saugumo, reikalavimus ir kriterijus.”*
3. Informacijos sistemų studijų kryptis *„apima šias pagrindines teorines ir praktines žinių sritis: (...), informacijos saugą.”*

Atliekant studijų krypčių aprašų analizę taip pat buvo rasta, kad dešimtyje (teises, verslo, statistikos, socialinio darbo, slaugos ir akušerijos, reabilitacijos, mitybos, etnologijos ir folkloristikos, ekonomikos,

burnos priežiūros) iš 53 aprašų raktažodžiai, susiję su kibernetiniu saugumu, buvo įvardinti kitokia formuluote. Dažniausiai tai buvo įvardijama kaip gebėjimas *„naudotis šiuolaikinėmis informacinėmis technologijomis, tinkamai elgtis su konfidencialia informacija"*. Tokį apibrėžimą galima priskirti prie vieno iš anksčiau paminėtų raktažodžių – elektroninės informacijos sauga. Likusiuose 42 studijų krypties aprašuose nebuvo įvardijamas nė vienas raktinis žodis susijęs su kibernetiniu saugumu.

> Kibernetinis saugumas nėra studijų kryptis, o kibernetinio saugumo kompetencijos dalinai padengiamos informatikos mokslų studijų krypčių apraše, nurodytos abstrakčiu lygmeniu. Keliuose kituose aprašuose minimi gebėjimai tinkamai elgtis su konfidencialia informacija ir naudotis informacinėmis technologijomis.

Lietuvos profesijų klasifikatoriaus (LPK) Lietuvos profesijų klasifikatoriaus (LPK) versija LPK 2012 yra parengta pagal Tarptautinį standartinį profesijų klasifikatorių ISCO-88 [33] ir yra viešai pasiekiama priemonė [42] sistemiškai pateikianti profesijų hierarchiją ir aprašus. Lietuvos profesiniame klasifikatoriuje ieškant su kibernetiniu saugumu sietinų ir naudojamų raktinių žodžių, jie randami tik septyniose profesijose, kurios pateikiamos 1.2 lentelėje. Pavyzdžiui, Informacinių technologijų ir ryšių paslaugų srities vadovai be visų kitų funkcijų yra atsakingi ir už IRT sistemų saugumo priežiūrą.

Lietuvos profesijų klasifikatoriaus perkeliamumą užtikrina Europos komisijos valdomas ESCO (angl. European Skills, Competences, Qualifications and Occupations) klasifikatorius [61], kuriame apibrėžiamos su kibernetiniu saugumu sietinos darbinės profesijos, žinios ir įgūdžiai. LPK klasifikatoriaus 1.2 lentelei ekvivalenti yra ESCO klasifikatoriaus 1.3 lentelė su apibrėžtomis profesijomis (originalo kalba).

Svarbu atkreipti dėmesį, kad pavyzdžiui saugumo inžinieriaus rolei (orig. ICT security engineer) ESCO pateikia alternatyvas security architect, security advisor, security consultant, kurios ENISA modelyje yra visiškai skirtingos rolės.

> Lietuvos profesijų klasifikatorių reikia atnaujinti, atsižvelgiant į dabartines darbo rinkos tendencijas ir pasinaudojant tarptautiniais standartais.

1.4. Formalusis ir neformalusis ugdymas

Kibernetinio saugumo švietimas Lietuvoje paremtas ne tik formaliuoju ugdymu aukštosiose mokyklose. Didelę dalį kompetencijų specialistai ir pradedantieji įgyja ir tobulina dalyvaudami užsienio šalių rengiamuose dirbtuvėlėse, mokymuose, sertifikavimo kursuose. Pavyzdžiui, lietuviai dalyvauja tarptautinėse pratybose NATO CCDCOE Locked Shields. Lietuvoje yra rengiamos kibernetinio saugumo pratybos Kibernetinis skydas (Nacionalinis kibernetinio saugumo centras NKSC) ir Gintarinė migla (Lietuvos kariuomenė), kuriose savo bendradarbiavimo, procedūrinius ir technologinius įgūdžius

1.2 lentelė. Lietuvos profesijų klasifikatoriuje randamos profesijos su KS raktažodžiais

Kodas	Klasifikacija hierarchijoje	Pavadinimas
133	Vadovai (1) | Gamybos ir specializuotų paslaugų srities vadovai (13) | Informacinių technologijų ir ryšių paslaugų srities vadovai (133)	Informacinių technologijų ir ryšių paslaugų srities vadovai
1330	Vadovai (1) | Gamybos ir specializuotų paslaugų srities vadovai (13) | Informacinių technologijų ir ryšių paslaugų srities vadovai (133) | Informacinių technologijų ir ryšių paslaugų srities vadovai (1330)	Informacinių technologijų ir ryšių paslaugų srities vadovai
25	Specialistai (2) | Informacinių technologijų ir ryšių sistemų specialistai (25)	Informacinių technologijų ir ryšių sistemų specialistai
252	Specialistai (2) | Informacinių technologijų ir ryšių sistemų specialistai (25) | Duomenų bazių ir tinklų specialistai (252)	Duomenų bazių ir tinklų specialistai
2521	Specialistai (2) | Informacinių technologijų ir ryšių sistemų specialistai (25) | Duomenų bazių ir tinklų specialistai (252) | Duomenų bazių projektuotojai ir administratoriai (2521)	Duomenų bazių projektuotojai ir administratoriai
2529	Specialistai (2) | Informacinių technologijų ir ryšių sistemų specialistai (25) | Duomenų bazių ir tinklų specialistai (252) | Kitur nepriskirti duomenų bazių ir tinklų specialistai (2529)	Kitur nepriskirti duomenų bazių ir tinklų specialistai
3514	Technikai ir jaunesnieji specialistai (3) | Informacinių ir ryšių sistemų technikai (35) | Informacinių technologijų ir ryšių sistemų eksploatavimo ir pagalbos jų naudotojams technikai (351) | Saityno technikai (3514)	Saityno technikai

1.3 lentelė. ESCO rolės susijusios su KS kompetencijomis

Kodas	Klasifikacija hierarchijoje	Pavadinimas
1219.1.2	Managers | Administrative and commercial managers | Business services and administration managers | Business services and administration managers not elsewhere classified | business service manager	security manager
2529	Professionals | Information and communications technology professionals | Database and network professionals | Database and network professionals not elsewhere classified	
2529.1		chief ICT security officer
2529.2		digital forensics expert
2529.3		embedded systems security engineer
2529.4		ethical hacker
2529.5		ICT resilience manager
2529.6		ICT security administrator
2529.7		ICT security engineer
2529.8		ICT security manager
5414.1.8	Service and sales workers | Protective services workers | Protective services workers | Security guards | security guard	security consultant (*Physical security*)

tobulina suinteresuotos pusės ir ypatingos svarbos infrastruktūros specialistai. Aukštosios mokyklos rengia dirbtuvėles, pavyzdžiui, DELTA1 (KTU) ir VU Cyberthon (VU KnF).

Kaip minėta anksčiau, pagal teisinę bazę Lietuvos KS mokymų lauke veikia aukštosios mokyklos, studijų programose tiesiogiai ar daline apimtimi ugdančios kibernetinio saugumo kompetencijas.

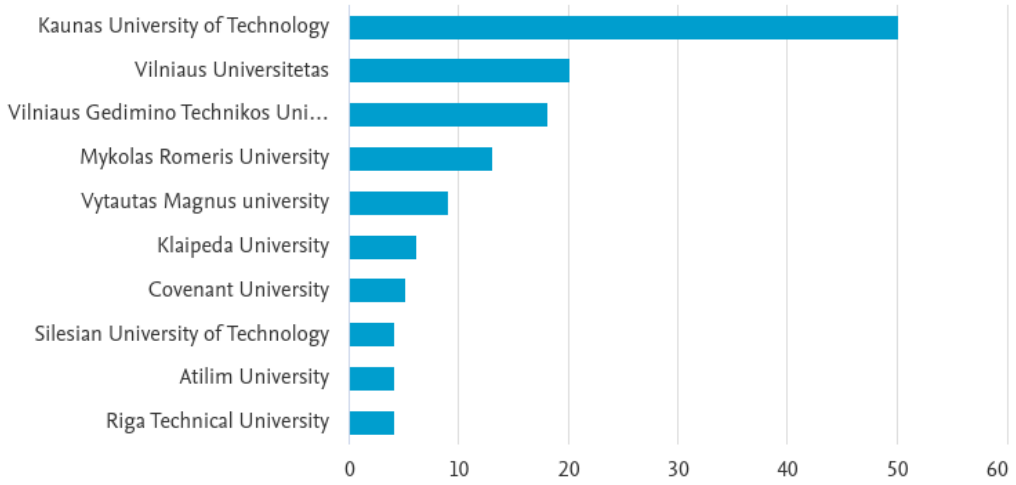
- **Magistro**:
  - *Informacijos ir informacinių technologijų sauga*, **informatikos inžinerijos** mokslų magistras, Kauno technologijos universitetas.
  - *Kibernetinio saugumo valdymas*, **verslo vadybos** mokslų magistras, Mykolo Romerio universitas.
  - *Informacijos ir informacinių technologijų sauga*, **informatikos inžinerijos** mokslų magistras, Vilnius Tech.
  - *Kompiuterinis modeliavimas*, **Informatikos** mokslų magistras, Vilniaus universitetas.
- **Bakalauro**:
  - *Informatikos*, **informatikos** mokslų bakalauras, Kauno Technologijos universitetas.
  - *Kibernetinio saugumo vadyba*, **verslo vadybos** mokslų bakalauras, Mykolo Romerio universitas.
  - *Informatikos sistemos (Informacinių technologijų mokymo specializacija)*, **Informatikos** mokslų bakalauras, Vytauto didžiojo universitetas.
  - *Informacijos sistemos ir kibernetinė sauga*, **informatikos inžinerijos** mokslų bakalauras, Vilniaus universitetas.
  - *Informacinės technologijos*, **Informatikos** mokslų bakalauras, Vilniaus universitetas.
  - *Informacijos sistemos*, **Informacinių** mokslų bakalauras, Vilnius Tech.
- **Profesinio bakalauro**:
  - *Kibernetinės sistemos ir sauga*, **Informatikos mokslų** profesinis bakalauras, Kauno kolegija.
  - *Informacijos sistemos*, **Informatikos mokslų** profesinis bakalauras, Vilniaus kolegija.
- Kitos neformaliojo švietimo programos ir kursai:
  - *Duomenų apsaugos pareigūno kursai*, Kazimiero Simanavičiaus universitetas.
  - Kibernetinio saugumo pagrindai, Hack IT to Defend IT, Hack IT to Defend IT: web applications, Etiškasis hakeris-praktikas, Saugus programavimas ir t.t., Kibernetinio saugumo akademija.
  - *Kibernetinio saugumo kursai*, LCC International universitetas.
  - *Įvadas į Cyber security*, Vilnius coding school.
  - Kibernetinio saugumo mokymai, Vilniaus universitetas.

1.5. Mokslo grupės ir atliekami tyrimai

Moksliniai tyrimai atliekami keturiuose akademiniuose centruose (laboratorijos ir mokslininkų grupėse) – didžiuosiuose Lietuvos universitetuose ir jų rezultatai publikuojami Clarivate Web Of Science ir Scopus indeksuojamuose leidiniuose:

- Kibernetinio saugumo mokslo grupė, Kauno technologijos universitetas.
- Saugumo tyrimų laboratorija, Mykolo Romerio universitetas
- Kibernetinio saugumo laboratorija (Vilniuje) ir kibernetinio saugumo tyrimų grupė (Kaune), Vilniaus universitetas.
- Informacinių technologijų saugos laboratorija, Vilnius Tech.

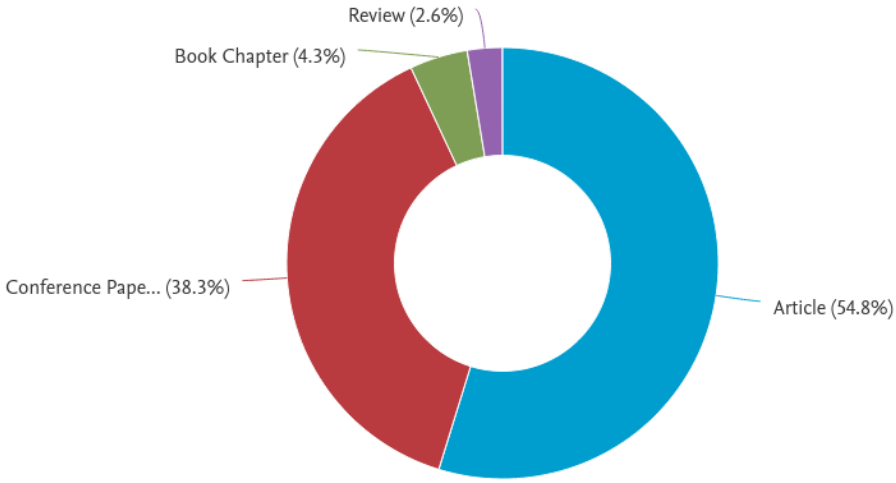
Pagal Scopus indekse registruotus KS srities mokslo darbus 1.1 paveikslėlyje pateikiami top Lietuvos



1.1 pav. Publikacijų skaičius KS srityje pagal Scopus duomenų indeksą (mokslo darbai 2017–2022)

universitetai ir bendraautorių afilijuoti universitetai. Institucijų mokslininkų grupės aktyviai viešina mokslinę produkciją, kuria inovacijas ir dalyvauja nacionaliniuose ir tarptautiniuose projektuose. Lietuvos mokslo tyrimai kibernetinio saugumo tematika viešinami dažniau žurnaliniuose leidiniuose 1.2 pav. (straipsnis, angl. Article (54,8 proc.)). Pagal Lietuvos mokslo vertinimo kriterijus, mokslo rezultatų viešinimas žurnaliniuose leidiniuose rodo aukštos kokybės ir ilgalaikę vertę turinčius tyrimus.

Svarbu pabrėžti, kad mokslininko pareigybėms minimalius kvalifikacinius reikalavimus pagal mokslų sritis nustato LMT pirmininko įsakymu, o dėstytojo, atliekančio mokslinę veiklą, kvalifikaciniai reikalavimai yra reglamentuoti aukštosiose mokyklose.



1.2 pav. Publikacijų skaičiaus KS srityje klasifikavimas 2017–2022 pagal Scopus duomenų indeksą

1.6. Organizacijos veikiančios KS lauke Lietuvoje

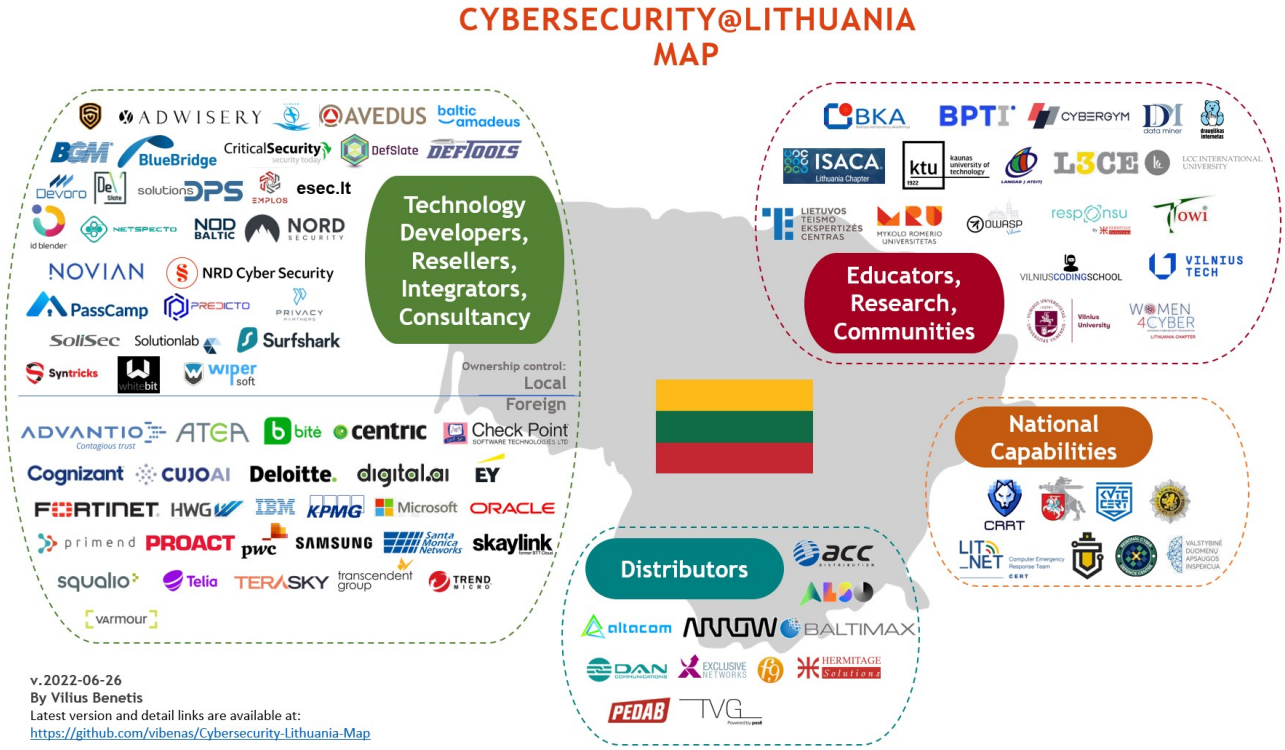
Įmonių, veikiančių Lietuvoje ir turinčių ryškias kibernetinio saugumo dimensijas, žemėlapis [3] pateiktas 1.3 pav. Žemėlapyje pateikiamos mokslo ir švietimo formalios ir neformalios iniciatyvos, organizacijos bei grupės (viso 20), prisidedančios prie kibernetinių specialistų ugdymo bei mokslinių tyrimų, o taip pat Lietuvos ir tarptautinio kapitalo įmonės – technologijų diegėjai, sistemų vystytojai, integratoriai, tiekėjai, paslaugų teikėjai bei saugumo sistemų konsultantai (viso 69). Sudarytame organizacijų žemėlapyje autorius, Vilius Benetis, pateikia ir tas nacionalines organizacijas, kurios turi kibernetinio saugumo kompetencijų, dalyvauja kibernetinių incidentų valdyme, kibernetinės politikos formavime.

1.7. Tarptautiniai projektai, iniciatyvos ir užsienio šalių geroji praktika

1.7.1. Projektai ir gerosios patirtys

EU projektas SPARTA [57] (dalyvauja ir lietuviai) sudarė KS kompetencijų žemėlapį pagal NIST NICE kaip jo dalį (angl. fork), sugretindami su KS taksonomija [47]. O projektas ECHO [22] išskyrė mokymosi rezultatų grupes, sudarydami treniravimo programas pagal veiklos sektorius, o lietuvių inicijuoto projekto metu [15] yra sudarytas sąrašas modulių su mokymosi siekiniais, siekiant kovoti *phishing* atakomis, dėl kurių dažnai nukenčia gyventojai. Lietuvių inicijuotas ketverių metų Erasmus+ projektas (2020–2024) REWIRE siekia sukurti Europos kompetencijų ugdymo karkasą (angl. blueprint) pagal EU projektus SPARTA, ECHO ir kt. Projekte dalyvauja 25 partneriai, ir jiems skirtas beveik 4 mln. eurų biudžetas.

Nacionalinės KS strategijos turi derėti su edukacinėmis programomis [1], o strateginių tikslai



1.3 pav. Lietuvoje veikiančių kibernetinio saugumo organizacijų laukas [3]

smarkiai įtakoja studijų programų dizainą siekiant tvarumo nacionaliniu lygiu. Suomija, kaip ir Lietuva yra maža šalis. Viešoje medžiagoje pabrėžiamas Suomijos viešojo ir privataus sektoriaus bendradarbiavimas, aukščiausio lygio mokslas tiksliniuose sektoriuose ir inovacijos, kurių kūrimą įtakoja stipri į IRT orientuota ekosistema, todėl visam pasauliui siūlo KS sprendimus [8], kurie didina atsparumą skaitmeninėje erdvėje. Visapusis suomių KS modelis [9] remiasi penkiomis dimensijomis (politinė, karinė, ekonominė, technologinė ir visuomenės) bei aštuoniomis sritimis (tarp jų yra švietimas, samprata, tarptautinis bendradarbiavimas ir pan.), jie KS mato ne kaip naštą, bet galimybę. Prieš kelerius metus Danijoje [17] buvo išskirtos trys sritys, svarbios šalies KS lygmens stiprinimui. Viena iš krypčių yra KS kompetencijos, o šiai sričiai gerinti privaloma įtraukti KS į bendrąjį išsilavinimą, reguliuoti reikalavimus organizacijų mokymams, gerinti bendrąjį KS supratimą, investuoti į mokslinius tyrimus (tam tikros specifinės kryptys) bei didinti tarpsektorinį bendradarbiavimą. Kitos sritys – saugus šalies skaitmeninis perimetras ir saugumas pagal nutylėjimą kuriant produktus (angl. security by design). Praėjus keleriems metams [27] dar labiau buvo išskirtas siekis bendradarbiauti (tarp sektorių ir tarp šalių) bei visuomenės švietimas, kompetencijas ugdant nepriklausomai nuo amžiaus, taip pat įtraukiant naujus ugdymo modulius aukštojo mokslo institucijose ir didinant dėmesį mokslo ir studijų aplinkose.

> Mažos šalys rūpinasi KS ekosistemos vystymu nuo politinio lygmens iki visuomenės supratimo apie KS.

1.7.2. Kibernetiniai šauktiniai

Kibernetiniai šauktiniai yra gana naujas reiškinys ir nėra bendros šios sąvokos apibrėžties. Kibernetiniai šauktiniai gali atlikti įvairias funkcijas, įskaitant techninio kibernetinio saugumo ir kibernetinės gynybos, taip pat rūpintis bendrąja IT parama, programavimu ar sistemų kūrimu. Tarptautinis gynybos ir saugumo centras Estijoje atliko kibernetinių šauktinių šešiose šalyse (Danijoje, Estijoje, Suomijoje, Norvegijoje, Švedijoje ir Šveicarijoje) studiją [31]. Tyrimas parodė, kad šiuo metu nėra susiformavusio vieningo kibernetinių šauktinių modelio, tačiau ginkluotosios pajėgos (ir net valstybė) potencialiai iš to gali turėti labai daug naudos.

> "Kibernetiniai šauktiniai" galėtų būti didelis išteklius sprendžiant kibernetinio saugumo specialistų trūkumo problemą.

Pavyzdžiui, Švedijoje kibernetiniai šauktiniai iš pradžių yra apmokomi ginti ir prižiūrėti kompiuterines sistemas, o tarnybos pabaigoje jie paskiriami į įvairias valstybines institucijas – muitinę, pasienio apsaugos tarnybą, policiją ar kritinės infrastruktūros organizaciją, kuriose trūksta specialistų. Tokiu būdu sprendžiamas KS specialistų trūkumo klausimas. Kaip tiksliai yra panaudojami kibernetiniai šauktiniai labai priklauso nuo konkrečios šalies šauktinių strategijos. Suomijos (ir panašiai Estijos bei Šveicarijos) tikslas – užpildyti gausaus rezervo gretas, tačiau nežiūrint visuotinio šaukimo suomiai koncentruojasi į kokybę, o ne kiekybę, todėl per metus į kibernetinius šauktinius gali paimti dvidešimt naujų karių, jei jie tinkami, arba apsiriboti vos dviem, jeigu kiti neatitinka kriterijų. Danų tikslas – užpildyti profesionalų gretas kariuomenėje, todėl kibernetiniai šauktiniai yra priemonė pritraukti būsimus karininkus ar puskarininkius. Austrai (studijoje neaprašyti, duomenys paimti iš asmeninių susirašinėjimų) kibernetinius šauktinius naudoja kaip "rankas" žvalgybai (OSINT). Nežiūrint skirtingų būdų ir modelių, kibernetinių šauktinių nauda yra akivaizdi, tad mūsų tyrime atkreipsime dėmesį ir į šį klausimą.

2. Tyrimas

Šioje dalyje pateikiami KS lauko tyrimą įtakojančios taksonomijos bei tyrimo dizainą apibrėžiantys etapai, tyrimo patikimumo ir etikos principai, duomenų rinkimo instrumentai ir duomenų analizės įrankiai, kurie taikomi gaunant rezultatus, pagal kuriuos bus sudaromas KS kompetencijų modelis.

Tiriant KS specialistų kompetencijų poreikį buvo vadovautasi Profesinės veiklos lauko tyrimo metodika [4], parengta Lietuvos aukštojo mokslo sistemoje diegiant Europinę kreditų perkėlimo ir kaupimo (ECTS) sistemą ir pilotuota bei pritaikyta identifikuojant aštuonių studijų krypčių bendrąsias ir dalykines kompetencijas, įskaitant Informatikos studijų kryptį. Profesinio lauko tyrimo (*toliau – PLT*) metodika pasirinkta, nes *„suteikia argumentų įvertinti atitinkamų kompetencijų ugdymo svarbą(...)“*.

Šio tyrimo metu metodikos taikymas buvo išplėstas, neapsiribojant tik dokumentų analize (KS veiklos klasifikatoriai) ir darbdaviais (viešojo ir verslo sektorių įmonių vadovai), bet įtraukta ir specialistų grupė. Kadangi KS yra besivystanti ir specializuota informacinių technologijų profesijų sritis, numatyta ir įvairių visuomenės grupių apklausa siekiant išsiaiškinti įvairių socialinių grupių santykį su KS.

KS lauko kompetencijų žemėlapio sudarymo seka:

1) pirminio KS lauko veiklų sąrašo sudarymas, pasitelkiant dokumentų analizės rezultatus;
2) veiklų, kurioms reikia KS kompetencijų, įtraukimas į planuojamus tyrimus siekiant nustatyti, ar KS rinkoje įvardintos rolės / veiklos / kompetencijos yra atpažįstamos (organizacijų vadovų ir specialistų tyrimas), kokios yra dominuojančios veiklų sritys;
3) žinių ir gebėjimų, kurie yra reikalingi KS srityse įvairiose rolėse, nustatymas (ekspertinis ir fokusuotų grupių tyrimas);

4) KS kompetencijų žemėlapio projekto parengimas.

Aukštojo mokslo sistemoje ugdymo tikslams kompetencijų sąrašas yra pradinis etapas, leidžiantis nustatyti studijų pakopą, studijų programų išskirtinumus bei pačią studijų kryptį ar krypčių persidengimus, kurie turi atitikti teisinį reguliavimą.

KS sritis (žr. 1 skyrių) yra įtakojama kelių mokslo sričių, todėl mes žemėlapį konstruosime atsižvelgdami į sritis ir susijusias veiklas, nenuleisdami iki kompetencijų lygmenų. Visų pirma, išryškinant veiklos sritis naudojama schema, pateikta 2.1 lentelėje.

2.1 lentelė. Su kompetencijomis sietinų veiklų atrinkimo principas

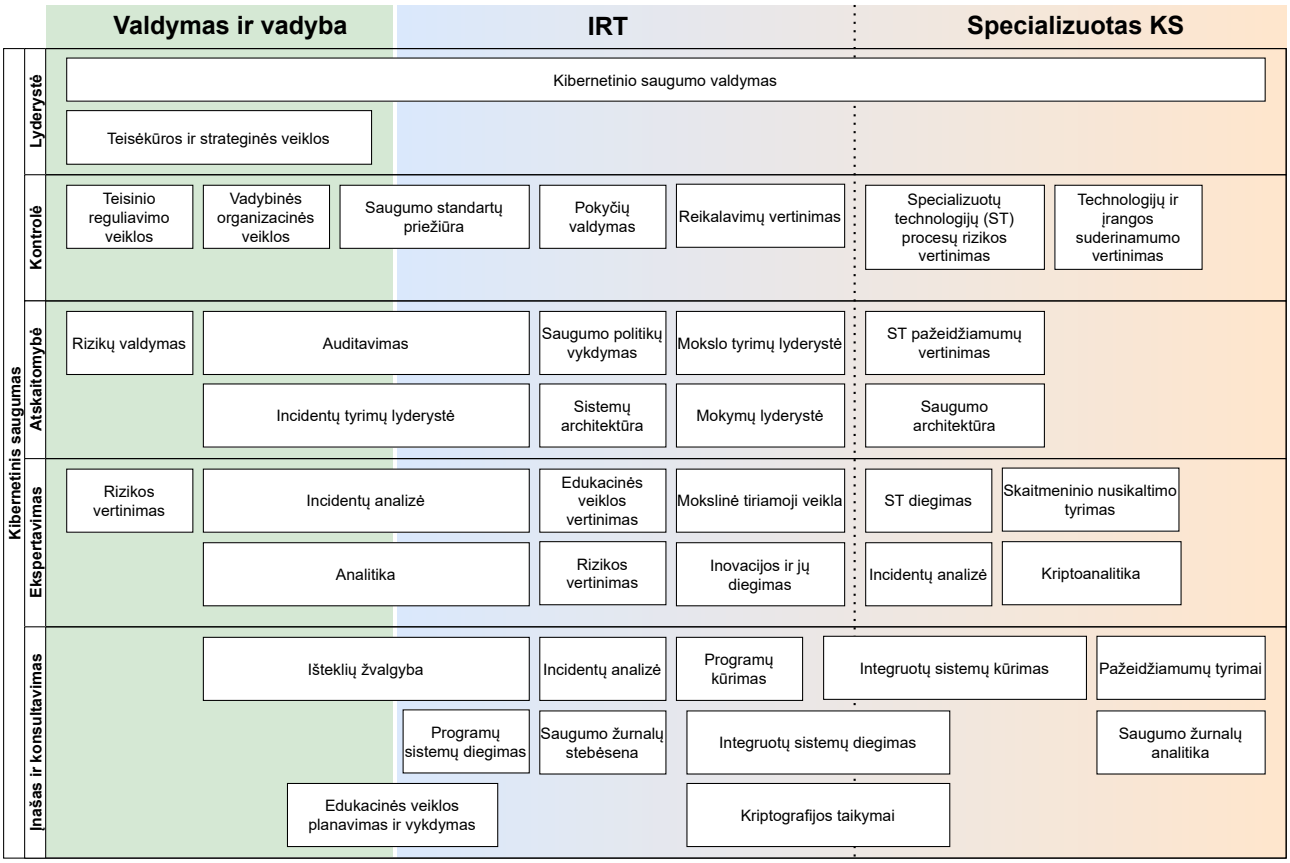
KS dalykinė sritis	Darbuotojo veiklos (rolės) lygmuo	KS veikla
1. Dalykinė sritis	Veiklos (rolės) lygmuo	1. Veikla
2. Dalykinė sritis	Veiklos (rolės) lygmuo	1. Veikla 2. Veikla 3. Veikla
3. Dalykinė sritis	Veiklos (rolės) lygmuo	1. Veikla
...	...	...

Šiuolaikinio aukštojo mokslo sistema neapsiriboja tik dalykinių kompetencijų ugdymu ir akcentuoja bendrąsias kompetencijas, kurios suprantamos kaip perkeliamieji ar universalūs gebėjimai, svarbūs bet kurioje veikloje ir gali padėti asmeniui būti mobiliu tarp įvairių veiklos sričių. Taigi šiuo tyrimu taip pat siekiama nustatyti bendrųjų kompetencijų poreikį ir sudaryti jų sąrašą.

Atsižvelgiant į tai, kad KS yra besiformuojantis ir nuolat kintantis profesinis laukas KS kompetencijų žemėlapį struktūrizuojame pagal kompetencijų tipus ir sritis, veiklų lygmenis ir atsakomybes organizacijose (žr. 2.1 pav.), veiklas surinkdami ir jungdami iš profesinių bendruomenių rekomendacijų. Pavyzdžiui, saugumo architektūra besirūpinantis specialistas neša didesnę atsakomybę nei pačią architektūrą įgyvendinantis darbuotojas, o taip pat ši veikla užeina už IT architektūros projektavimo ribų kaip KS specifinė veikla. Incidentų analizė paminėta kaip specializuota KS sritis, reikalaujanti technologinių žinių, ir kaip veikla, apimanti vadybą bei IRT, kuri reikalauja užtikrinti kokybišką ir profesionalų incidento valdymo procesą.

2.1. Kompetencijų taksonomijos

Analizuojant kompetencijas, reikalingas veikloms atlikti, svarbu identifikuoti jų lygmenis. Bloom [38] lygmenys nusako, ką besimokantysis turi pasiekti mokymosi metu ir arba specialistas turi būti pasiekęs atliekant veiklą. Bloom taksonomijos lygmenų patogi naudoti ir skaidoma sritimis.



2.1 pav. Veiklų skirstymas pagal organizacinius lygmenis ir atsakomybes

- Bloom **pažinimo** sritis apima mokymosi lygmenis bei pasiekimų etapų lygius.
- Bloom **psichomotorinė** sritis apima mokymosi ir taktilinių (mechaninių judesio) veiksmų lygmenis tikslams pasiekti.
- Bloom **emocinė** sritis nusako mokymosi emocinės kokybės lygius, pasirengimu priimti informaciją įsitikinimų, idėjų bei nuostatų integravimu.

Gebėjimams nusakyti ir apibrėžti per pažinimo veiklas įprasta naudoti 6 lygių taksonomiją (žr. 2.2 lentelę, priderintą KS veikloms generalizuotu požiūriu).

2.2 lentelė. Bloom pažinimo srities taksonomijos perkėlimas į KS

	Lygis	Aprašas
BE.1.	Žinoti	**Žinoti**, **prisiminti**, teisingai **įvardinti**, **priskirti** pagrindinius KS konceptus, **atkartoti** apibrėžtis ir sąvokas
BE.2.	Suprasti	**Suprasti**, alternatyviai **paaiškinti**, **perrašyti**, **iliustruoti** pavyzdžiais, **atkartoti** interpretuojant pagal KS kontekstą.
BE.3.	Taikyti	**Taikyti**, **apjungti** KS metodus, **organizuoti** KS procesų vykdymą pagal kontekstą, **numatyti** ir **planuoti** pokyčius
BE.4.	Analizuoti	**Analizuoti**, **lyginti**, **klasifikuoti** KS konceptus, **išskirti** kokybinius parametrus ar rizikas, **nustatytiti** prioritetus, **skaidyti** į subproblemas
BE.5.	Vertinti	**Vertinti**, **palyginti**, **planuoti** KS kontekstą, **valdyti**, **prioretizuoti**, **integruoti** ir **projektuoti** KS procesus
BE.6.	Kurti	**Kurti**, **valdyti**, **matuoti**, **objektyvizuoti**, **kritikuoti** naują KS kontekstą

Lygmuo *Žinoti* – informacijos (teorijų, faktų) pasyvus atgaminimas, pateikimas iš atminties nebūtinai informaciją suvokiant. *Suprasti* – informacijos atpažinimas, paaiškinimas, atvaizdavimas kita forma. *Taikyti* – įgytos žinios (teorijos, taisyklės, dėsniai ir pan.) taikomos įvairiose situacijose. *Analizuoti* – visuma skaidoma į sudėtines nagrinėjamas dalis. *Vertinti* – informacija/duomenys/procesas ir kt. vertinami pagal įvairius parametrus/kriterijus, pateikiamos išvados. *Kurti* – atskiri elementai, dalys jungiami į visumą, sistemą kuriamos santykinai nauji ir kokybiškai kitokie žinių elementai.

Bloom psichomotorinė sritis leidžia nusakyti lygmenis, kuriose yra vyrauja laboratoriniai darbai, inžinerija ar reikalaujama daugiau automatizmo įgūdžių (žr. 2.3 lentelę).

Lygmuo *Imitavimas* – kito asmens elgesio stebėjimas ir šio elgesio kopijavimas. Tai pirmasis etapas, mokantis sudėtingo gebėjimo. IRT srityje toks imatavimas dažnai asocijuojamas su pažingsniniu mokymusi (angl. tutorial) ar instrukcijų "paraidžiui" laikymusi. *Manipuliavimas* – gebėjimas atlikti tam tikrus veiksmus, vadovaujantis nurodymais ir lavinant turimus įgūdžius. *Tikslumas* – besimokantis

2.3 lentelė. Bloom psichomotorinės srities taksonomijos perkėlimas į KS

	Lygis	Aprašas
BP.1.	Imitavimas	mokomųjų veiksmų **pažingsninis vykdymas** KS **komandų**, **įrankių** ir **protokolų** nuoseklus **vykdymas** ir **atkartojimas**
BP.2.	Manipuliavimas	paprastų ar **rašytinių** ir **žodinių instrukcijų laikymasis** su įrankių, komandų, protokolų **pritaikymu** pagal KS kontekstą
BP.3.	Tikslumas	**nepriklausomas** KS konteksto **supratimas** ir tinkamų KS įrankių, komandų ir protoklų paiešką bei jų pirminis **vertinimas** arba **pritaikymas**
BP.4.	Suderinimas	instrukcijų, komandų ar protokolų **perkėlimas** pagal KS kontekstą **taikant reikalavimus** ar jų aibę
BP.5.	Natūralizacija	**laisvas** (**įvaldytas**) įrankių, komandų, ir protoklų KS kontekste taikymas bei naujų sprendimų kūrimas problemai išspręsti

asmuo geba atlikti užduotį, padarydamas keletą klaidų ir tiksliau atlieka veiksmus be pirminio šaltinio įtraukimo. Išsiugdytą gebėjimą parodo sklandus ir tikslus atlikimas. *Suderinimas* – tai gebėjimas derinti keletą veiksmų, susiejant du arba daugiau gebėjimų. Elgsenos modeliai gali būti keičiami, siekiant prisitaikyti prie specialių reikalavimų arba išspręsti problemą. *Natūralizacija* – tai puikus veiklos atlikimas nesąmoningai (negalvojant), pasiektas automatizmo lygmuo. Gebėjimai derinami, veikla atliekama nuosekliai bei lengvai.

Bloom afekto klasifikatorius remiasi žmogaus emocinėmis savybėmis (nuostatos, jausmai, vertybės). Sritis aprėpia klausimus, susijusius su emociniu mokymosi aspektu, pradedant paprastu pasirengimu priimti informaciją ir baigiant įsitikinimų, idėjų bei nuostatų integravimu. Lygmuo *Priėmimas* – pasirengimas priimti informaciją, asmuo suvokia, kad jam privalu būti visuomenišku, pagarbiai išklausyti kitus. *Reagavimas* – asmens aktyvus mokymasis, pavyzdžiui, rodo susidomėjimą, geranoriškai padeda kitiems ir panašiai. *Vertinimas (vertės suteikimas)* – gali būti tik paprastas vertės pripažinimas, bet gali būti ir įsipareigojimo prisiėmimas, pvz., vertina mokslo vaidmenį, rūpinasi kitų gerove, yra jautrus žmogui ir kultūriniams skirtumams. *Vertybinė elgsena* – procesas, kai asmuo susieja skirtingas vertybes, prisiima atsakomybę už savo elgesį, remiasi profesinės etikos standartais, derina elgesį prie vertybių sistemos. *Emocinis stabilumas* – asmuo yra nuspėjamas, turi vertybių sistemą (įsitikinimus, idėjas ir nuostatas), kuria vadovaujasi, pavyzdžiui, asmuo pasitiki savo jėgomis dirbdamas savarankiškai, rodo profesinį įsipareigojimą laikytis etiškos praktikos, išlaiko tinkamą asmeninę, socialinę ir emocinę pusiausvyrą. Tačiau, šie lygmenys taip pat gali turėti KS kontekstinę informaciją ir galima perkelti į KS (žr. 2.4 lentelę).

2.4 lentelė. Bloom afekto srities taksonomijos perkėlimas į KS

	Lygis	Aprašas
BA.1.	Priėmimas	KS kontekste valdomos informacijos, procesų **svarbos** supratimas, **dalinimasis prisitaikant** prie jurisdikcijos
BA.2.	Reagavimas	**Naujų** KS **pažeidžiamumų stebėjimas** bei išankstinis **reagavimas dalinantis** patiritimi ar **užkardant** būsimus pažeidžiamumas **pagal procedūrą**
BA.3.	Vertinimas	**pavojų** ir **rizikų supratimas** bei **realistiškas** situacijos **vertinimas** taikymų **aplikoje**
BA.4.	Vertybinė elgsena	**konfidencialumo**, **privatumo** ir duomenų **apsaugos lygių** supratimas ir **taikymas** kasdieninėje **veikloje**
BA.5.	Emocinis stabilumas	elgsena grįstas KS **procedūrų laikymasis** atsižvelgiant į kontekstą

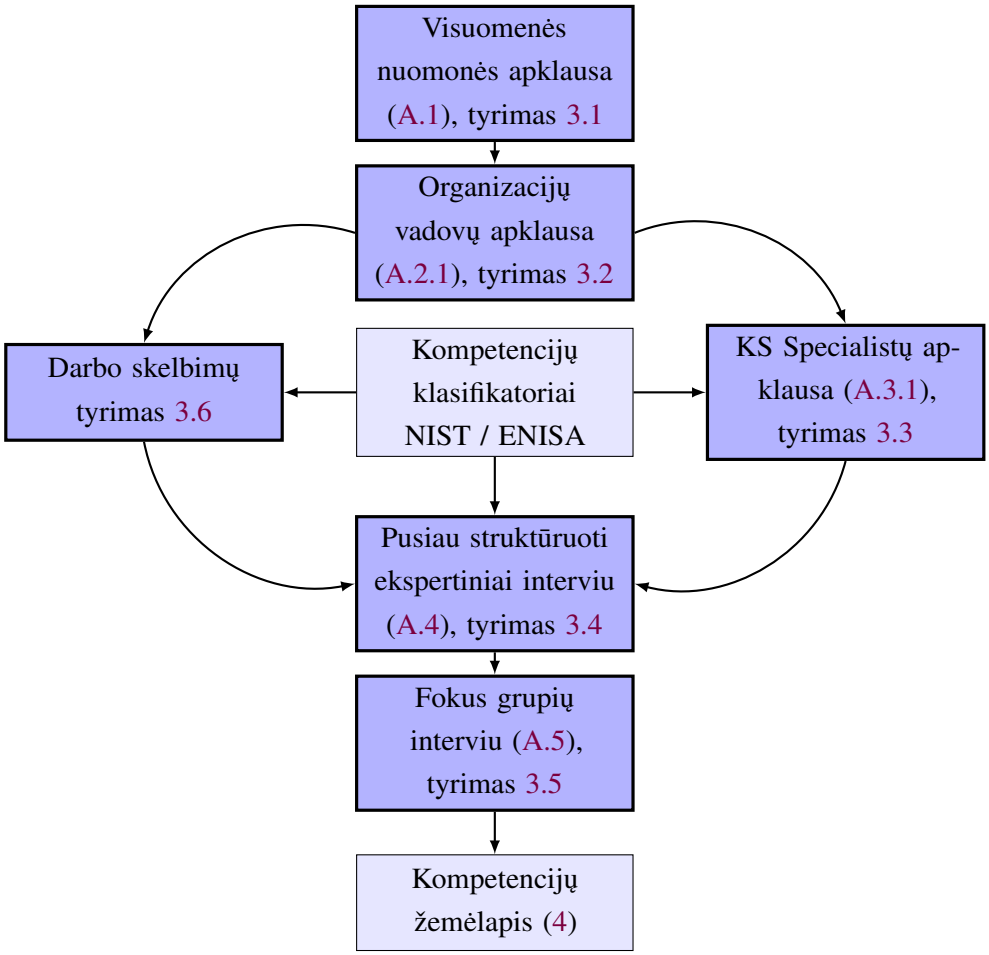
2.2. Tyrimo dizainas ir rezultatų patikimumas

Įprastai PLT atliekamas etapais, kurie gali būti atskiri savarankiški tyrimai. Taigi šiame KS lauko tyrime buvo suplanuoti 6 tyrimai (žr. 2.2 pav.), kurie teikia papildomą gilesnę informaciją apie KS lauką, jame reikalingas kompetencijas ir vykdomas veiklas.

Tyrime buvo taikyta mišri – kiekybinio ir kokybinio – tyrimo metodologija. Ji taikytina siekiant atsakyti pirmąjį uždavinį (atlikti KS lauko tyrimą, vykdant įmonių vadovų ir specialistų apklausas keliuose aktualiuose sektoriuose – krašto apsaugos sistemos, IT, privataus KS, viešojo valdymo bei kituose sektoriuose, kuriuose yra KS kompetencijų poreikis, o taip pat ištirti viešoje erdvėje žiniatinklyje skelbiamus darbo pasiūlymus KS specialistams), kuriame naudojami kiekybiniams ir kokybiniams tyrimams būdingi duomenų rinkimo metodai.

Kiekybinis tyrimas (Omnibus) apėmė ir su kibernetiniu saugumu tiesiogiai kaip profesine veikla nesusijusios populiacijos apklausą (žr. A.1 priedą), kuri padėjo apsibrėžti vyresnių nei 18 metų gyventojų požiūrį į kibernetinį saugumą bei išsiaiškinti, kaip yra suprantamas KS specialisto darbas. Omnibus buvo įgyvendintas kaip reprezentatyvus visuomenės tyrimas, kuriam taikyta atsitiktinė atranka.

Kiekybinės organizacijų vadovų apklausos (žr. A.2.1 priedą) metu buvo siekiama nustatyti organizacijų žmogiškųjų išteklių poreikius kibernetiniam saugumui užtikrinti ir pasiruošti tolimesniam tyrimo etapui su kibernetinio saugumo specialistais (žr. A.3.1 priedą) siekiant išsiaiškinti jų kompetencijų specifikaciją praktikoje. Vadovų apklausos imtį sudarė daugiausia vidutinio ir stambaus verslo įmonių vadovai. Kadangi mus domino segmentas, kuris gali skirti išteklių KS veikloms padengti arba samdyti išorinius paslaugų tiekėjus.



2.2 pav. Tyrimų loginė seka ir jų dermė

Organizacijų vadovų ir specialistų nuomonių tyrimas buvo papildytas darbo skelbimų tyrimu, siekiant nustatyti realią darbo pasiūlos ir paklausos situaciją KS darbo rinkoje.

Kokybinis tyrimas susidarė iš trijų susijusių dalių:

1) kibernetinio saugumo specialistų apklausa (žr. A.3.1 priedas),
2) pusiau struktūruotų ekspertinių interviu (A.4 priedas) ir
3) fokusuotų grupių interviu (A.5 priedas).

KS specialistų buvo prašoma išskirti organizacijoje padengiamas KS veiklas, o taip pat veiklas, kurios perkamos iš išorinių tiekėjų. Veiklų sąrašas buvo parengtas pagal NIST ir ENISA kompetencijų sąrangas. Taip pat buvo prašoma pateikti įžvalgas, kokių KS specialistų reikės ateityje.

Pusiau struktūrizuotų ekspertinių interviu tikslas – patikslinti specialistų apklausos metu surinktus duomenis ir sudaryti rekomenduojamus kelius bei galimybes tapti KS specialistu.

Fokusuotų grupių interviu tikslas – nustatyti moterų karjeros galimybes KS srityje, kai į šią sritį yra įeinama iš kitų veiklos sričių, kurios nesusijusios ar netiesiogiai susijusios su KS. Šis tyrimo etapas buvo įterptas gavus Omnibus rezultatus, kurių metu paaiškėjo KS patrauklumas moterų populiacijai.

Atliekant kokybinį tyrimą surinkta informacija negali pateikti tikslių populiacijos skaičių ar skaitiškai išsakomų koreliacijų, tačiau leidžia atskleisti tendencijas: vyraujančias nuostatas, patirtis, vertybes ir suvokimą kibernetinio saugumo kompetencijų vertinimui.

Kokybiniame tyrime taikyta įvairiausių atvejų atranka, nes interesantų įėjimo galimybės ir keliai į KS sritį gali būti labai įvairūs ir netipiniai.

Kiekybinio tyrimo klausimynai pateikti prieduose (A.1, A.2.1 ir A.3.1). Kokybinio tyrimo klausimų gairės pateiktos prieduose (A.5 ir A.4).

2.2 paveiksle pateikta kiekybinio ir kokybinio tyrimo dalių seka, kurioje pagrindinis apjungiantis konstravimo elementas yra NIST NICE ir ENISA ECSF kompetencijų klasifikatoriai. Jų pagrindu klausimynuose buvo apibūdinamos KS specialistų rolės ir funkcijos, o kokybinio tyrimo etapuose nustatomos galimybės ugdytis KS kompetencijas. Tyrimų rezultate pateikiamas tyrimų įrodymais pagrįstas KS kompetencijų žemėlapis.

Tyrimo validumą užtikrino tai, kad buvo taikoma metodologinė trianguliacija, t.y. buvo taikomi skirtingi duomenų rinkimo metodai: apklausiami klausimyno pagalba organizacijų vadovai, o iš KS darbuotojų duomenys buvo renkami fokusuotos diskusijos ir ekspertinio interviu būdu. KS specialistų rolės buvo identifikuojamos dviem metodais: analizuojant NIST bei ENISA klasifikatorius ir atliekant darbo skelbimų analizę. Visi informantai buvo informuoti apie tyrimo tikslus ir sutiko dalyvauti tyrime.

Kokybinio tyrimo duomenų analizei taikytas kokybinės (angl. content) turinio analizės metodas.

2.2 Tyrimo dizainas ir rezultatų patikimumas

Analizė atlikta Colaizzi [16] metodika. Kokybiniuose tyrimuose įprastai naudojamos apklausos su atvirais klausimais arba laisvos struktūros interviu, siekiant išsiaiškinti, kaip žmonės galvoja ir jaučiasi tam tikrose situacijose, šiuo atveju kibernetinio saugumo samprata organizacijose ar kompetencijų poreikis. Tyrėjas, analizuodamas apklausos ar interviu metu surinktus duomenis, gali taikyti septynis Colaizzi žingsnius.

Išskiriami esminiai tyrimo eigos punktai:

1) skaitomi respondentų atsakymų aprašai ir išskiriant esmines kategorijas pagal „raktinius" žodžius ar minimas koncepcijas bei teiginius;
2) identifikuojami prasminiai elementai, kai kategorijų turinys skaidomas išskiriant jų elementus;
3) prasminiai elementai suskirstomi į subkategorijas;
4) interpretuojami turinio duomenys.

Aprašomosios duomenų statistikos skaičiavimai buvo atlikti naudojantis programomis:

- JASP – Amsterdamo universiteto tobulinamas atvirojo kodo statistikos įrankis.
- GNU PSPP psppire sąsaja – Atvirojo kodo, bendruomenės palaikomas statistikos įrankis.

3. Tyrimo rezultatai

Šioje dalyje pateikiami tyrimo etapų rezultatai, jų aprašomoji statistika ir kokybinė analizė. Tyrimai atlikti pagal 2 skyriuje pateiktą metodiką.

3.1. Omnibus: Visuomenės požiūrio į kibernetinį saugumą tyrimas

Reprezentatyvios Lietuvos gyventojų apklausos metu buvo apklausti 1004 Lietuvos gyventojai, vyresni nei 18 metų. Apklausa buvo vykdoma 2021 m. rugsėjo 17 d. – spalio 3 d. Apklausos tikslas buvo sužinoti gyventojų požiūrį į kibernetinį saugumą bei supratimą apie kibernetinio saugumo specialisto darbo specifiką. Tyrimas buvo atliekamas individualių interviu būdu. Reikminiam tyrimui aktualūs klausimai su galimais atsakymais yra pateikti A.1 priede.

Kiekybiniame reprezentatyviame visuomenės (Omnibus) tyrime taikyta atsitiktinė atranka, apribojant respondentų amžių nuo 18 metų. Ši amžiaus riba svarbi dėl tyrimo apimties apsibrėžimo aukštojo mokslo ir tęstinio ugdymo srityse. Pasirinktas imties dydis (1004 respondentai) apriboja rezultatų paklaidą iki 3,1 proc.

Iš reprezentatyvios apklausos šiame tyrime buvo naudojami šeši klausimai (*Pastaba: tikslios klausimų ir atsakymų formuluotės nurodytos priede*):

K1. Ką manote apie visuomenės švietimą kibernetinių grėsmių klausimu?
K2. Kokias funkcijas atlieka kibernetinio saugumo specialistas?
K3. Pasakykite, kaip sutinkate su teiginiais apie galimybę tapti kibernetinio saugumo specialistu (trys teiginiai).

K4. Kaip manote, kokios mokslo sritys yra svarbios ruošiant kibernetinio saugumo specialistus bei dirbant šioje srityje (keturios sritys)?
K5. Kaip manote, kokia dalis procentais tarp kibernetinio saugumo specialistų turėtų būti moterys?
K6. Jei jus pakviestų tarnauti į kariuomenę, ar jūs norėtumėte tarnauti kaip kibernetinio saugumo šauktinis – dirbti su kompiuteriu ir mokytis ginti kompiuterines sistemas?

Klausimams K1, K2 ir K5 reikėjo parinkti vieną labiausiai respondento požiūriu tinkamą atsakymą. K3 ir K4 klausimams reikėjo vertinti kiekvieną galimą atsakymą nurodytoje skalėje. Į K6 klausimą reikėjo atsakyti taip ar ne, jis buvo skirtas tik šaukiamojo amžiaus respondentams.

3.1.1. Gauti rezultatai

K1 klausimu buvo prašoma išreikšti nuomonę, kiek reikia šviesti visuomenę apie kibernetines grėsmes, ar švietimas pakankamas, ar mokyklose ir universitetuose turėtų būti daugiau mokymų. Buvo penki galimi atsakymai, iš kurių reikėjo pasirinkti labiausiai tinkamą:

M1. Per daug jau mokymų ta tema — daugiau nieko nereikia.
M2. Žiniasklaida apie tai rašo pakankamai, tegu ir toliau tai daro.
M3. Šia tema galėtų būti daugiau mokymų mokyklose ir universitetuose.
M4. Informacijos apie kibernetines grėsmes nepakanka – reikėtų daugiau viešai prieinamų šaltinių ir mokymų ta tema.
M5. Nežino, neatsakė.

3.1 lentelėje kiekvienam atsakymui matoma respondentų nuomonė pagal amžiaus grupes. Reikminiam tyrimui itin svarbūs jaunų (18–25 metų) respondentų atsakymai, nes jie turi šviežiausią patirtį edukacinėje sistemoje. Apie pusę tokio amžiaus respondentų mano, kad mokymų nepakanka (atsakymai M3–M4): 33,3 proc. teigia, kad mokyklose ir universitetuose turi būti daugiau mokymų ir 19,2 proc. teigia, kad reikėtų daugiau mokymų ir viešai prieinamų šaltinių. Nors 26,8 proc. mano, kad žiniasklaida jau pakankamai rašo šiuo klausimu ir toliau taip turėtų tęstis (M2), ir net 10,8 proc. mano, kad informacijos jau per daug (M1). Amžiui didėjant, daugėja ir respondentų, kurie nežino, ką atsakyti, ir tokių, kurie nemano, kad reikia daugiau mokymų mokyklose ir universitetuose. Net 41,7 proc. respondentų virš 65 metų į klausimą neatsakė arba nežinojo, ką atsakyti.

Lyginant moterų ir vyrų atsakymus žymaus skirtumo nepastebėta. Analizuojant atsakymus pagal gyvenamąją vietą bei šeimos ūkio pajamas (žr. 3.2 lentelę), matyti, kad daugiau uždirbantys arba gyventojai miestuose mano, kad informacijos jau pakanka žiniasklaidoje (taip mano 33,8 proc. respondentų iš šeimų, uždirbančių daugiau nei 1501 €, ir apie 28 proc. miesto gyventojų), o kaime 30,9 proc. neatsakė ar nežinojo, ką atsakyti. Didelė dalis respondentų, neatsakiusiųjų apie pajamas mano, kad mokymų galėtų būti daugiau ir jų trūksta (M3–M4). Didelė dalis mažas pajamas turinčių respondentų į klausimą neatsakė.

3.1 lentelė. Atsakymai apie mokymų ir informacijos poreikį pagal amžiaus grupes

K1	**≤ 25**	**26-45**	**46-65**	**Virš 65**	**Iš viso**
M1	10.8%	6.9%	5.2%	3.9%	6.1%
M2	**26.8%**	21.9%	32.1%	22.7%	26.2%
M3	**33.3%**	29.0%	19.6%	13.4%	22.7%
M4	**19.2%**	28.9%	25.9%	18.3%	24.3%
M5	9.9%	13.2%	17.2%	**41.7%**	20.8%
	100.0%	100.0%	100.0%	100.0%	100.0%

3.2 lentelė. Atsakymai apie mokymų ir informacijos poreikį pagal gyv. vietą ir šeimos ūkio pajamas

	Lytis		**Šeimos pajamos**				**Gyvenvietė**			
K1	**Vyras**	**Moteris**	**≤800 €**	**801–1500€**	**≥1501€**	**N/D**	**Kaimas**	**Miestas**	**Didmiestis**	**Iš viso**
M1	7.3%	5.0%	5.4%	8.6%	6.0%	4.4%	7.2%	4.3%	6.2%	6.1%
M2	25.6%	26.6%	22.2%	26.6%	**33.8%**	22.4%	21.5%	**28.5%**	**28.4%**	26.2%
M3	23.9%	21.7%	15.4%	21.1%	26.2%	**27.5%**	18.3%	20.0%	27.7%	22.7%
M4	24.3%	24.4%	21.2%	21.2%	26.3%	**28.1%**	22.2%	26.9%	24.5%	24.3%
M5	19.0%	22.3%	**35.8%**	22.5%	7.7%	17.6%	**30.9%**	20.3%	13.2%	20.8%
Eil. %	45.7%	54.3%	24.0%	24.8%	24.5%	26.8%	32.7%	24.7%	42.6%	100.0%
Stulp. %	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

3.3 lentelėje pateikiami atsakymai, atsižvelgiant į respondentų užsiėmimą. Didžiausia dalis specialistų (30,6 proc.) mano, kad žiniasklaidoje informacijos yra pakankamai. Nors dauguma pasirinko M3–M4 atsakymo variantus, taigi dauguma mano, kad mokymų ir informacijos galėtų būti daugiau. Daugiau nei pusė vadovų (52,4 proc.) identifikavo, kad reikėtų daugiau viešai prieinamų šaltinių ir mokymų apie kibernetines grėsmes. Verslo savininkų didžiausia dalis (39,8 proc.) mano, kad mokyklose ir universitetuose turėtų būti daugiau mokymų apie kibernetinį saugumą. Didžiausia dalis moksleivių ir studentų taip pat pasirinko pastarąjį atsakymą (33,9 proc.), nors beveik ketvirtis mano, kad žiniasklaidoje informacijos yra pakankamai. Tarp pensininkų, bedarbių ir ūkininkų didelė dalis respondentų neatsakė arba nežinojo, ką atsakyti.

3.3 lentelė. Atsakymai apie mokymų ir informacijos poreikį pagal užsiėmimą

K1	**Neatsakė**	**Darbin.**	**Special.**	**Vadov.**	**Ūkinink.**	**Verslo sav.**	**Pens.**	**Moksl., Stud.**	**Namų šeim.**	**Bedarb.**	**Iš viso**
M1		7.0%	5.4%			5.9%	3.9%	7.3%	14.6%	12.3%	6.1%
M2	64.5%	27.2%	**30.6%**	22.5%	16.4%	12.3%	23.6%	**24.1%**	27.4%	25.5%	26.2%
M3		24.9%	27.2%	9.7%	22.9%	**39.8%**	11.4%	**33.9%**	14.7%	28.2%	22.7%
M4	35.5%	24.8%	26.9%	**52.4%**	32.2%	31.7%	18.7%	24.1%	30.4%	14.6%	24.3%
M5		16.0%	9.9%	15.5%	28.5%	10.2%	**42.4%**	10.6%	12.9%	19.4%	20.8%
	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

3.4 lentelėje pateikiami atsakymai pagal išsilavinimą. Lentelės paskutinėje eilutėje agreguoti atsakymai sudedant M3 ir M4 atsakymų pasirinkimus, nes jie rodo mokymų poreikį. Čia išsiskiria magistro laipsnį (58,9 proc.) ir kolegijos aukštąjį išsilavinimą (62,3 proc.) turintys respondentai,

manantys, kad mokymų reikia daugiau. Pusė turinčiųjų bakalauro laipsnį taip pat mano, kad mokymų reikia daugiau, nors 28,6 proc. mano, kad žiniasklaidoje informacijos pakanka, o didelė dalis (16,0 proc.) nežinojo, ką atsakyti, arba neatsakė. Didelė dalis grupėse, kurios reprezentuoja neturinčiuosius aukštojo mokslo išsilavinimo, neatsakė arba nežinojo, ką atsakyti. Bendrai paėmus, Chi kvadrato testas parodė (p<0,001) labai stiprų ryšį tarp šių kintamųjų: kuo aukštesnis respondento išsilavinimas, tuo labiau jis/ji pageidauja mokymų KS tema.

3.4 lentelė. Atsakymai apie mokymų ir informacijos poreikį pagal išsilavinimą

K1	Prad.	Pagr.	Vid.	Prof.	Aukštesn.	Neuni.aukšt.	Bak.	Mag.	Neatsakė	Iš viso
M1		3.6%	9.6%	6.4%	4.5%	7.4%	5.3%			6.1%
M2		24.6%	24.8%	24.2%	30.9%	22.5%	28.6%	29.4%	46.3%	26.2%
M3		12.4%	27.1%	21.0%	22.3%	30.1%	22.3%	21.3%		22.7%
M4		14.4%	18.4%	25.7%	23.8%	32.2%	27.9%	37.6%		24.3%
M5	100.0%	45.0%	20.2%	22.7%	18.6%	7.7%	16.0%	11.8%	53.7%	20.8%
	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
M3+M4:		**26,8%**	**45,5%**	**46,7%**	**46,1%**	**62,3%**	**50,2%**	**58,9%**		**47,0%**

Viešai prieinamų KS mokymų bei mokymų mokyklose ar universitetuose turėtų būti daugiau.

K2 klausimu buvo siekiama ištirti, kaip visuomenė identifikuoja pagrindines kibernetinio saugumo specialisto funkcijas. Kibernetinis saugumas priskiriamas IT sričiai dėl technologinių kompetencijų [36], reikalingų specialistams, tačiau mums rūpėjo išsiaiškinti, ar visuomenės nuomone KS specialisto rolė yra labiau traktuojama kaip įprastinė IT administratoriaus rolė (atsakymas F3), ar visgi kaip atskira rolė (atsakymas F1, kuriame pateiktas gana siauras, reaguotojo į kibernetinius incidentus aprašymas). Kiti du galimi atsakymai (F2 ir F4) mūsų supratimu rodo, kad respondentas nesupranta apie KS specialisto vaidmenį (bet pats to nežino), o penktuoju variantu buvo palikta galimybė neatsakyti arba nežinoti (t.y. respondentas bent jau žino, kad nesupranta):

F1. Stebi kompiuterinių sistemų veiklą ir reaguoja į iškilusius saugumo įvykius.
F2. Kuria žiniatinklio svetaines, puslapius, informacines sistemas.
F3. Prižiūri kompiuterių tinklus, administruoja kompiuterius.
F4. Kuria telefonams skirtas programėles ir / ar kompiuterinius žaidimus.
F5. Nežino, neatsakė.

Buvo tikimasi, kad respondentai identifikuos F1 kaip labiausiai KS būdingą funkciją. Kitos galimybės atitiko kai kurias IT sektoriaus funkcijas. Atsakymas F1 buvo specialiai sukonstruotas taip, kad būtų skatinama jį pasirinkti – jame pavartotas tas pats žodis "saugumo", kaip ir klausime, be to jis pateiktas pirmasis iš galimų variantų, todėl apie respondentus, kurie šio atsakymo nepasirinko, galime teigti, kad jie nėra susipažinę su KS specialisto role.

K2 klausimas apie kibernetinio saugumo specialisto pagrindines funkcijas išryškino (žr. į lentelę 3.5), kad tik šiek tiek daugiau nei pusė (57,9 proc.) pasirinko F1 atsakymą (kaime 47 proc.,

miestuose 57 proc., didmiesčiuose – 67 proc. [37]). Jaunimas (iki 25 metų) nenustebino, iš jų F1 variantą rinkosi palyginti didelė dalis respondentų – 67,6 proc. (kaime 58,9 proc., miestuose 65 proc., didmiesčiuose 77 proc.). Tad bendrai Lietuvos mastu tiksliausi buvo vyrai iki 25 metų (F1 atsakė 70,5 proc.) ir 25-45 metų moterys (69,5 proc.). Taip pat pastebėjome, kad aukštesnis išsilavinimas susijęs su teisingų atsakymų skaičiumi (Chi kvadrato testo p<0.001). Apie 40 proc. vyriausiųjų respondentų neatsakė arba nežinojo, ką atsakyti. Visgi, nemažai respondentų pasirinko F3 atsakymą (12,4 proc.), kuris nurodo bendrines IT administratoriaus funkcijas – taip teigė net 15 proc. jaunų moterų (ir tik 6 proc. jaunų vyrų). Bendrai paėmus, daugiau nei trečdalis Lietuvos gyventojų nežino, kas yra KS specialistas. Taip pat (nežiūrint tendencingai suformuluotų atsakymų) nemaža dalis (virš 12 proc.) gyventojų linkę KS rolę tapatinti tiesiog su IT specialistu. Tai rodo, kad KS rolė visuomenės akyse dar yra pakankamai jauna. Taip pat svarbu pastebėti, kad didesnė dalis jaunų moterų, nei vyrų, yra nesusipažinusi su KS role – į tai turėtų būti atsižvelgta reklamuojant šią sritį.

3.5 lentelė. Atsakymai apie pagrindines funkcijas pagal lytį ir amžiaus grupes

	Vyrai					**Moterys**					Visi
K2	**≤ 25**	**26-45**	**46-65**	**Virš 65**	Visi	**≤ 25**	**26-45**	**46-65**	**Virš 65**	Visos	Iš viso
F1	70.5%	68.4%	60.2%	40.5%	60.9%	63.9%	69.5%	55.4%	37.4%	55.3%	57.9%
F2	2.8%	2.3%	7.8%	6.2%	4.9%	10.5%	8.5%	4.9%	5.4%	6.5%	5.8%
F3	6.1%	13.6%	9.8%	12.5%	11.1%	15.5%	12.3%	13.5%	14.2%	13.5%	12.4%
F4	2.3%	1.5%	1.7%	2.1%	1.8%	3.1%	1.4%	2.1%	1.4%	1.8%	1.8%
F5	18.2%	14.2%	20.5%	38.7%	21.4%	7.1%	8.4%	24.1%	41.5%	22.8%	22.1%

Didelė dalis gyventojų negali identifikuoti pagrindinės KSS funkcijos, tapatindami ją su IT sritimi.

Trečiu klausimu (ir trimis būdais) paklausėme ar lengva tapti KS specialistu – taip mėginome netiesiogiai įvertinti visuomenės lankstumą. Kuo sudėtingesnė ir labiau nepasiekiama atrodo ši rolė, tuo sunkiau atitinkamos grupės žmones pritraukti į KS sritį.

3.6 lentelėje pateikti agreguoti atsakymai į klausimą, ar KS specialistu galima tapti persikvalifikavus iš bet kurios kitos profesijos. Daug vyriausiųjų respondentų (29,0 proc.) ir mažiausiai uždirbančiųjų neatsakė į šį klausimą. Kitose grupėse didžiausia dalis buvo greičiau sutinkančių, amžiaus grupėje iki 29 metų – net 43,0 proc. Statistiškai (Chi kvadrato testas, p<0,001), kuo jaunesnis žmogus, tuo labiau jis linkęs sutikti, kad KS specialistu galima tapti iš bet kurios kitos profesijos. Vis dėlto, reikia atkreipti dėmesį, kad pusė jaunuolių mano, jog ši profesija pasiekiama ne visiems. Akivaizdu, kad jiems trūksta informacijos apie skirtingas KS specialisto roles ir galimybes įvairiausių profilių žmonėms siekti karjeros šioje srityje.

Pagal apklausos duomenis ir amžius neturėtų būti kliūtis KS srities specialistui. Į klausimą, ar kibernetinio saugumo specialistu galima tapti bet kurio amžiaus, beveik pusė atsakė, kad sutinka su teiginiu arba greičiau sutinka (žr. 3.7 lentelę). Grupėje iki 29 metų tokių respondentų buvo virš 58 proc. (47,4 proc. greičiau sutinka ir 10,7 proc. visiškai sutinka). Greičiau sutinka ir vidutines ar didesnes

3.6 lentelė. Atsakymai apie persikvalifikavimą iš bet kurios profesijos

	Lytis		Amžius			Šeimos pajamos				
K3.1	**Vyr.**	**Mot.**	**18–29**	**30–49**	**50+**	**≤800 €**	**801–1500€**	**≥1501€**	**N/D**	**Iš viso**
Visiškai sutinku	10.6%	5.6%	8.0%	10.9%	6.0%	5.1%	8.7%	12.7%	5.3%	7.9%
Greičiau sutinku	34.0%	33.4%	**43.0%**	32.2%	31.5%	28.5%	36.9%	31.5%	37.5%	33.7%
Greičiau nesutinku	23.4%	27.9%	27.9%	28.4%	23.6%	21.6%	25.8%	29.1%	26.8%	25.9%
Visiškai nesutinku	13.0%	9.3%	10.1%	13.2%	9.9%	11.3%	7.7%	13.4%	11.5%	11.0%
N/D	18.9%	23.7%	11.0%	15.2%	**29.0%**	**33.5%**	20.9%	13.3%	18.9%	21.6%

pajamas gaunantys gyventojai. Su amžiumi optimizmas akivaizdžiai slopsta, tačiau tik grupėje virš 50 metų teigiamai mąstančių dalis sumažėja žemiau pusės.

3.7 lentelė. Atsakymai dėl specialistų amžiaus

	Lytis		Amžius			Šeimos pajamos				
K3.2	**Vyr.**	**Mot.**	**18–29**	**30–49**	**50+**	**≤800 €**	**801–1500€**	**≥1501€**	**N/D**	**Iš viso**
Visiškai sutinku	12.8%	8.4%	10.7%	11.9%	9.4%	8.0%	12.1%	16.1%	5.7%	10.4%
Greičiau sutinku	38.4%	36.9%	**47.4%**	37.7%	34.2%	30.4%	**38.9%**	**37.5%**	42.8%	37.6%
Greičiau nesutinku	19.0%	25.7%	21.3%	26.6%	20.6%	19.0%	24.9%	26.8%	19.9%	22.6%
Visiškai nesutinku	11.2%	7.7%	11.2%	10.3%	7.9%	10.8%	6.2%	9.8%	10.2%	9.3%
N/D	18.6%	21.4%	9.4%	13.5%	27.8%	31.7%	17.8%	9.8%	21.3%	20.1%

Į klausimą, ar galima tapti kibernetinio saugumo specialistu mokantis savarankiškai (žr. 3.8 lentelę), tik ketvirtis (26,4 proc.) sutiko, didžiausia dalis respondentų pasirinko greičiau nesutinku (30,8 proc.). Apie pusė respondentų nesutinka ir greičiau nesutinka, ir 23,5 proc. negalėjo atsakyti. Įdomu pastebėti, kad net jaunimo tarpe (šiuo atveju jaunimu pavadinome visus iki 29 metų) neišryškėjo noras mokytis savarankiškai. Nėra ryškių skirtumų ir tarp skirtingas pajamas gaunančių grupių (ir net tarp skirtingose vietovėse gyvenančių). Tai rodo, kad visuomenėje yra tvirtai susiformavusi formalaus išsilavinimo reikšmė, todėl universitetų ir kolegijų vaidmuo pritraukiant naujus KS specialistus yra labai svarbus.

3.8 lentelė. Atsakymai dėl tapimo specialistu mokantis savarankiškai

	Lytis		Amžius			Šeimos pajamos				
K3.3	**Vyr.**	**Mot.**	**18–29**	**30–49**	**50+**	**≤800 €**	**801–1500€**	**≥1501€**	**N/D**	**Iš viso**
Visiškai sutinku	7.7%	4.9%	8.4%	5.6%	5.8%	5.1%	8.0%	9.6%	2.4%	6.2%
Greičiau sutinku	22.3%	18.4%	25.7%	21.8%	17.3%	14.5%	23.0%	21.3%	21.7%	20.2%
Greičiau nesutinku	28.3%	32.9%	32.7%	32.0%	29.4%	26.8%	32.9%	29.8%	33.2%	30.8%
Visiškai nesutinku	20.3%	18.5%	21.6%	23.2%	16.1%	19.5%	13.5%	24.2%	20.1%	19.3%
N/D	21.4%	25.3%	11.6%	17.5%	31.3%	24.1%	22.5%	15.1%	22.7%	23.5%

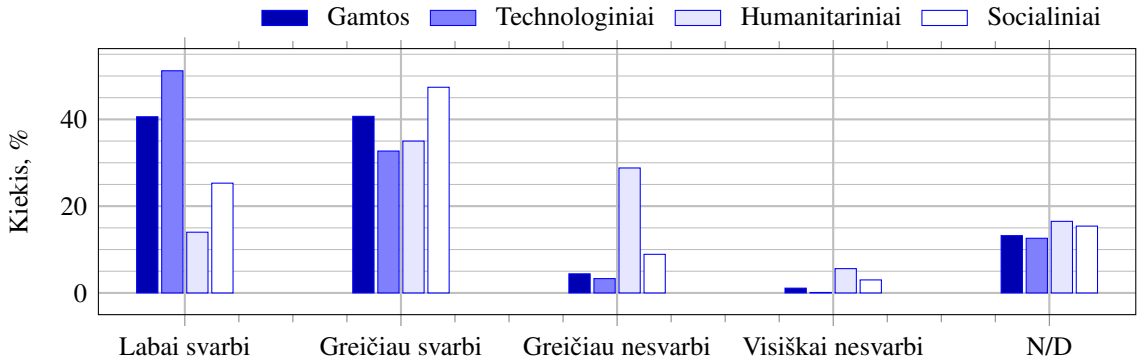
Amžius ar būtinybė persikvalifikuoti nėra kliūtis ateinant į KSS, bet savarankiškas pasirengimas neatrodo realistiškas.

K4 klausimu respondentams buvo pateiktos keturios sritys su mokslo šakomis. Buvo prašoma įvertinti kiekvienos srities svarbą ruošiant KS specialistą keturių verčių skalėje, taip pat su galimybe palikti neįvertintą.

1. Gamtos mokslai (fizika, informatika, matematika)

2. Technologiniai mokslai (informatikos ir elektronikos inžinerija)
3. Humanitariniai mokslai (istorija, filologija, filosofija)
4. Socialiniai mokslai (komunikacija ir informacija, teisė, politikos mokslai, psichologija)

3.1 paveiksle pateikti vertinimai kiekvienai iš sričių. Kaip buvo tikėtasi, respondentai įvardino technologinių ir gamtos mokslų svarbą – virš 80 proc. pasirinko kaip labai svarbius arba greičiau svarbius. Taip pat didelė dalis respondentų socialinius mokslus įvertino kaip greičiau svarbius. Atsakymai rodo vyraujančią nuomonę, kad KS specialistu galima tapti per STEM studijų kryptis. Tai nestebina, tačiau tik dar kartą pabrėžia, kad visuomenę (ir ypač jaunimą) verta informuoti apie mažiau techninės KS specialisto roles (pvz., teisininką, duomenų apsaugos pareigūną, ar fizinių pažeidžiamumų testuotoją), į kurias galima patekti net ir "išsigandus" tiksliųjų mokslų.



3.1 pav. Atsakymai apie mokslo sričių svarbą ruošiant KS

Kibernetinio saugumo srityje dirba iki 11 proc. moterų [23, 68], todėl K5 klausimu apie moterų specialisčių dalį kibernetinio saugumo srityje buvo siekiama sužinoti visuomenės požiūrį į moterų perspektyvą šioje srityje. 3.9 lentelėje pateikiami respondentų atsakymai į šį klausimą. Didelė dalis respondentų nežinojo, ką atsakyti, arba neatsakė (29,6 proc.). Mažiau uždirbantys dažniau neatsakė į klausimą. Didmiesčiuose 44,4 proc. atsakė, kad moterų turėtų būti 30–60 proc.

3.9 lentelė. Nuomonė, kiek turėtų būti moterų tarp kibernetinio saugumo specialistų

	Lytis		**Šeimos pajamos**				**Gyvenvietė**			
K5	**Vyras**	**Moteris**	**≤800 €**	**801–1500€**	**≥ 1501€**	**N/D**	**Kaimas**	**Miestas**	**Didmiestis**	Iš viso
< 30%	28.8%	18.5%	19.7%	25.3%	25.3%	22.4%	21.0%	27.9%	22.1%	23.2%
30–60 %	31.0%	38.7%	32.1%	34.3%	38.8%	35.5%	27.8%	29.1%	44.4%	35.2%
60–90 %	10.9%	10.7%	9.4%	11.0%	12.0%	10.9%	13.6%	10.2%	9.0%	10.8%
> 90 %	0.5%	1.8%	1.7%	0.9%	2.3%		1.1%	3.0%	0.2%	1.2%
Nežino, neatsakė	28.8%	30.3%	37.1%	28.6%	21.5%	31.2%	36.5%	29.7%	24.3%	29.6%

Didžiausia dalis respondentų atsakė, kad turėtų būti 30–60 proc. moterų specialisčių (35,2 proc.). Analizuojant atsakymus pagal lytį ir amžiaus grupes (žr. 3.10 lentelę), matyti, kad moterys, ypač jaunesnės (iki 25 metų ir 25–45 metų), dažniausiai mano, kad moterų turi būti apie pusę (atitinkamai 41,4 proc. ir 45,5 proc. moterų šiose grupėse). Jauniausi vyrai (iki 25 metų) mano, kad moterų turi

būti iki 30 proc. (39,3 proc.), o 26–45 metų amžiaus grupėje vyrauja atsakymas, kad turėtų būti apie pusę (40,5 proc.). Matome, kad pačios moterys linkusios matyti gerokai daugiau moterų KS srityje, negu šiuo metu yra rinkoje. Tai yra gera žinia, kadangi moterų pritraukimas į šią sritį ne tik padėtų spręsti specialistų trūkumo problemą, tačiau padidintų ir patį kibernetinį organizacijų saugumą.

3.10 lentelė. Nuomonė apie moterų kibernetinio saugumo specialisčių kiekį

	Vyrai				**Moterys**			
K5	**$\leq$ 25**	**26–45**	**46–65**	**Virš 65**	**$\leq$ 25**	**26–45**	**46–65**	**Virš 65**
< 30 %	39.3%	25.5%	27.4%	28.9%	11.6%	20.6%	19.3%	17.5%
30–60 %	24.4%	40.5%	32.1%	16.9%	41.4%	45.5%	37.9%	31.8%
60–90 %	9.3%	9.2%	13.7%	10.5%	19.1%	14.0%	9.2%	6.4%
> 90 %	1.8%			1.0%	0.7%	0.6%	3.9%	0.5%
Nežino, neatsakė	25.1%	24.8%	26.8%	42.7%	27.2%	19.2%	29.6%	43.8%

Kibernetinio saugumo specialistų trūkumas yra aktuali problema daugeliui valstybių, įskaitant tų valstybių ginkluotąsias pajėgas, tačiau kai kurios kariuomenės (plačiau žr. 1.7.2 skyrių) jau keletą metų sėkmingai naudoja kibernetinius šauktinius (šauktinius, kurie tarnauja kiber pajėgose) spręsdamos šią problemą. Atsižvelgdami į tai, jauniems (iki 25 metų) respondentams buvo užduotas klausimas, ar jie norėtų tarnauti kibernetiniu šauktiniu, jei būtų pakviesti į karinę tarnybą. 3.11 lentelėje pateikiami agreguoti šio klausimo atsakymai. Iš viso 51,6 proc. atsakė, kad eitų tarnauti kibernetiniais šauktiniais ir 12,5 proc. nežinojo, ką atsakyti arba neatsakė. Tarp vyrų teigiamai atsakė 65,8 proc., tarp moterų – tik 33,1 proc., bet būtų galima teigti, kad gana daug moterų yra neapsisprendusios (neatsakė ar nežinojo net 20,9 proc.). Moksleivių tarpe, sutinkančių buvo dar daugiau – net 82 proc. vaikinų ir 36,5 proc. merginų. Vyrų gyvenamoji vieta atsakymams neturėjo daug įtakos – kuo didesnis miestas, tuo didesnė dalis vyrų norėtų tarnauti KS šauktiniais, tačiau skirtumas buvo nedidelis. Moterų atveju tendencija priešinga ir ryškesnė: kuo didesnis miestas, tuo mažiau moterų norėtų tarnauti KS šauktinėmis – kaime sutiktų net 40 proc., tuo tarpu didmiesčiuose tik 26 proc. Visgi, statistiškai (Chi kvadrato testas) priklausomybė nuo gyvenamosios vietos nėra reikšminga, tačiau yra statistiškai reikšmingai daugiau teigiamai atsakiusių vyrų, negu moterų. Nežiūrint į tai, net trečdalis moterų sutiktų tarnauti kibernetinėmis šauktinėmis, tad į tai ateityje turėtų atsižvelgti kariuomenės rekrūtinimo tarnybos.

3.11 lentelė. Požiūris į galimybę tarnauti kibernetiniais šauktiniais

	Vyrai				**Moterys**				Visi
	Kaimas	**Miestas**	**Didmiestis**		**Kaimas**	**Miestas**	**Didmiestis**		
Taip	61.9%	67.8%	68.6%	65.8%	40.0%	36.5%	26.0%	33.1%	51.6%
Ne	36.1%	11.6%	29.0%	28.3%	30.4%	50.6%	57.3%	46.0%	36.0%
N/D	2.0%	20.6%	2.5%	6.0%	29.6%	12.9%	16.7%	20.9%	12.5%

Papildomai patikrinome, ar sutinkantys ir nesutinkantys tarnauti kibernetiniu šauktiniu vienodai gerai identifikuoja KSS rolę. Iš teigiamai atsakiusiųjų, 73 proc. identifikuoja F1 kaip pagrindinę

kibernetinio saugumo specialisto funkciją (žr. 3.12 lentelę) ir 8,2 proc. pasirinko F3. Tarp neigiamai atsakiusiųjų, F1 rinkosi 69,9 proc., o F3 – 10,5 proc. Statistiškai, šie skirtumai yra nereikšmingi. Taigi galima teigti, kad visi atsakiusieji vienodai gerai atpažįsta kibernetinio šauktinio profilį.

3.12 lentelė. KS funkcijų identifikavimas tarp šaukiamojo amžiaus jaunuolių

K2 - Ką veikia KS	Taip	Ne	Nežinau	Iš viso
F1: Stebi kompiuterinių sistemų veiklą ir reaguoja į iškilusius saugumo įvykius	73.0%	69.9%	39.2%	68%
F2: Kuria žiniatinklio svetaines, puslapius, informacines sistemas	2.6%	6.7%	19.3%	6%
F3: Prižiūri kompiuterių tinklus, administruoja kompiuterius	8.2%	10.5%	17.6%	10%
F4: Kuria telefonams skirtas programėles ir / ar kompiuterinius žaidimus	0.6%	3.7%	8.3%	3%
F5: Nežino, neatsakė	15.7%	9.3%	15.5%	13%

Trečdalis šaukiamojo amžiaus merginų ir du trečdaliai vaikinų sutiktų tarnauti kibernetiniais šauktiniais.

3.1.2. Išvados

1. Visuomenę reprezentuojančiose grupėse virš 18 metų (studentai, vadovai, specialistai, verslo savininkai) dominuoja nuomonė, kad mokymai mokyklose ir universitetuose yra nepakankami bei trūksta atviros prieigos šaltinių apie KS grėsmes ar jų prevenciją. Išsiskiria pensijinio amžiaus grupė, bedarbiai, ūkininkai, kurie KS grėsmių ir prevencijos aspektų neidentifikuoja kaip svarbių mokymuisi, o tai gali turėti įtakos šių grupių raštingumo ugdymui KS klausimais.
2. Daugiau nei trečdaliui gyventojų KS specialisto rolė dar nėra gerai pažįstama. Jaunimas šiuo atžvilgiu taip pat nelabai skiriasi nuo suaugusiųjų, tad KS srities viešinimas ir įvairių galimų KS rolių žinomumo didinimas mokyklose galėtų reikšmingai prisidėti prie KS specialistų skaičiaus didinimo.
3. Jaunimo grupė (iki 25 metų) išsiskyrė lanksčiu požiūriu į tapimą KS specialistu, manydami, kad amžius tam neturi reikšmės, kas leidžia daryti išvadą, kad jaunesnėse kartose profesijos ar srities keitimas yra įprastas požiūris ir ši grupė prisirišimu konkrečiai veiklai nepasižymi. Tai iškelia naujus uždavinius perspektyvoje kaip motyvuoti įsitraukusius darbuotojus išlikti profesijoje arba siekiant pritraukti į KS sritį daugiau žmogiškųjų išteklių dairytis į neseniai studijas baigusius asmenis, kuriems ši sritis gali būti patraukli.
4. Lietuvos visuomenės tyrime tik ketvirtis respondentų mano, kad KS srities specialistu galima tapti mokantis savarankiškai. Tai leidžia daryti išvadą, kad universitetų ir kolegijų formalaus mokymosi pasiūla įeiant į KS veiklos lauką yra labai aktuali.
5. Nors KS srityje dirba iki 11 proc. moterų, pačios moterys itin palankiai vertina veiklos galimybes šioje srityje ir mano, kad jų turėtų būti apylygiai su vyrais. Didelė dalis (40 proc.) darbingiausios amžiaus grupės (25-45 metų) vyrų taip pat sutinka, kad srityje turėtų būti lygios proporcijos. Tai

reiškia, kad požiūris į profesijos stereotipizavimą keičiasi ir ateityje KS sritis gali nebeišlikti vyrų dominuojama veikla.

6. Didžioji dalis (66 proc.) šaukiamojo amžiaus vaikinų ir net trečdalis merginų sutiktų tarnauti kibernetiniu šauktiniu, jei būtų pašaukti į kariuomenę. Tarp moksleivių teigiamų atsakymų procentas dar didesnis. Tai naujas fenomenas, kurį kariuomenė galėtų sėkmingai panaudoti.

3.2. Organizacijų vadovų tyrimas

Siekiant išsiaiškinti organizacijų sprendimų priėmėjų požiūrį į kibernetinį saugumą ir šios srities specialistų poreikį, buvo atlikta įmonių vadovų ir žmogiškųjų išteklių skyrių vadovų apklausa. Vadovų apklausos imtį (246) sudarė daugiausia vidutinio ir stambaus verslo įmonių vadovai. Kadangi mus domino segmentas, kuriame kibernetinio saugumo klausimams suteikiamas pakankamai aukštas prioritetas – a priori, buvo žinoma, kad daug mažųjų įmonių neturi resursų dedikuotiems KS specialistams, todėl buvo apribota įmonių iki 10 darbuotojų imtis. Vadovų apklausos rezultatų paklaida – iki 7 proc. Kadangi mažos įmonės retai turi dedikuotų KS specialistų, taikėme kvotinę įmonių atranką, kad mažosios įmonės (iki 10 darbuotojų) sudarytų ne daugiau 25 proc. visų apklausiamųjų įmonių. Anketos klausimai pateikti A.2.1 priede. Apklausą vykdė UAB „Rinkos tyrimų centras”, vykdymo duomenys pateikiami 3.13 lentelėje.

Anketa telefonu	199
Anketa užpildyta gavus el. paštu	55
viso užpildė:	**254**
Gavo anketą el. paštu, bet neužpildė	128
Nepavyko susisiekti	460
Atsisakė	373
Netinkamas kontaktas	130
Viso susisiekta:	**1343**

3.13 lentelė. Apklausos vykdymo duomenys

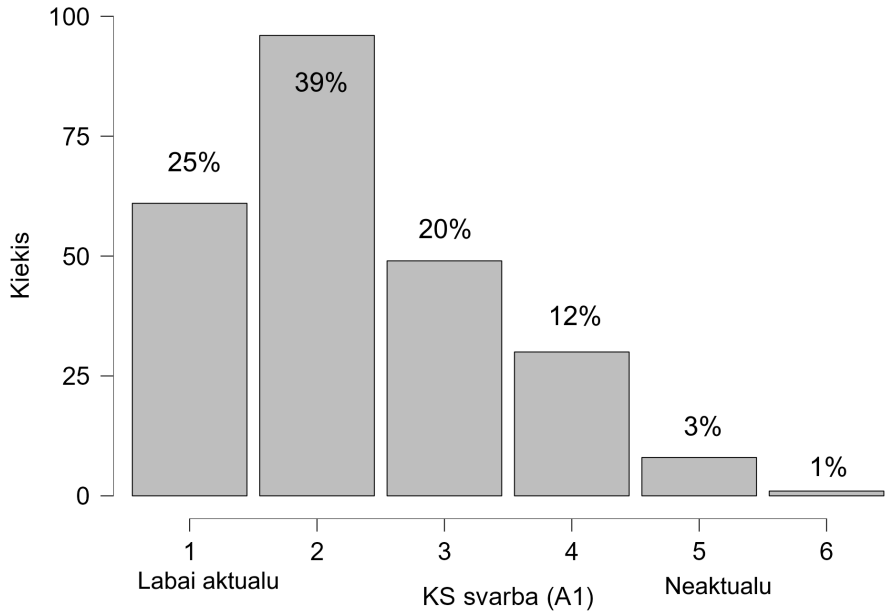
Į anketą atsakė 254 respondentai [7]. Analizei naudojami tik 246 įrašai, kadangi 4 atvejais buvo pateikti atsakymai ne į visus klausimus, o 4 atvejų duomenys buvo nevalidūs, pavyzdžiui, nulinis darbuotojų skaičius ar atsitiktinių simbolių sekos vietoj veiklos sektoriaus.

Aprašomoji bendro pobūdžio informacija apie respondentus plačiau pateikta A.2.3 priede, kur taip pat pateikti papildomi duomenų validumo tikrinimai. Apklausa tiksliai atitinka didesnių, negu 50 darbuotojų įmonių pasiskirstymą Lietuvoje (žr. priede A.1 pav.), iš 2820 tokių įmonių buvo apklaustos 210 (t.y. 7,5 proc.), tad šių įmonių tyrimo rezultatų paklaida neviršija 7 proc., kai patikimumo riba imama 0,95.

3.2.1. Gauti rezultatai

Respondentai pripažįsta KS svarbą organizacijoje (žr. 3.2 pav.) – net 64 proc. mano, kad tai yra aktualu arba labai aktualu, ir tik 15 proc. teigia, kad tai mažai aktualu arba visiškai neaktualu (klausimas A1).

Respondentų atsakymai apie KS aktualumą yra pateikti nominalinėje skalėje (jie tiesiog turėjo pasirinkti aktualumo kategoriją), tačiau jeigu sugraduotume kategorijas ir suteiktume joms skaitines vertes (1 – labai aktualu, 2 – aktualu, 3 – vidutiniškai, 4 – mažai, 5 – visiškai neaktualu) ir padarytume (nemokslinę) prielaidą, kad skirtumai tarp jų yra tos pačios vertės, tai galėtume suvidurkinti atsakymus, tuos vidurkius pavadinti KS svarbos koeficientu ir tada įvertinti, kaip KS saugumo aktualumas priklauso nuo įmonės dydžio. Tokiu atveju pamatytume, kad KS saugumo svarba tolygiai auga kartu su įmonės apyvarta, nes 3.14 lentelėje matyti, jog kuo mažesnis KS svarbos koeficientas, tuo labiau yra svarbi KS sauga, aki vienetas reiškia „Labai aktualu", o penketas - „Visiškai neaktualu". Išties, net 68 proc. didesnių įmonių (kur dirba 50 ar daugiau darbuotojų) vadovai mano, kad KS yra aktualus arba labai aktualus, kai taip teigia tik 39 proc. mažesnių įmonių vadovų. Kadangi maža apyvarta ir mažas darbuotojų skaičius atitinkamai apriboja mažų įmonių resursus kibernetinei gynybai, tai toks vadovų požiūris dar labiau padidina mažų įmonių pažeidžiamumą.



3.2 pav. Kibernetinio saugumo aktualumas organizacijai

3.14 lentelė. KS svarba priklausomai nuo įmonės apyvartos

	A1-KS-svarba				
Apyvarta (M€)	1: <0,145	2: 0,145-1	3: 1-5	4: 5-10	5: >10
Atsakymų kiekis	13	36	69	36	34
Trūkstami	0	0	1	0	1
KS svarbos koef. (vidurkis)	3,308	2,583	2,290	2,250	1,941

Apklausa parodė aiškų požiūrio išsiskyrimą KS klausimu tarp tų įmonių, kurios jau rūpinasi saugumu, ir tų, kurios nesirūpina. Paprastai šnekant, tos įmonės, kurios skiria dėmesį kibernetiniam

saugumui, ketina ir toliau skirti dėmesį ir jį didinti, tuo tarpu likusios ketina toliau jį ignoruoti. Pavyzdžiui, tarp visų įmonių, net 56 proc. skyrė didesnį dėmesį kibernetiniam saugumui per pastaruosius 2-5 metus (klausimas A5), 52 proc. ketina skirti daugiau dėmesio per ateinančius 2-5 metus (klausimas A6), ir 26 proc. greičiausiai samdys KS specialistų (klausimas A7). Tuo tarpu tarp įmonių, kurias mes vadiname nesaugiomis (kurios neturi savo KS specialistų ir nesinaudoja išorinėmis KS paslaugomis), tik 26 proc. skyrė didesnį dėmesį saugumui praeityje, 35 proc. skirs didesnį dėmesį ateityje, ir tik 12 proc. tikisi samdyti KS specialistų.

> Organizacijos, kurios šiuo metu nesirūpina kibernetiniu saugumu, linkusios ir toliau jį ignoruoti.

Kalbant apie KS specialistų poreikį (klausimas A8), 56 proc. įmonių vadovų mano, kad jų trūksta, o 17 proc. galvoja, kad trūkumas yra labai didelis. 28 procentai didesnių įmonių (su 50 darbuotojų ir daugiau) per artimiausius 2-5 metus tikisi samdyti KS specialistų, o tai reiškia, kad per tą laikotarpį galima tikėtis 800 ± 56 naujų darbo vietų (iš jų 122 – labai tikėtina ir 678 – tikėtina) kibernetinio saugumo specialistams didesnėse įmonėse. Tarp mažų įmonių, 16 proc. atsakė, kad naujų KS specialistų samdymas yra tikėtinas. Šių (mažų) įmonių imtis mūsų tyrime yra per maža, kad galėtume daryti skaitines prognozes, tačiau net ir be jų duomenų yra numatomas didelis KS specialistų poreikio augimas. Augimą patvirtina ir darbo skelbimų analizė (žr. skyrelį 3.6), kuri rodo daugiau nei dvigubai per pastaruosius metus išaugusį skelbimų skaičių KS srityje.

> Per artimiausius 2-5 metus Lietuvoje didžiosios įmonės (virš 50 darbuotojų) ieškos 800 naujų kibernetinio saugumo specialistų.

Dauguma respondentų (iš viso 81 proc., o viešajame sektoriuje net 84 proc.) mano, kad IT specialistas galėtų visiškai ar bent iš dalies pasirūpinti ir kibernetiniu saugumu (klausimas A10), ir tik 13 proc. teigia, kad KS yra atskira rolė (detalesnis pasiskirstymas pateiktas priedo lentelėje A.2).

> Virš 80 proc. vadovų nuomone IT specialistai gali visiškai ar bent iš dalies pasirūpinti kibernetiniu saugumu organizacijoje.

Šioje vietoje galima būtų kaltinti klausimo formuluotę - tikėtina, kad pakeitus žodį "gali" į "turi", IT specialistui nebūtų priskiriama tiek daug atsakomybės už kibernetinį saugumą, tačiau detalesnės apklausos (žr. kitą skyrių 3.3) rodo, kad įmonėse (ypač - mažesnėse) IT specialistai dažnai vykdo KS rolėms tenkančias funkcijas. Išties, apklausoje galima pastebėti, kad kai kurie įmonių vadovai paklausti apie jų KS specialistų skaičių (klausimas A2), neretai nurodė tiesiog bendrą savo IT specialistų skaičių. Deja, net ir tokiu atveju, pusė Lietuvos įmonių neturi darbuotojo, kuris rūpintųsi KS (lentelė 3.15). Tarp įmonių, kurios turi savo KS specialistų, mažiau nei pusė (48 proc.) turi pareiginius nuostatus, kuriuose bent iš dalies būtų aprašytos KS specialisto funkcijos (klausimas A3). Dalis (apie pusė) savo specialistų neturinčių įmonių samdo išorinius KS paslaugų teikėjus (klausimas A4), tačiau didelis kiekis įmonių neturi nei savo KS specialistų, nei samdo išorinius KS paslaugų teikėjus. Sugrupavus

įmones pagal jų apyvartą, matome, kad tokių neapsaugotų kibernetinio saugumo prasme įmonių procentas kiekvienoje grupėje tolygiai mažėja su įmonės apyvarta (lentelė 3.16) – Lietuvoje iš viso yra apie 23 proc. neapsaugotų įmonių, o tarp mažų įmonių (kurių metinė apyvarta nesiekia 145 tūkst.€), tokių yra beveik 70 proc.

Pusė Lietuvos įmonių neturi darbuotojų, kurie rūpintųsi kibernetiniu saugumu.

3.15 lentelė. Įmonių pasiskirstymas pagal KS specialistų skaičių

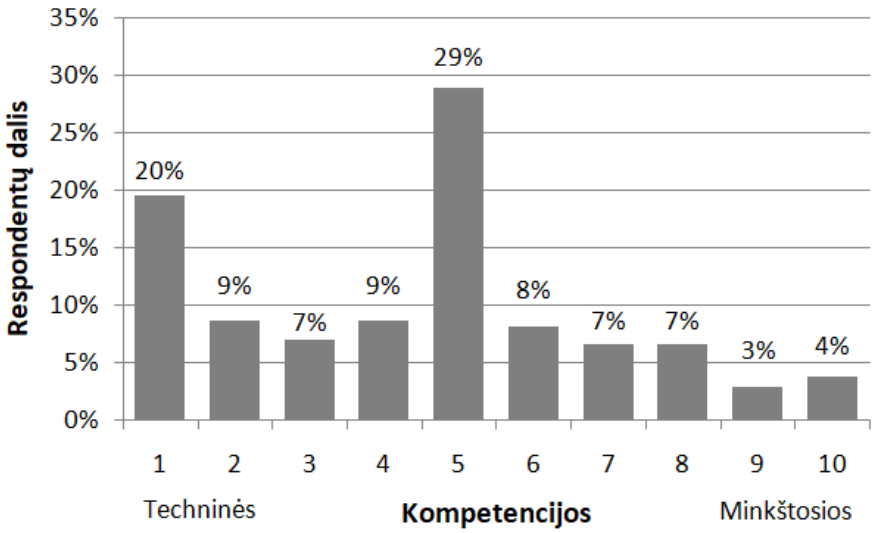
KS specialistų kiekis	Įmonių kiekis	Procentas
0	126	51%
1	63	26%
2 ir daugiau	57	23%
Iš viso	246	100%

3.16 lentelė. Neapsaugotos įmonės – įmonės be savo KS specialistų, kurios nesamdo išorinių KS paslaugų teikėjų

Apyvarta, M€	Apklausta įmonių	Įmonės be KS	Įmonės be KS, proc.
<0,145	13	9	69,2%
0,145-1	36	12	33,3%
1-5	70	15	21,4%
5-10	36	3	8,3%
>10	35	3	8,6%
Nenurodyta	56	15	26,8%
Iš viso	246	57	23,2%

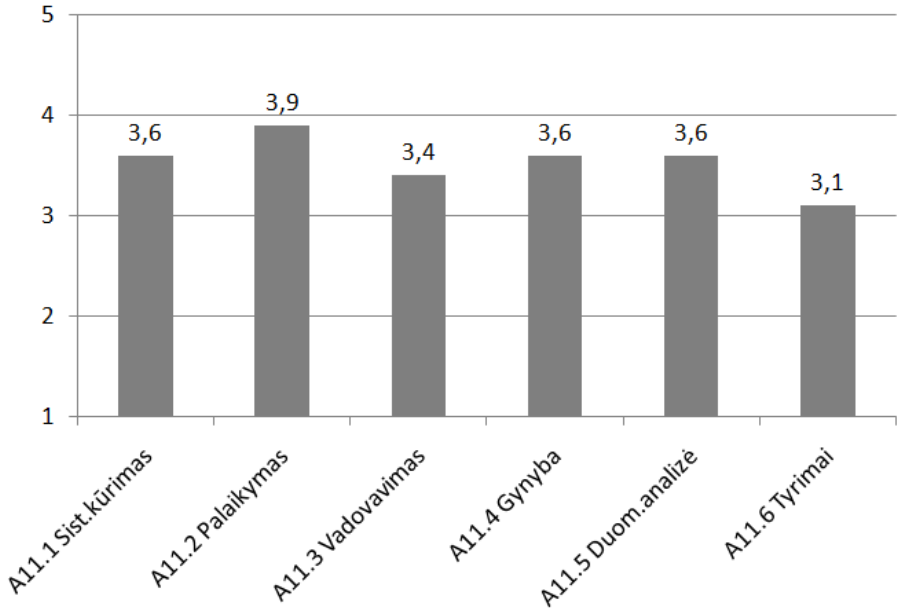
Paklausti, ar KS specialistui reikia daugiau techninių žinių, ar „minkštųjų" kompetencijų (klausimas A9), įmonių vadovai buvo neapsisprendę ir didelį jų dalis (29 proc.) stengėsi atsakyti per vidurį (pav. 3.3), nors penktadalis išsiskyrė ir itin tvirtai akcentavo technines žinias (pasirinko vienetą skalėje nuo 1 iki 10). Vidutinė atsakymų vertė buvo 4,3 (vidurkis būtų ties 5,5) ir ji beveik nepriklausė nuo įmonės dydžio ar įmonės KS specialistų kiekio, tačiau skyrėsi priklausomai nuo sektoriaus: viešojo sektoriaus vidurkis buvo 3,6, o privataus sektoriaus – 4,6. Tai reiškia, kad viešojo sektoriaus vadovai žymiai daugiau svorio suteikia KS specialisto techninėms kompetencijoms.

Į klausimą apie KS kompetencijų poreikį per ateinančius 2-5 metus (klausimas A11) organizacijų vadovai maždaug vienodai pažymėjo visas KS sritis (pav. 3.4), tik šiek tiek mažiau dėmesio paskyrė tyrimų („forensics") sričiai ir kiek labiau akcentavo veikiančių sistemų palaikymo svarbą. Kitaip tariant, svarbiausia yra organizacijos veiklos nenutrūkstamumas. Kadangi tyrimai („forensics") reikalingi



3.3 pav. Kokių kompetencijų reikia KS specialistui vadovo nuomone

dažniausiai po to, kai nutinka incidentas, tai galima teigti, kad vadovai tikisi incidentų išvengti (tiesa, viešajame sektoriuje vadovai šiek tiek mažiau optimistiški, bet statistiškai nereikšmingai).



3.4 pav. Kompetencijų organizacijose poreikis ateityje (skalėje nuo 1 iki 5) įvairiose KS srityse

3.2.2. Išvados

Organizacijos vadovų požiūris į kibernetinį saugumą priklauso nuo organizacijos dydžio (apyvarta, darbuotojų skaičius) – įmonei didėjant, KS aktualumas tolydžiai didėja. Įmonių saugumas auga atitinkamai. Dauguma mažiausių įmonių, kurių metinė apyvarta nesiekia 150 tūkst. eurų (ir kurių yra

daugiausia) išvis neturi jokio specialisto, kuris rūpintųsi kibernetiniu saugumu, nesamdo pagalbininkų iš išorės ir neplanuoja turėti darbuotojų KS srityje. Įmonės apyvartai artėjant prie milijono eurų per metus, galima tikėtis (60 proc. tikimybė), kad joje bus bent vienas IT specialistas – jam įprastai atitenka visos KS specialisto funkcijos. Apyvartai artėjant prie 10 mil. eurų, IT specialistų paprastai bus daugiau nei vienas – tada jau galima tikėtis darbuotojų, kurie vykdys specifines KS funkcijas, nepersiklojančias su įprastine IT administravimo veikla. Tai, be abejo, negalioja IT technologijų įmonėms (jose IT ir KS darbuotojų nepalyginamai daugiau, ir tik viena IT įmonė pateko į mūsų apklausą, todėl rezultatų neiškraipė).

Remiantis vien tik didesniųjų įmonių (kuriose dirba 50 ir daugiau darbuotojų) vadovų nuomone, per ateinančius 5 metus Lietuvoje reikės maždaug du kartus daugiau KS specialistų, nei šiuo metu dirba organizacijose.

Dauguma KS specialistų Lietuvoje dirba (ir dirbs) IT administratoriaus rolėje, bent jau to tikisi dauguma įmonių vadovų ir tą lemia daugumos įmonių dydis. Kitaip suformulavus šią mintį – dauguma IT administratorių turi vykdyti ir KS specialisto funkcijas. Įprastai vadovai iš šių specialistų tikisi ne tik gerų IT žinių, bet ir minkštųjų kompetencijų (t.y. gebėjimo gerai komunikuoti).

Įmonių vadovai iš KS specialistų labiausiai tikisi tinkamo visų sistemų veikimo palaikymo (availability), ir viliasi, kad kibernetinių nusikaltimų tyrimų („forensics”) jiems neprireiks.

3.3. Žvalgomasis kibernetinio saugumo ir IT specialistų tyrimas

Siekdami pamatyti KS problematiką iš specialisto pusės, atlikome žvalgomąjį Lietuvoje dirbančių kibernetinio saugumo specialistų nuomonės tyrimą. Anketos klausimai (žr. A.3.1 priedą) buvo pateikti kibernetinio saugumo specialistams profesionalams, kurie nuolat dirba Lietuvoje IT ir KS sektoriuose nacionalinėse ar tarptautinio lygio įmonėse/organizacijose. Apklausą vykdė UAB „Rinkos tyrimų centras". Anketa buvo individualiai nusiųsta 35 specialistams, kurie buvo identifikuoti pagal jų LinkedIn profilyje deklaruotą informaciją. Į ją atsakė 29 asmenys – 13 viešojo sektoriaus ir 16 privataus, tačiau vienas privataus sektoriaus respondentas iš tolimesnių rezultatų eliminuotas dėl ypatingai didelio jo įmonės dydžio (virš 800 tūkst. darbuotojų).

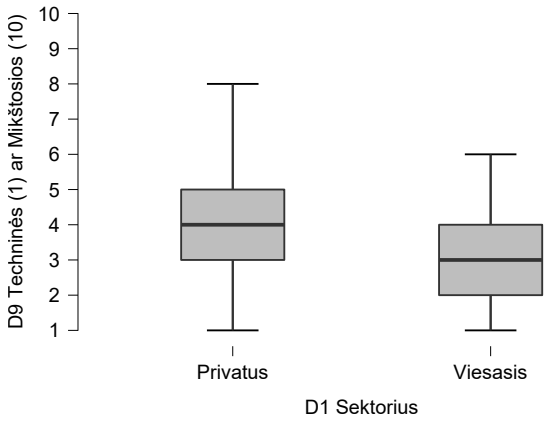
Pagal LinkedIn duomenis (atlikus paiešką su KS raktažodžiais), Lietuvoje yra apie 1000 darbuotojų, kurie vienaip ar kitaip yra susiję su kibernetiniu saugumu. Nors 29 apklausti specialistai sudaro apie 3 proc., bet ši apklausa nėra reprezentatyvi, tik 5 respondentai (18 proc.) buvo iš įmonių, kuriose dirba mažiau nei 51 darbuotojas, tačiau suteikia įžvalgų, kurios vėliau bus tikslinamos pusiau struktūrizuotuose ekspertų interviu.

3.3.1. Gauti rezultatai

Apie pusė respondentų atsakė, kad jų organizacija samdo išorinius KS paslaugų teikėjus (D6.1 klausimas), daugiausia – sistemų auditavimui (31 proc.) arba pažeidžiamumų testavimams (angl. pentesting) (34 proc.).

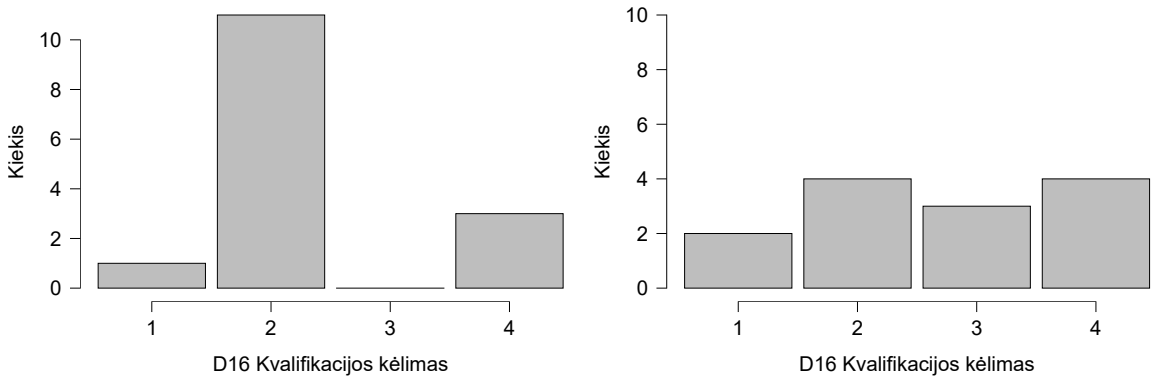
Į D7.1 klausimą apie tai, kokių sertifikatų ar diplomų tikimasi iš KS specialistų, 35 proc. atsakė, kad iš KS specialistų tikisi diplomų arba sertifikatų (viešajame sektoriuje 31 proc., privačiame – 40 proc.). Minimi labai įvairūs: CEH, CISSP, GIAC, Offensive Security, ISACA, CISA, tinklo administratoriaus; įrangos gamintojų – Cisco, Fortinet, Rapid, Checkpoint. Kartojosi ir nuomonė, kad naujam KS darbuotojui pakanka turėti aukštojo mokslo diplomą, o vėliau jau organizacija turi pasirūpinti jo ugdymu ir pritaikymu konkrečiai sričiai.

Respondentai mano, kad KS specialistui daugiau reikalingos gilios techninės žinios, negu „minkštosios" kompetencijos, tą ypač akcentuoja viešojo sektoriaus respondentai. Skalėje nuo 1 (techninės žinios) iki 10 (minkštosios) vidurys būtų ties 5,5, tačiau vidutinė atsakymo vertė buvo 3,6 (viešajame sektoriuje 3,2, privačiame – 4,1). Statistiškai, šis skirtumas tarp viešojo ir privataus sektoriaus atsakymų yra nereikšmingas (t-testo $p = 0.156$), tačiau respondentų polinkis prioretizuoti techninę kompetencijų dalį yra statistiškai reikšmingas (vieno mėginio t-testas: $t = -5,84$, $df = 27$, $p < 0,001$) su didele efekto verte (Cohen'o $d = -1.1$) (žr. 3.5 pav.). Tai skiriasi nuo įmonių vadovų požiūrio, jų vidutinis atsakymas buvo 4,3 (viešajame sektoriuje 3,6, privačiame 4,6, žr. ankstesnį 3.2 skyrelį), t.y. vadovai minkštosioms KS specialisto kompetencijoms skiria šiek tiek daugiau svarbos, negu patys KS specialistai.



3.5 pav. Kokių kompetencijų (techninių ar minkštųjų) pageidaujama iš KS specialisto priklausomai nuo sektoriaus

Organizacijos mano, kad jos skiria pakankamai dėmesio savo KS specialistų kvalifikacijos kėlimui – taip į D16 klausimą pažymėjo 80 proc. privataus sektoriaus atstovų (žr. 3.6a). Tiesa, taip atsakė tik 46 proc. viešojo sektoriaus atstovų, ir dar 23 proc. viešojo sektoriaus respondentų pasakė, kad skiria „beveik pakankamai" dėmesio (žr. 3.6b pav.).



(a) privačiame sektoriuje (b) viešajame sektoriuje

3.6 pav. Kiek dėmesio skiriama KS specialistų kvalifikacijos kėlimui Jūsų organizacijoje (1 - daugiau nei pakankamai, 2 - pakankamai, 3 - beveik pakankamai, 4 - nepakankamai)

Paklausti, kokių KS specialistų labiausiai trūksta Lietuvoje (D15), net 4 atsakė, kad visų sričių. Kiti paminėjo tokias sritis (skliaustuose mūsų mėginimas priskirti vieną iš ENISA rolių): Pažeidžiamumų paieškos operatorius (E12, $\times 2$), Kibernetinio saugumo vadovas (E1), Linux DevOps (įgyvendintojas, E8), KS architektas (E5, $\times 6$), Linux administratorius (IT specialistas), Duomenų valdymo įgaliotinis (teisės, politikos ir atitikties pareigūnas, E3), KS teisininkas (teisės, politikos ir atitikties pareigūnas, E3), techninių specialistų ($\times 3$, bet neaišku kokio tipo), OT (operacinių technologijų, t.y. pramonės sistemų kontrolės) specialistas (įgyvendintojas, E8), Tinklo įrangos administratorius (IT specialistas), Kenkėjiško kodo tyrėjas (skaitmeninių nusikaltimų tyrėjas, E12), KS konsultantas (auditorius, E6), KS

analitikas (E2, ×3), *Aplikacijų* saugumo specialistas (pažeidžiamumų testuotojas, E12), CIRT/SOC specialistas (E2, ×2), Tinklo ir ugniasienių administratorius (IT specialistas), Forensic tyrėjas (E11, ×4), OSINT specialistas (E4), Komunikacijos specialisto (E3), Grėsmių medžiotojas (E4). Rezultatai apibendrinti 3.17 lentelėje.

3.17 lentelė. Kokių sričių KS specialistų trūksta (pagal ENISA roles 1.1 lentelėje)

Rolė	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	IT	Nedetalizuota
Kiekis	1	5	3	2	6	1		2			4	4	3	3

Iš paminėtų atsakymų galima spręsti, kad techninių specialistų poreikis yra kelis kartus didesnis, nei netechninių (vadovų[E1]/teisininkų[E3]/auditorių[E6] – 5, kitų rolių – 26). Sprendžiant iš to, kad kartais paminėtos tiesiog IT pareigybės, galima susidaryti įspūdį, jog IT specialistams neretai tenka dirbti ir KS specialistų darbą. Įdomu, kad niekas nepasigedo KS ugdytojų (E7) ir mokslininkų (E9). Rizikos vertinimas (E10) atskirai taip pat nebuvo išskirtas – galima daryti prielaidą, kad ši rolė atitektų kuriai nors kitai vadovaujančiai rolei arba audito sričiai.

Respondentų buvo paklausta, kokiose KS rolėse jų organizacija atlieka veiklas (D8, D10-14). Buvo pateiktas ENISA rolių sąrašas (D8) ir NIST NICE rolių sąrašas (D10-14). Apklausos metu ENISA leido pasinaudoti jų tuo metu dar tik ruošiamu juodraštiniu europietiškos KS įgūdžių sąrangos rolių sąrašu, todėl klausimyne buvo apjungtos Architekto [E5] ir Įgyvendintojo [E8] rolės (D8.3), bei Ugdytojo [E7] ir Mokslininko [E9] rolės (D8.4), kurios vėlesniame ENISA sąrangos variante yra atskirtos. Taip pat nebuvo pateiktas Grėsmių žvalgybos pareigūno [E4] variantas – respondentai galėjo jį pasirinkti kaip punktą *Kita* (D8.10). Daugiausia – 90 proc. buvo pažymėta E1 rolė (vadovavimas ir valdymas), dažnai pasirinktos E3 (Teisės, politikos ir atitikties pareigūnas) ir E6 (Auditorius) – po 83 proc.. Mažiausiai paminėtos Skaitmeninių nusikaltimų tyrėjo (E11) bei Ugdytojo ir Mokslininko (E7+E9) rolės, po 59 proc. Dauguma organizacijų vykdo veiklas, kurios apima daugelį rolių – vidutiniškai buvo pasirinktos net 6,7 rolės iš 10 galimų. Rolių skaičius didėja kartu su organizacijos dydžiu (žr. 3.18 lentelę, kur eilutė „Vidurkis" rodo pasirinktų ENISA bei NIST sąrangos rolių skaičių priklausomai nuo įmonės dydžio, kur dydis 1 reiškia iki 10 darbuotojų, 2 – iki 50, 3 – iki 250, 4 – virš 250 darbuotojų) – tai suprantama. Tačiau įdomus rezultatas, kad net ir labai mažose įmonėse (kur KS pareigas eina tik vienas žmogus), vykdomų KS rolių skaičius išlieka labai didelis (6). Tai reiškia, kad mažose organizacijose KS specialistams tenka labai didelis spektras užduočių.

Analogiškai buvo paprašyta respondentų pažymėti organizacijoje esančias roles pagal amerikietišką NIST NICE klasifikaciją. Daugiausia kartų buvo pažymėta Sistemų administratoriaus rolė (D13.6) – 90 proc., antrą vietą pasidalijo kitos trys rolės: Incidentų sprendėjas (D11.3), Techninės pagalbos specialistas (D13.4) ir Tinklo operacijų specialistas (D13.5) – po 86 proc.. Visos šios rolės (išskyrus Incidentų sprendėją) pagal europietišką klasifikaciją yra priskiriamos ne KS, o IT rolėms. Mažiausiai kartų buvo paminėtos Kibernetinės žvalgybos (D12.4, 21 proc.), Komunikacinių sistemų saugumo

vadovo (COMSEC, D10.6, 28 proc.) bei Teisininko kibernetinėje srityje (D10.1, 26 proc.) rolės, kadangi Teisininkas yra atskirtas nuo Duomenų apsaugos pareigūno (D10.2, 59 proc.). Vidutiniškai buvo pasirinktos 23,2 NIST NICE rolės iš pateiktų 41.

3.18 lentelė. Keliose KS rolėse organizacijoje vykdomos veiklos (priklausomai nuo įmonės/organizacijos dydžio, kur 1 - mažiausios, 4 - didžiausios įmonės)

	ENISA				NIST			
Įmonės dydis	1	2	3	4	1	2	3	4
Atsakymų	1	4	8	15	1	4	8	15
Vidurkis	6	6	5	7.667	20	20.250	15.125	27.867
Stand.nuokrypis		1.826	2.976	2.024		19.138	8.476	9.576
Min.	6	4	1	2	20	3	3	10
Maks.	6	8	9	9	20	41	27	40

Apibendrinant, Lietuvos organizacijose yra aktualios visos KS rolės kokią klasifikaciją bepaimtume, tačiau net iš tokios mažos imties matomas sumažintas dėmesys kibernetinių grėsmių žvalgybos/medžioklės, mokslinių tyrimų (ir potencialiai – ugdymo), ir kibernetinės teisės srityse.

Respondentai papildomai galėjo išsakyti savo pageidavimus KS specialistų rengimui. Jų komentarai pateikti A.3.3 priede. Nors pasisakymų skaičius nėra didelis, tačiau galima įžvelgti dominuojančią nuomonę, kad iš naujų KS darbuotojų tikimasi ne tiek specializuotų KS žinių, kiek plačių IT žinių ir bendrųjų KS žinių. Organizacijos linkusios pačios toliau ugdyti KS specialistus savo norimoje srityje.

> Iš naujo kibernetinio saugumo darbuotojo tikimasi išsamių IT, o ne specializuotų KS žinių.

3.3.2. Išvados

1. Ekspertai mano, kad IT žinių KS specialistams reikia daugiau, lyginant su vadovais, kurie atitinkamai išskiria ir bendrąsias kompetencijas KS specialistams.
2. Privatus sektorius rūpinasi savo specialistais ir net 80 proc. sudaro sąlygas kelti kvalifikaciją, deja, viešajame sektoriuje taip elgiasi mažiau nei pusė organizacijų. Įmonės yra linkusios gauti IT specialistą su plačiomis IT žiniomis ir paruošti jį KS sričiai.
3. Trūksta viso spektro specialistų, bet techninio profilio darbuotojų reikia kelis kartus daugiau nei netechninio profilio (vadovų ar teisininkų).
4. Ekspertai neišskiria mokslininkų ir ugdytojų kaip atskiros KS specializacijos.
5. Lietuvos organizacijose vykdomos visų rolių veiklos, vidutiniškai vienoje organizacijoje padengiama 67 proc. ENISA ECSF ir 57 proc. NIST NICE veiklų.

6. Net ir mažose įmonėse padengiamas platus veiklų spektras, o tai reiškia, kad vienas darbuotojas vykdo kelių rolių funkcijas.

3.4. Ekspertinių interviu tyrimas

Apklausos gali suteikti tik apibendrintą informaciją, todėl siekdami atlikti kokybinį tyrimą ir gauti detalesnių įžvalgų apie KS specialistus versle, jų pritraukimą ir išsilavinimo kelią, susisiekėme su ilgametę patirtį KS srityje turinčiais ekspertais, kurie visi virš 5 metų dirba vyriausiojo (angl. senior) KS specialisto rolėse didžiausiose Lietuvos įmonėse ir tuo pačiu aktyviai dalyvauja didžiausiose tarptautinėse kibernetinėse pratybose Locked Shields, organizuojamose NATO CCDCOE, atstovaudami Lietuvai, tad nežiūrint užimamų pareigų vis dar išlaiko aukščiausio lygio technines žinias. Visi jie sutiko duoti įrašomą interviu 2021 metų rudenį ir žiemą. Interviu buvo transkribuoti ir atlikta jų teksto analizė (žr. A.4 priedą).

Ekspertų buvo prašoma pakomentuoti, kas yra kibernetinio saugumo specialistas ir kaip juo tapti, kokios svarbiausios kompetencijos, ateinant į sritį ar dirbant joje.

3.4.1. Gauti rezultatai

Ekspertų nuomone, pagrindinis karjeros kelias prasideda turint IT profilį – IT išsilavinimą ir/ar patirtį, nes IT persidengia su KS. 3.19 lentelėje išskirti esminiai reikalavimai KS specialistui. Ekspertai pamini, kad KS galima vadinti tai, kas yra IT, nes susiję su pasiekiamumu (angl. availability) ir jei IT specialistas suvokia KS grėsmes bei taiko metodus jų prevencijai, tai jis automatiškai yra KS specialistas. IT profilį gali turėti ne tik IT srityje dirbantys ar dirbę kandidatai, nes į KS sektorių galima ateiti ir su savarankiškai įgytomis kompetencijomis. Ekspertų nuomone, KS pradedančiajam svarbiausia turėti IT bazines žinias, gebėti skaityti programinį išeities kodą, gebėti programuoti / skriptinti ir susikurti savo įrankius (naudotis komandinės eilutės įrankiais, rašyti skriptus). Baziniu IT žinių lygmeniu laikomi infrastruktūros, programų kūrimo, tinklų administravimo, debesijos, virtualizacijos pagrindai. Asmeniniam tobulėjimui reikia valios, motyvacijos, noro, skirti papildomo laiko, praktikuotis ir bandyti. Ekspertai įvardija, kad toks žmogus turi būti neišlepęs, užsispyręs, nebijantis iššūkių.

> Motyvacija, užsispyrimas ir gebėjimas savarankiškai nuolat mokytis išskiriamos kaip būtinos KS specialisto savybės.

Aukštojo mokslo diplomas nėra labai svarbus, bet aukštojo mokslo studijos suteikia „plačią žinių paletę” ir bendrą išprusimą, nors ir negilias žinias. Pagrindiniai filtrai atrenkant darbuotojus yra patirtis, sertifikatai ir atrankos pokalbiai bei užduotys. Sertifikatai parodo žmogaus motyvaciją, asmeninius tikslus ar ambicijas, gebėjimų profilį, taip pat naudojami kandidatų „atsijojimui”, ypač pradedančiųjų pozicijoms.

> Sertifikatai naudojami kandidatų "atsijojimui" ir motyvuotų bei turinčių patirties darbuotojų suradimui.

3.19 lentelė. KS specialisto kelias į sritį (technologinis profilis)

IT profilis • IT išsilavinimas ir / arba darbo patirtis	⇒	**KS specialistas** • KS grėsmių suvokimas • Metodų taikymas KS grėsmių prevencijai ⇑
Gebėjimų rinkinys • Baziniai IT pagrindai • Programinio kodo skaitymas • Programavimas / skriptinimas • Įrankių kūrimas	⇒	**Filtras** • Diplomas ir patirtis • Sertifikatai
⇑ ⇑ ⇑		
Asmeninės savybės • Noras, motyvacija • Domėjimasis, papildomo laiko skyrimas • Praktikavimasis, bandymas		

Specialistų amžius. Ekspertai pastebi, kad pretendentų į pradedančiojo pozicijas netrūksta, jaunų žmonių, kurie domisi karjeros galimybėmis KS, yra. Jauni žmonės dažniausiai nebijo bandyti, suklysti, o vyresnieji yra "lėtesni" ir, kai kurių ekspertų nuomone, ne visada nori mokytis, nors taip deklaruoja. Lietuvoje daug KS specialistų yra jauni, nors ateityje vyresnių tik daugės. Vakarų šalyse yra įvairaus amžiaus ekspertų. Ekspertai pamini, kad galbūt Lietuvoje dar nėra nusistovėję mokymosi visą gyvenimą tradicijos ir kultūra.

Specialistų poreikis ir pasiūla. Ekspertai paklausti, koks yra KS specialistų poreikis Lietuvoje, pamini, kad didelės įmonės turi darbuotojų specializuotoms KS funkcijoms atlikti. Vidutinio dydžio įmonės mąsto apie KS grėsmes ir ieško balanso tarp KS ir kitų funkcijų, pavyzdžiui, IT. KS funkcijos gali „pasislėpti” po kitomis rolėmis, pavyzdžiui, QA inžinieriumi (angl. Quality Assurance Engineer). Mažos įmonės ribojamos finansų ir samdyti KS specialistą joms per brangu. Ekspertai pamini, kad Lietuvoje dėl taupymo dažnai ieškoma ar tikimasi žmogaus-orkestro.

> Lietuvoje dažniausiai ieškoma plataus profilio KS specialisto arba IT specialisto, kuris atlieka KS funkcijas, o ne specializuoto KS specialisto.

Ekspertai akcentuoja, kad trūksta patyrusių, „gerų” specialistų, jau mokančių, kad jų nereikėtų mokyti. O patyrusių darbuotojų pasiūla yra maža. Specialistų trūkumas susijęs su dideliu IT specialistų trūkumu. Kai kurie patyrę specialistai brangūs, todėl įmonės auginasi juos pačios. Ekspertai pabrėžia, kad imti pradedančiuosius galima, kai jau yra pakankamas kiekis patyrusių, kad rengiant kolegą nesitrukdytų pagrindinės veiklos. Taip pat įmonės įžvelgia riziką, kad apmokius darbuotoją, jį perperka kitos įmonės. Interviu metu buvo akcentuoti keli aspektai apie darbuotojų paiešką:

- Darbo skelbimai mažai naudojami, neduoda daug naudos.
- Darbuotojų ieškoma per pažintis, uždaras grupes, o ne vien per žmogiškųjų išteklių skyrių.

- Vyksta „galvų medžioklė" ir viliojimas iš kitų įmonių/organizacijų: centrai (t.y. stambios užsienio įmonės, bankai) perima/perperka iš verslo, o verslas "susiurbia" iš viešojo sektoriaus.

> Pretenduojančių į pradedančiųjų pozicijas yra, bet dalis įmonių pradedančiųjų darbuotojų mokymą ir rengimą funkcijoms atlikti mato kaip papildomą naštą, todėl didžiausia paklausa yra patyrusių specialistų.

Darbuotojų atranka į pareigybes. Ekspertai pasidalino patirtimi, kaip vyksta atranka į KS pareigybes. Po pirminio darbuotojų filtro pagal CV ar pokalbio, kandidatuojantiems į technines pareigybes duodami techniniai iššūkiai. Nors kandidatų nėra perteklius, dalis jų nepriimami, nes atrankos metu paaiškėja tam tikri individualūs niuansai:

1. Nenori išmokti programuoti
2. Pripratę naudotis GUI paremtais spartaus diegimo įrankiais
3. Pateikia ne savo spręstų techninių iššūkių sprendimus
4. Žino skelbime pateiktus raktažodžius, bet neturi žinių ar gebėjimų
5. Pretenduoja į kelias vietas vienu metu, ir greitai atrankos procesas nutrūksta
6. Negali pagrįsti techninės užduoties sprendimo
7. Nedera požiūris ar darbo kultūra su įmonės standartais

Kai kuriems tokiems kandidatams duodamos rekomendacijos, kaip savarankiškai padirbėti, pasimokyti, ir dalis jų grįžta įgavę kompetencijų.

> Mentorystė padeda surasti asmeninį karjeros kelią.

Ekspertai pamini, kad dalis naujų darbuotojų turi tik išankstinį požiūrį ar supratimą apie KS specialisto funkcijas. Pavyzdžiui, įsivaizduoja sistemų pažeidžiamumų testuotojo darbą kaip techninį ir atliekamą izoliuotai kitų žmonių atžvilgiu arba kaip žaidimą, kuris naudojamas techninių gebėjimų ugdymui. Bet didelė dalis darbo iš tikrųjų yra ataskaitų rašymas. Labai svarbu gebėti dirbti komandoje, valdyti laiką ir komunikuoti su kolegomis ar kitomis komandomis.

> KS sritis yra patraukli ir atrodo perspektyvi naujiems darbo rinkos dalyviams ar keičiantiems savo profilį, bet jie ne visada supranta, kokios funkcijos atliekamos arba pervertina savo žinias, siekdami darbo vietos.

Dauguma ekspertų paminėjo, kad specialisto kelias gali prasidėti nuo sistemų ar tinklų administratoriaus. Pradinė KS pozicija galėtų būti pagalbos teikimo komandoje (angl. incident response, IR), atliekant analitiko funkcijas, gilinant KS žinias. Bazinis IT žinių rinkinys ar, anot pašnekovų, patirtis IR komandoje leistų rinktis tolimesnį karjeros kelią, pavyzdžiui, diegti ir valdyti saugumo sistemas (saugumo inžinierius) arba pasirinkti veiklas, kur yra mažiau techninio darbo, pavyzdžiui, informacijos saugos vadyba, konsultacijos, auditas, BDAR atitikties vertinimas.

Netechninėms pareigybėms, pavyzdžiui, susijusioms su procedūrų ar procesų ir atitikties reguliavimui užtikrinimu, taip pat reikalingas kompetencijų rinkinys, susijęs su kelių sričių derinimu ir komunikacija tarp komandų:

- gebėti nebijoti klausti, prašyti informacijos,
- gebėti versti techninę kalbą į verslo kalbą.

Be abejo, šioms pareigybėms reikalingas ir IT žinių bazinis lygmuo, kad galėtų susikalbėti su techniniais žmonėmis.

Interviu metu, ekspertai minėjo roles ir atsakomybes, jų apibendrintos pastabos rolėms pateikiamos 3.20 lentelėje. Ekspertai pabrėžia, kad atskiros rolės aktualios didelėms įmonėms, o mažesnėje nebus išskirtos.

Ekspertai akcentavo technines ir netechnines specialistų grupes. Netechninėse paminėti duomenų saugos įgaliotiniai, informacijos saugos vadovai, atitikties reguliavimui pareigūnai ir auditoriai. Nors tarptautinėse rolių sąrangose atitiktis atskirta nuo valdymo, bet interviu išryškėjo Lietuvai būdingi rolių persidengimai. Ekspertų manymu, netechninių rolių ir specialistų poreikis padidėjo ir vis dar yra didelis dėl EU BDAR reglamento.

Techninėse grupėse išskirtas incidentų valdymas, saugumo įgyvendinimas ir kasdieninis užtikrinimas (angl. DevOps), pažeidžiamumų valdymas ir testavimas, sistemų stebėsena.

Interviu metu ekspertai neminėjo mokslo, inovacijų, grėsmių žvalgybos ar skaitmeninių nusikaltimų tyrimų, o rizikos valdymas buvo priskirtas kitoms grupėms, o ne išskirtas atskirai. Ekspertai pabrėžė, kad darbuotojų KS sampratos lygio kėlimas yra kiekvieno KS specialisto atsakomybė, o patys mokymai susiję su išsilavinimu, sertifikatais ir savarankišku tobulėjimu, naudojant nuotolinius kursus. O KS specialistų poreikis ateityje gali dar didėti dėl NIS reglamento.

3.4.2. Išvados

1. Nepaisant esamų KS rolių sąrangos standartų ir rekomendacijų, Lietuvoje KS rolės dažniausiai skirstomos į technines ir netechnines. Techninis KSS profilis smarkiai persidengia su IT funkcijomis, o pradedančiajam, net ir netechninėse pareigose, rekomenduotina turėti IT bazinių žinių rinkinį, įskaitant programavimą. Motyvacija, užsispyrimas ir domėjimasis sritimi yra kertinės savybės ateinant į sritį, nepriklausomai nuo išsilavinimo.
2. Sertifikatai darbo skelbimuose naudojami kaip filtras siekiant atbaidyti dalį kandidatų, ypač jei jie neturi patirties ar išsilavinimo. Dažniausiai tikimasi, kad darbuotojas turės platų supratimą apie IT ir bus įmonėje žmogus-orkestras.
3. Lietuvoje yra didelis patyrusių specialistų poreikis, bet įmonės ne visada nori užsiimti pradedančiųjų mokymu, o parengtą darbuotoją vilioja kitos įmonės. Mokymosi visą gyvenimą programos

3.20 lentelė. Ekspertų paminėtos KS funkcijos, rolės, jų kategorijos ir komentarai

Informacijos saugos valdymas ir procesų atitikties užtikrinimas
CISO: politikos formuotojas; IT profilis – privalumas, reikia techninių žinių, gebėti matyti rizikas, sudaryti saugumo planą, matyti specialistų poreikį. **DAP:** didėjantis specialistų poreikis dėl BDAR reglamento; būsima tendencija labiau rūpintis realiais asmens duomenų apsaugos klausimais; tinkama sritis teisininkams. **Informacijos valdymo pareigos:** procesų valdymo rolė: tinkama veikla specialistams iš kitų sričių, moterims (red. įvardijamas kruopštumas kaip savybė).

Incidento valdymas
Analitikas, SOC specialistas: pareigybės pradedančiajam, prieš pereinant į inžinierius, leidžiančios įgyti bazinių KS žinių.
Auditas
Konsultantas, auditorius: reikalauja mažiau techninių gebėjimų, bet reikia bendrųjų gebėjimų; pradeda nuo ataskaitų skaitymo, išauginami iš kitų sričių auditorių. Reikia saugos, technologijų ir vadybos pagrindų.

Mokymai
Darbuotojų lygio kėlimas yra bendrai visų pareigybių rūpestis, o ne atskiro dedikuoto žmogaus.
Įgyvendinimas
Dauguma Lietuvos KS ir IT specialistų. **Saugumo inžinierius:** įgyvendina saugumo politiką bei standartus, rūpinasi KS gynyba ir vartotojų saugumu, diegia sistemas.

Pažeidžiamumų testavimas
Gilių techninių žinių specialistai, kuriems atskira rolė būna tik didelėse įmonėse. **Pažeidžiamumų testuotojas:** siaura sudėtingesnė techninė sritis. Kol kas niekas neruošia, išauginamas iš gero analitiko, dažnai perperkamas į kitas įmones. Įsilaužėlio įvaizdis.

suteiktų dalinę galimybę specializuotis savarankiškai arba įgyti reikalingų kompetencijų pradedančiojo pozicijoms.

4. KS specialisto sritis patraukli persikvalifikuojantiems ar naujiems darbo rinkos žaidėjams, bet supratimas apie roles ir darbo funkcijas yra ribotas, pavyzdžiui, įsivaizduojamas vien techninis darbas, bet KSS turi rašyti ataskaitas ir komunikuoti su kitais specialistais. Taigi būtina išgryninti KS karjeros specifiką edukacinėje aplinkoje bei šviečiant visuomenę.

3.5. Fokus grupių tyrimas

Visuomenės apklausos rezultatai atskleidė KS srities patrauklumą moterims ir pozityvią vyrų populiacijos nuomonę apie galimybes moterims įsilieti į šį sektorių.

Siekiant įsigilinti į KS sritį įsiliejusių moterų karjeros galimybes ir sukauptas patirtis buvo organizuotos dvi fokusuotos moterų grupės, kurios pasižymėjo viena bendra charakteristika – visos į KS sritį įsiliejo iš kitų veiklos sričių.

Iš viso tyrime dalyvavo 9 respondentės. Duomenys buvo renkami fokusuotose grupėse, taikant pusiau struktūruotą interviu (žr. A.5 priedą) pagal iš anksto parengtą pokalbio planą. Pirmoji fokusuota grupė (4 respondentės) vyko 2022 m. vasario 3 d., antroji (5 respondentės) – 2022 m. vasario 10 d. Diskusijos trukmė – 1 val.

Atliekant indukcinę kokybinę turinio analizę pasirinktas manifestinis tipas, kai atskleidžiama, iš kokių komponentų susideda analizuojami tekstai. Subkategorijos ir kategorijos formuluojamos, pasitelkiant pagrindines nagrinėjamų tekstų sąvokas ir ištraukas.

3.5.1. Gauti rezultatai

Analizuojant respondentų patirtį išskirta atliekamų veiklų tema, kuri pagrįsta detalizuojant veiklos variantus (subkategorija) ir abstrahuojama (kategorija) įvardijant veiklos sritį.

Respondenčių veiklos spektras platus, apimantis šias pareigybes valstybės valdymo institucijose ir verslo organizacijose. Dominuoja projektų vadovės pareigybė, kitos pareigybės daugiau pritaikytos organizacijų specifikai: CISO informacinės saugos vadovė, regiono vadovė, valstybės valdymo institucijos padalinio vadovė, sprendžianti pažeidžiamumo problemas, viešojo administravimo atstovės, sprendžiančios KS klausimus, taip pat tarpininkės tarp techninių darbuotojų: inžinierė, inžinierių komandos vadovė, programuotoja (žr. 3.5 lentelę).

Veiklų tema pagrįsta repondentų patirtimi 1,5-15 metų profesinės veiklos laikotarpiu, kuris apėmė ne tik KS sritį. Tačiau respondentės sukauptą patirtį pritaikė naujame veiklos turinyje (KS). Sukauptos patirties indėlis į KS būtų tarpininkavimas tarp skirtingų specialistų, komandų telkimas, projektų valdymas, konsultavimas, strategijų kūrimas, teisinis išsilavinimas, informacinių technologijų išsilavinimas. Diskusijų metu įvardintos **veiklos yra universalios ir susijusios su bendrųjų kompetencijų taikymu specializuotoje srityje**. KS specifiškumas atsiranda dirbant su KS rizikų valdymu, realių grėsmių prevencija ir verslo vystymu, kuriame yra KS dalis. Valstybės valdymo institucijų atstovių veikloje atsiranda švietimo elementas, kai diegiama nulinio pasitikėjimo koncepcijas, šviečiami darbuotojai apie grėsmes ir sistemų apsaugojimą nuo kibernetinių grėsmių.

Analizuojant **KS apsibrėžimą/sampratą** raktiniu teiginiu paminėti *duomenys kaip organiza-cijų*

3.21 lentelė. Grupių patirtis KS srityje pagal atliekamas veiklas pareigybėje

Subkategorija	Kategorija
• Pardavimai • Klientų konsultavimas	KS projektų valdymas
• KS strategijos kūrimas • Teisinis KS reguliavimas, atitikimas teisinei bazei	Viešojo ir verslo sektorių bendradarbiavimo užtikrinimas
• Kliento standarto įgyvendinimas • Vadovavimas inžinierių komandoms	Atstovavimas klientams
• Skaitmeninės transformacijos koordinavimas	Verslo vystymas KS
• Rizikų vertinimas, dizainas, diegimas • KS brandos vertinimas • Klientų nusiskundimų administravimas • Penetration testing koordinavimas • Vidaus ir išorės auditai • Incidentų raportavimas • Svetainių ugniasienių tikrinimas	KS rizikų valdymas

turtas, kuris turi būti saugomas; *naudojamų informacinių sistemų nepažeidžiamumo / atsparumo / saugumo užtikrinimas nuo individualaus iki valstybės lygmens*, *rizikų valdymas*. Šie teiginiai išskleisti iliustracijomis, kurios apibūdina prevencinius veiksmus: prieigų prie duomenų higiena; teisės aktų taikymo įgūdžiai; galimos žalos įvertinimas, jei duomenys būtų prarasti; slaptažodžiai. Apibendrintai sampratoje išskiriami trys komponentai – grėsmių, kylančių ir kibernetinės erdvės numatymas, įvykusių incidentų valdymas ir priemonių incidentų užkardymui parengimas. Respondentės atkreipė dėmesį į *KS misiją*, pavyzdžiui, *„gelbėti skaitmeninį pasaulį nuo blogiečių"*.

Moterų atėjimą iš kitų sričių į KS sritį nulėmė:

- *Atsitiktinės aplinkybės* → gauti pasiūlymai; veiklos tęstinumas pasukus į saugumo užtikrinimo kryptį (veiklos duomenų apsauga)
- *Smalsumas* → perspektyvi dinamiška sritis, įdomūs projektai, noras įsigilinti, nuolatinio mokymosi galimybė, domėjimasis IT, pvz., iš diskusijos [pergudrauti hakerius yra įdomus iššūkis];
- *Persikvalifikavimas* → iš plačios teisinės srities posūkis į specializuotą KS sritį, kurioje svarbus teisinis reguliavimas;
- *Bendruomeninio gėrio kūrimas* → saugumo kūrimas, tinklaveika su kolegomis.

Išskirtinas unikalus požiūris, kuris kaip gebėjimas svarbus sektoriui apjungiant *į partnerystę bendram interesui* (saugumo užtikrinimui) interesų grupes – konsultantus, klientus, konkurentus. Įėjimui į KS sritį didelę įtaką daro ankstesnėje veikloje įgyta patirtis ir gebėjimas ją taikyti naujoje veikloje (žr.

3.22 lentelę).

3.22 lentelė. Integruotis į KS sritį padedančios kompetencijos

Subkategorija	Kategorija
• Įsiklausymas į klientą • Klientų aptarnavimas • Produktų, paslaugų pardavimai • Klientų nusiskundimų administravimas	Darbui su klientais svarbios kompetencijos
• Gebėjimas dirbti projekto įvairiose stadijose	Projektų valdymas
• Naujausių žinių paieška, gavimas • Domėjimasis tendencijomis • Žingeidumas	Nuolatinio mokymosi kompetencija
• Gebėjimas dirbti partnerystėje: konsultantai, klientai, konkurentai • Gebėjimas dirbti komandose iš organizacijos skirtingų padalinių • Gebėjimas susirasti tinkamus asmenis mokymuisi	Tinklaveikos kompetencija
• Analitinis mąstymas • Gebėjimas matyti bendrą vaizdą • Gebėjimas susikalbėti su vadovais • Planavimo gebėjimai • Gebėjimas taikyti ankstesnę įgytą patirtį • Bendradarbiavimo gebėjimai • Gebėjimas koordinuoti • Jautrumas: gebėjimas pamatyti situaciją iš įvairių perspektyvų	Bendrieji gebėjimai
• IT pradinis išsilavinimas • IT supratimas • Inžinierinis mąstymas	Specializuota techninė kompetencija
• Teisinis išsilavinimas	Specializuota kitos srities kompetencija

Diskusijose išryškėjo tiek **bendrųjų kompetencijų** (*lyderystės, komunikacijos*), tiek **specialiųjų kompetencijų** (*IT specializuotos žinios*) **įgijimo poreikis** (žr. 3.23 lentelę). Kompetencijos *įgyjamos dalyvaujant realiuose projektuose, t.y. mokantis veikloje. Diskusijose įvardinti mokymosi būdai: dalinimasis patirtimi, mokymasis vieniems iš kitų (ypač iš technines žinias turinčių kolegų), mokymasis per praktiką/veikimą, mokymasis tinkluose*.

Respondentės patvirtino, kad KS sritis (tipinė iliustracija *„nėra tik vyrų, sėdinčių su gobtuvais*

3.23 lentelė. Reikalingos įgyti kompetencijos. Poreikis

Subkategorija	Kategorija
• Vadovavimas inžinieriams	Lyderystės
• KS svarbos komunikavimas įvairioms grupėms • Operavimas/kalbėjimas srities sąvokomis	Komunikacijos
• IT žinių taikymas praktikoje • Specializuotos žinios • Sertifikatai	IT ar techninės žinios

kampe") gali būti įvairi, imponuoja srities platumas, į kurią galima atsinešti jau turimą patirtį ir įgyti naujų IT specializuotų žinių ir praktikuotis (žr. 3.24 lentelę). Nepatrauklumas sietinas su vis dar vyraujančiu stereotipiniu mąstymu, tačiau sėkmės istorijos ar sektino pavyzdžio (angl. role models) yra svarbios skleidžiant žinią apie plačias galimybes šioje srityje neapribojant srities tik techniniu išmanymu. Todėl anksčiau išskirtos komunikacijos ir lyderystės kompetencijos yra svarbios atveriant KS sritį įvairaus išsilavinimo asmenims.

3.24 lentelė. KS srities patrauklumas moterims bruožai.

Subkategorija	Kategorija
• Vyrų ir moterų žiūros skirtumai ir jų apjungimas • Dėmesys ir pagalba	Požiūrių sinergija
• Dinamiškumas • Greita kaita • Skaitmenizacijos augimas • Plati sritis, neįrėminanti	Perspektyvi sritis dalyvauti
• Dalinimasis savo istorijomis • Informacijos skleidimas augančiose amžiaus grupėse, mokyklose	Galimybės daryti įtaką būsimoms kartoms ir kitoms moterims

Moterų **konkurencingumas** šioje srityje išsiskiria *tobulumo siekiu* (pvz., iš diskusijos *„vyrams mažiau būdingas perfekcionizmas" ir turimos techninės žinios*. Konkurencingoms padeda būti įgimta *empatija* (pvz., *„pašnekovo ar piktavalio pajauta"*), išklausymas, įsiklausymas, *problemos pirminės priežasties atpažinimas, pasidalinimas žiniomis su kitais, bendradarbiavimas diplomatiškai siekiant apjungti nuomones, didesnis atsakomybės suvokimas*. Pastebėta, kad *KS srityje yra mažai dalinamasi informacija*, todėl moterų įsitraukimas į žinių sklaidą gali sustiprinti KS patrauklumą, be to, konkurencija neužgožia bendro tikslo – saugumo užtikrinimo.

Respondentės išskyrė **platų karjeros diapazoną KS srityje** – *nuo inžinierinės veiklos iki lyderystės valdant didelės apimties kompleksinius projektus*, kuriuose skaitmenizacija yra persipynusi

su KS sritimi. Diskusijose buvo išskirta ir edukacijos veikla mentorystės ir koučingo būdu, siekiant padėti daugiau moterų ateiti į KS sritį bei šviesti visuomenę nuo mažų dienų apie kibernetinės erdvės saugumo užtikrinimą.

Svarbu moterims yra *nebijoti rizikuoti, visada bandyti, dalintis informacija tinkluose, bendradarbiauti bendro tikslo link* (kaip apsisaugoti nuo hakerių), dalyvauti bendruomenėse, kuriose surandami sektini pavyzdžiai (angl. role model) ir įgyjamas pasitikėjimas (žr. 3.25 lentelę).

3.25 lentelė. Karjeros galimybės ir motyvacija likti ateityje KS

Subkategorija	Kategorija
• Inovacijos ir technologijos • Atsakinga elgsena kibernetinėje erdvėje	Domėjimasis naujovėmis
• Parodyti kitiems KS prasmę • Mokyti vaikus apie KS	Mentorystė
• Padėti į sritį ateiti daugiau moterų • Padėti į sritį ateiti daugiau specialistų • Padėti perskvalifikuoti	Koučingas
• Projektų turinys: skaitmenizacija ir KS	Dalyvavimas projektuose
• Žmonių telkimas bendram tikslui • Viešas kalbėjimas • Sektinas pavyzdys (angl. Role model)	Lyderystė

3.5.2. Išvados

Moterų fokusuotų grupių tyrimo metu nustatyta, kad KS srityje taikoma ankstesnėse veiklose įgyta patirtis yra svarbus indėlis į kibernetinių grėsmių valdymą tiek viešojo valdymo, tiek verslo organizacijose. Atsineštą patirtį apibūdinančios kompetencijos yra pakankamai universalios: projektų valdymo, lyderystės, nuolatinio mokymosi. Svarbūs respondenčių įvardinti bendrieji gebėjimai ir asmeninės savybės, kurios padeda griauti lyčių stereotipus. Moterų turimos specializuotos technologinės žinios yra privalumas, bet ne privalomumas, nes atliekant rizikų vertinimo ir jų valdymo, projektų valdymo specialisčių, ar auditorių roles svarbiau yra taikyti bendruosius gebėjimus, pavyzdžiui, gebėti telkti skirtingus asmenis bendram tikslui, veikti tinkle, dalintis turima informacija. Veiklos pradžioje esantis ir įvardintas nepasitikėjimas dėl lyčių stereotipizavimo bei technologinių žinių neturėjimo yra kompensuojamas gerai išvystytais bendraisiais gebėjimais.

3.6. Darbo skelbimų tyrimas

Žiniatinklyje esančių darbo skelbimų tyrimas – vienas iš būdų ištirti pasirinktos srities specialistų poreikį šalyje ir jiems keliamus reikalavimus. Toks tyrimas papildo ekspertų ir gyventojų apklausas ir leidžia sudaryti visapusiškesnį vaizdą apie kibernetinio ir informacinio saugumo sritį. Analogiški jungtiniai tyrimai daromi kitose šalyse, pavyzdžiui, Hall ir Rao 2020 m. tyrė darbo skelbimus ir vykdė apklausas, o po to išskyrė kompetencijų rinkinius pagal Australijos specifiką [29].

Darbo skelbimai – tai naujų darbuotojų pritraukimo įrankis, lengvai prieinamas tiek mažoms, tiek didelėms įmonėms. Darbdaviai paprastai pateikia skelbimuose išsamius reikalavimus kandidatams ir detalų pareigybių aprašymą. Šiuos duomenis galima analizuoti ne tik kokybiškai, bet ir kiekybiškai. Tokiu būdu buvo gautas gana tikslus kibernetinio ir informacinio saugumo darbo rinkos pjūvis.

Įmonių ir organizacijų veikiančių Lietuvoje žmogiškųjų išteklių poreikiai tiesiogiai siejasi su organizacinės, techninės ar programinės įrangos diegimu organizacijų veiklose. Kaip pastebi Lietuvos statistikos metraštis [19]: *2019 m. pradžioje bent vieną kibernetinio saugumo priemonę naudojo 93 proc. įmonių. Programinę įrangą (įskaitant operacines sistemas) nuolat atnaujino 79,8 proc. įmonių, atsargines duomenų kopijas laikė skirtingose vietose – 68,4 proc., taikė griežtą tapatumo (autentiškumo) patvirtinimą slaptažodžiu – 65,6 proc., vykdė tinklo prieigos kontrolę – 53,5 proc., testavo kibernetinį saugumą – 28,3 proc., taikė duomenų, dokumentų ar el. laiškų šifravimo metodus – 25,5 proc., vertino IT rizikas – 23,6 proc., atliko registracijos bylų analizę po kibernetinių incidentų – 22,5 proc.*

Įmonės, siekdamos apsaugoti savo IT sistemas, rūpinosi, kad darbuotojai žinotų kibernetiniam saugumui keliamus reikalavimus: 54,4 proc. įmonių apie reikalavimus informavo darbuotojus sudarant su jais darbo sutartis, 42,3 proc. – teikė laisvai prieinamą informaciją įmonės viduje, 21,4 proc. – organizavo privalomuosius mokymus arba privalomosios medžiagos peržiūrą. IT saugos įrangos priežiūrą įmonės dažniausiai patikėjo išorinių paslaugų teikėjams – 63,8 proc., o 46,3 proc. įmonių šį darbą atliko jų darbuotojai. 35,9 proc. įmonių turi pasirengusios dokumentaciją apie kibernetinio saugumo priemones, praktikas ar procedūras įmonėje (2017 m. – 19,4 proc.). [19]

Organizacijos Eurostat duomenimis – Lietuvoje 2021 metais buvo 52,2 tūkst. IRT darbuotojų (3,8 proc. visų dirbančiųjų) [25]. Lietuvos statistikos departamento duomenimis 2022 m. I ketvirtį šalies informacijos ir ryšių sektoriuje dirbo 41 433 žmonės [18]. Iš viso darbuotojų buvo 1 337 118, tad IRT srityje buvo įdarbinti 3,1 proc. dirbančių gyventojų. 2019 metais 8,6 proc. Lietuvos įmonių įdarbino ar ieškojo IT specialistų, o net 58,8 proc. įmonių turėjo laisvų darbo vietų IT specialistams, kurias sunku buvo užpildyti. Kaip paaiškėjo per ekspertų inverviu, įmonės dažnai ieško specialistų neformaliais kanalais, tačiau viešai prieinami darbo skelbimai yra vienas populiariausių būdų. Darbo skelbimų analizė atlikta stebint vieną stambiausių darbo skelbimų portalą Lietuvoje CVOnline bei tarptautinį profesinį socialinį tinklą LinkedIn.

Darbo skelbimai buvo rinkti vienerius metus keturiais etapais (žr. lentelę 3.26, [6]). Iš viso buvo peržiūrėti 4023 skelbimai „Informacinių technologijų" kategorijoje internetiniame portale CV-Online bei tarptautiniame profesiniame socialiniame tinkle LinkedIn. Ieškant skelbimų LinkedIn tinkle buvo pasirinktas papildomas ieškos kriterijus - darbo vieta Lietuvoje. IT srities darbo skelbimuose 171 (t.y. 7,5 proc. nuo visų IT skelbimų) buvo tiesiogiai susijęs su kibernetinio ir/ar informacinio saugumo specialistų pozicijomis.

Pažymėtina, kad kiekvienos imties metu kibernetinio saugumo specialistų poreikis buvo skirtingas. Tai gali būti susiję su COVID-19 pandemija ir jos poveikiu darbo rinkai. Dėl to išsamiai darbo skelbimų analizei buvo pasirinktos 2022-04-10 dienos CV-Online ir LinkedIn imtys. Šią dieną Lietuvoje ir daugelyje Europos Sąjungos šalių jau buvo atšaukti dauguma su COVID-19 susijusių ribojimų (oficialiai valstybės lygio ekstremalioji situacija dėl koronaviruso infekcijos plitimo grėsmės Lietuvoje atšaukta 2022 m. gegužės 1 d.).

Į išsamiąją analizę papildomai įtraukti keturi "Danske Bank" svetainėje 2022-04-10 dieną surasti darbo skelbimai, siūlantys pozicijas kibernetinio ir/ar informacinio saugumo specialistams. Tokiu būdu surastų kibernetinio/informacinio saugumo darbo skelbimų, pateiktų 2022 metų balandžio mėnesį, skaičius lygus 94-iems.

3.26 lentelė. Atrinktų tyrimui darbo skelbimų kiekis

Data	Skelbimų svetainė	IT skelbimų skaičius	KS skelbimų skaičius	KS skelbimų dalis
2021-03-28	CV-Online	936	14	1,5 proc.
2021-05-03	LinkedIn	126	23	18,3 proc.
2021-07-01	CV-Online	908	21	2,3 proc.
2021-07-01	LinkedIn	181	23	12,7 proc.
2022-04-10	CV-Online	1072	42	3,9 proc.
2022-04-10	Danke Bank	n/d	4	n/d
2022-04-10	LinkedIn	800	48	6,0 proc.
Iš viso:		4023	175	vidurkis 7,5 proc.

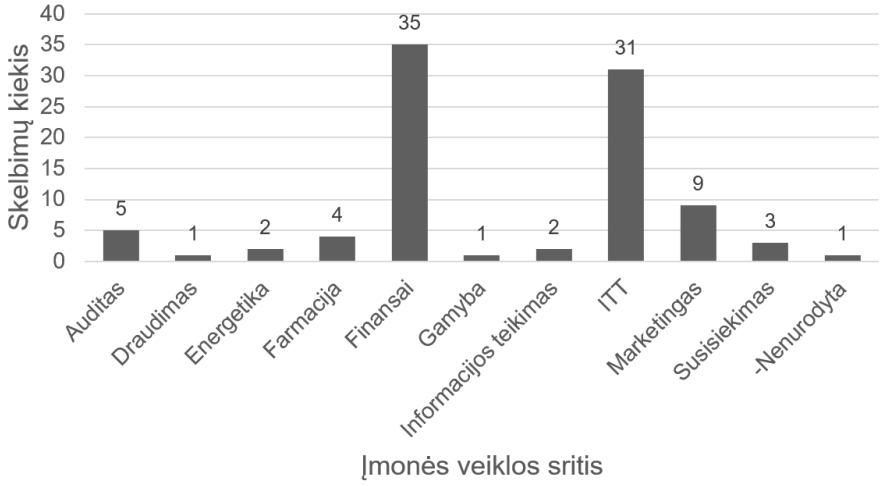
3.6.1. Gauti rezultatai

Kibernetinių specialistų trūkumas darbo rinkoje

2022 metų balandžio 10 dieną buvo ieškomi 1872 IRT specialistai. Organizacijos Eurostat duomenimis – Lietuvoje 2021 metais buvo 52,2 tūkst. IRT darbuotojų (3,8 proc. nuo visų dirbančiųjų) [25]. Remiantis CV-Online ir LinkedIn darbo skelbimų pjūviu galima daryti išvadą, kad šalies IRT darbo rinkai 2022 m. balanžio mėn. trūko 3,6 proc. darbuotojų.

5 procentai IRT darbo skelbimų buvo susiję su kibernetinio/informacinio saugumo sritimi. Kitais žodžiais, 2022 metų antrame ketvirtyje maždaug kas dvidešimtas naujas IRT specialistas turėjo pradėti dirbti kibernetinio saugumo specialisto pareigose. Jeigu remsimės LinkedIn paieškos duomenimis, pagal kuriuos Lietuvoje yra šiek tiek virš 1000 KS specialistų, tai Lietuvoje 2022 metų pradžioje buvo ieškoma apie 15 proc. nuo bendro KS specialistų skaičiaus.

Daugiausiai kibernetinio saugumo specialistų ieškojo IRT (33 proc. darbo skelbimų, žr. 3.7 pav.) ir finansų (36 proc.) įmonės. Šios specialybės darbuotojų taip pat trūko finansų valdymo, draudimo, informacijos teikimo (valstybinis sektorius), susisiekimo, farmacijos, audito, energetikos, marketingo ir gamybos sektoriuose (30 proc.). Pažymėtina, kad beveik 10 procentų darbo skelbimų įmonės ieškojo specialisto, teikiančio konsultacijas kibernetinio/informacinio saugumo klausimais išoriniams klientams.



3.7 pav. Skelbimų pasiskirstymas pagal įmonių veiklos sritį

Daugiausiai ieškomi patyrę specialistai

Rasti kibernetinio darbo skelbimai buvo surūšiuoti pagal ieškomų specialistų lygį. Skelbimų antraštėje dažnai nurodomas pozicijos lygis, pvz., angliškais žodžiais „junior" (pradedantysis), „mid" (patyręs) ir „senior" (vyriausiasis). Pastarajai darbuotojų kategorijai paprastai priskiriami ir vadovai (angl. *lead* arba *manager*). Pareigų lygį galima identifikuoti ir pagal keliamus reikalavimus patirčiai, kvalifikacijai, siūlomą atlyginimą.

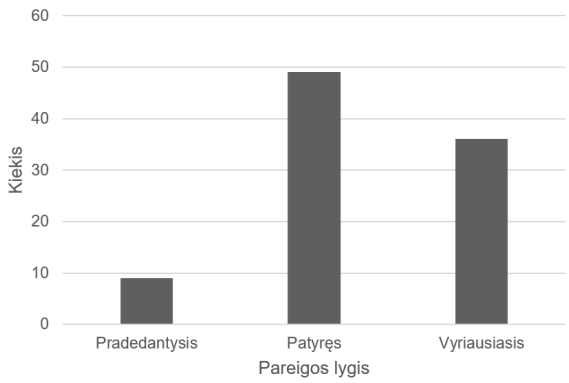
Darbo skelbimuose dominuoja patyrusių ir vyriausiųjų kibernetinio ir informacinio saugumo specialistų pozicijos (žr. 3.8a pav.). Siūlymai dirbti pradedančiųjų pozicijose sudarė 9,6 proc. visų darbo skelbimų. Dauguma įmonių ieško patirtį turinčių specialistų (vienas arba daugiau praktinės patirties metų kibernetinio/informacinio saugumo srityje, kartais – IT srityje, žr. 3.8b pav.).

Tik 7 darbo skelbimuose iš 94 iš pretendentų nereikalaujama praktinės patirties (tokiu atveju įprastai siūloma pradedančiojo pozicija). Kartais patirtis apibrėžiama ne konkrečiais metais, bet būdvardžiais

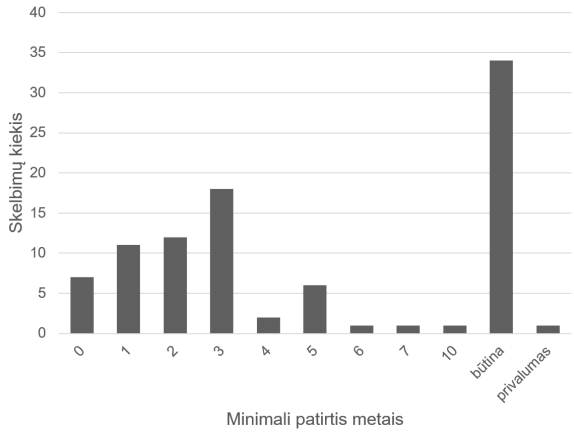
„didelė" arba „gili" (angl. strong knowledge, excellent understanding). Daugelyje skelbimų nurodoma ne tik minimali patirtis, bet ir jos rėžiai, pvz., „3-5 metai", arba prie metų prirašomas "+" ženklas (pvz., „3+"). Skelbimuose keliami pretendentams patirties ir lygio reikalavimai leidžia padaryti išvadą, kad įmonėse daugiausia galimybių įsidarbinti turi patyrę, kelis metus kibernetinėje srityje pradirbę specialistai.

Darbo skelbimais daugiausia ieškomi patyrę, bent kelerių metų darbo patirtį turintys kibernetinio saugumo specialistai.

Ieškantiems patyrusių darbuotojų patartina vengti rašyti darbo skelbimuose tikslų patirties metų skaičių. Tada nebus atbaidyti potencialiai geri, tačiau formaliai netinkantys kandidatai.



(a) Ieškomas pareigų lygis



(b) Kandidato minimali patirtis metais

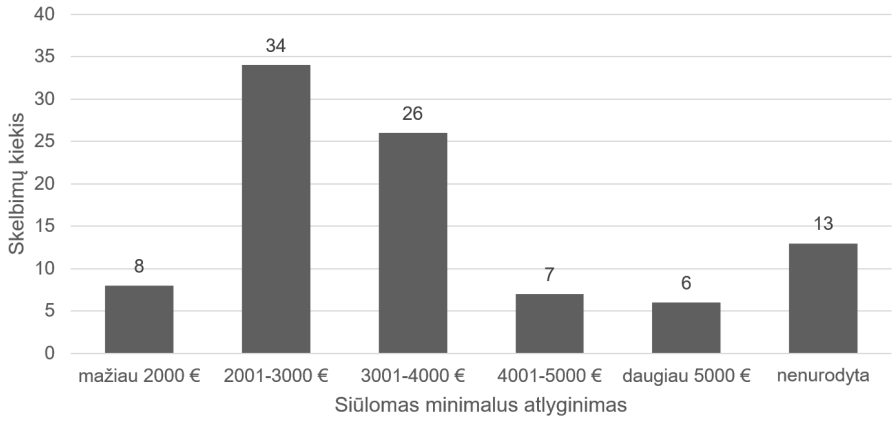
3.8 pav. Skelbimų pasiskirstymas pagal ieškomas pareigas ir patirtį, bendras skelbimų kiekis – 94

Atlyginimų žirklės valstybinėse įmonėse

Darbo skelbimuose dominavo 2000–3000 EUR minimalus bruto atlyginimas (36 proc. skelbimų, žr. 3.9 pav.). Į tokį atlyginimą gali pretenduoti minimalius reikalavimus atitinkantis patyręs arba pradedantysis kandidatas. Aukštesnes pareigas užimančių kibernetinio saugumo specialistų algos prasideda nuo 3000–4000 eurų. Užmokesčio ribos gali būti nenurodomos (14 proc. skelbimų minimalios ir 27 proc. – maksimalios algos atveju), paliekant laisvę deryboms.

Kaip matyti iš 3.27 lentelės, privačiose įmonėse, lyginant su valstybinėmis, specialistams siūlomas ne tik didesnis minimalus, bet ir maksimalus atlygis. Šis atlyginimų skirtumas pastebėtas tiek patyrusių, tiek vyriausiųjų specialistų atveju. Privačioje įmonėje kibernetinio saugumo specialistas vidutiniškai gali gauti nuo 15 iki 53 proc. didesnį atlyginimą. Be to, pradedantysis specialistas potencialiai gali gauti didesnį atlyginimą nei patyręs valstybinėje.

Privatūs darbdaviai vilioja specialistus ne tik aukštesniais atlyginimais, bet ir papildomais priedais, darančiais darbo vietą dar patrauklesnę (ypač jaunimui). Keletas būdingų pavyzdžių:



3.9 pav. Skelbimų pasiskirstymas pagal siūlomą minimalų atlyginimą (prieš mokesčius). Bendras skelbimų kiekis – 94

- lankstus darbo grafikas, galimybė dalį laiko dirbti nuotoliniu būdu;
- nemokama kava, arbata, užkandžiai;
- pigesnis sporto klubo abonementas, nemokamos jogos pamokos;
- papildomos atostogų dienos, laisva diena gimtadieniui;
- fiksuotas arba neribotas biudžetas profesiniams kursams, knygoms;
- papildomas sveikatos draudimas;
- vienkartinis biudžetas nuotolinei darbo vietai įkurti;
- galimybė atsivesti į biurą augintinį.

Galbūt valstybinės įmonės irgi siūlo panašius arba kitus priedus, tačiau darbo skelbimuose jie neminimi.

Rekomendacija valstybinėms įmonėms: darbo skelbimuose būtinai paminėti papildomus priedus, kuriuos gali gauti naujas darbuotojas. Taip pat būtinai pateikti svarią priežastį, kodėl valstybinėje įmonėje dirbti verta labiau nei privačioje.

3.27 lentelė. Minimalaus ir maksimalaus siūlomo atlyginimo (bruto) skirtumai privačiose ir valstybinėse įmonėse

	Minimalaus atlyginimo vidurkis		**Maksimalaus atlyginimo vidurkis**	
Pareigybės lygis	Privati įmonė	Valstybinė įmonė	Privati įmonė	Valstybinė įmonė
Pradedantysis	1881		3476	
Patyręs	2842	2213	5083	3318
Vyriausiasis	4282	3583	6153	5374

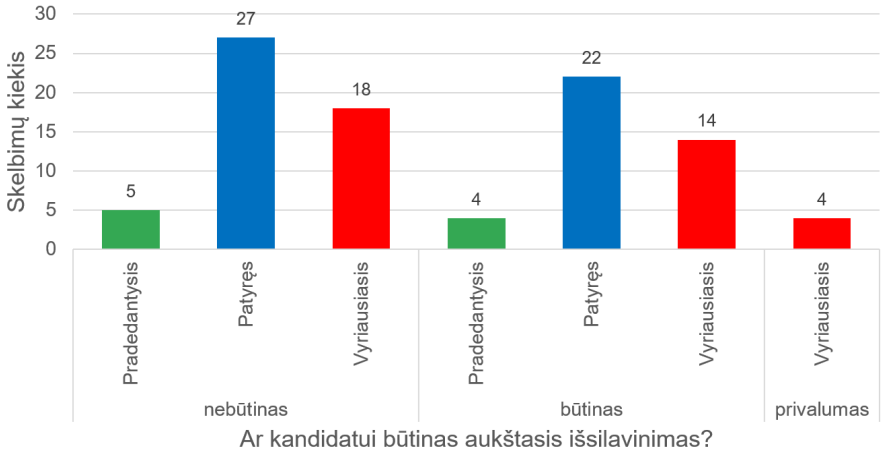
Aukštasis išsilavinimas nebūtinas

Daugiau nei pusėje darbo skelbimų (53 proc.) iš kandidatų nereikalaujama turėti aukštąjį išsilavini-

mą (žr. 3.10 pav.). Toks pasiskirstymas pastebėtas visų lygių specialistų atveju. Keliuose skelbimuose (4 iš 94) aukštasis išsilavinimas laikomas privalumu. Pastebėsime, kad tai prieštarauja visuomenėje vyraujančiai nuomonei, kad KS specialistu savarankiškai tapti yra sunku.

Jei iš kandidato į darbo vietą reikalaujamas aukštasis išsilavinimas, tuomet dažniausiai IRT srities bakalauro arba magistro diplomas – 37 iš 44 skelbimų (85 proc.). Kartais aukštąją išsilavinimą galima „pakeisti" industriniais sertifikatais arba patirtį įrodančiais dokumentais.

Darbo rinkoje aukštasis išsilavinimas nėra pagrindinis darbuotojo atrankos kriterijus - žymiai svarbiau turėti praktinę patirtį.



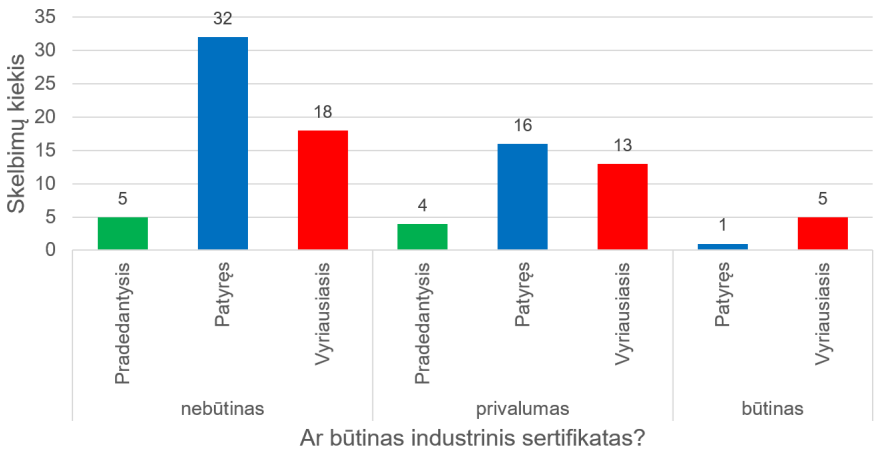
3.10 pav. Skelbimų pasiskirstymas pagal kandidatui keliamą reikalavimą išsilavinimui. Bendras skelbimų kiekis – 94

Industriniai sertifikatai - tik kaip privalumas

Viena iš įdomesnių darbo skelbimo analizės išvadų - iš kandidatų retai reikalaujama turėti industrinį sertifikatą. Tokių skelbimų buvo tik 6 iš 94 (6 proc., žr. 3.11 pav). Tai nereiškia, kad sertifikatai iš viso yra ignoruojami. Trečdalyje darbo skelbimų sertifikatai išskiriami kaip privalumas (35 proc. atvejų). Pokalbio su ISACA skyriaus Lietuvoje vadovais metu jie šį faktą komentavo tuo, kad organizacijos šiuo metu dėl bendro KS specialistų trūkumo yra sumažinusios savo reikalavimus, tačiau tikisi, kad ateityje tai gali pasikeisti.

Verta atkreipti dėmesį, kad darbo skelbimuose sertifikatas gali būti reikalaujamas vienodai tiek iš patyrusio, tiek iš pradedančiojo specialisto. Tai gali apsunkti pradedančiųjų specialistų paiešką. Lentelėje 3.28 pateikti darbo skelbimuose minimi industriniai kibernetinio/informacinio saugumo sertifikatai.

Populiariausi tarp darbdavių yra (ISC)^2 sertifikatas CISSP (Certified Information Systems Security Professional), ISACA išduodami CISM (Certified Information Security Manager) ir CISA (Certified Information Systems Auditor), „EC-Council" sertifikatas CEH ir „Offensive Security" siūlomas OSCP (Offensive Security Certified Professional).



3.11 pav. Reikalavimai turėti industrinį sertifikatą darbo ieškos skelbimuose. Bendras skelbimų kiekis - 94

Svarbūs bendravimo įgūdžiai

Dažnas nepatyręs kibernetinio saugumo specialistas klaidingai mano, kad jo specialybė susijusi tik su techninėmis žiniomis. Tikrovėje, šioje srityje dirbančiam personalui tenka dažnai bendrauti su bendradarbiais, kitų specializacijų kolegomis ir vadovais, taip pat nuolatos rašyti įvairias ataskaitas. Tad nieko nuostabaus, kad darbo skelbimuose „minkštieji gebėjimai" dažnai minimi pareigybių aprašyme ir/arba reikalavimuose kandidatams. Pavyzdžiui, iš 48 nagrinėtų „LinkedIn" svetainėje paviešintų darbo paieškos skelbimų, mažiausiai 19-oje (40 proc.) iš kandidato buvo tikimasi gerų komunikavimo įgūdžių, o 6-iuose (13 proc.) – ataskaitų rašymo įgūdžių. 18-oje skelbimų (38 proc.) kaip viena iš pareigų nurodomas ataskaitų vadovybei ar/ir kitiems įmonėms darbuotojams ruošimas.

Įmonės gana dažnai tikisi, kad kandidatai į kibernetinio saugumo specialisto pareigas sugebės konsultuoti arba net apmokyti kitose srityse plušančius kolegas saugumo pagrindų (34 proc. visų analizuotų darbo skelbimų). Dar viena neretai iš pretendento laukiama profesinė savybė - žingeidumas, siekis tobulėti savo srityje.

Darbo skelbimų analizė patvirtino „mažos šalies sindromo" hipotezę. Lietuvoje įmonės kibernetinio saugumo specialistui dažnai nori užkrauti per daug pareigų. Susiejus skelbimuose aprašomas darbuotojo pareigybines funkcijas su amerikietišku NIST NICE rolių modeliu, paaiškėjo, kad vidutiniškai pretendentas į kibernetinio/informacinio saugumo poziciją turėtų atlikti 7,8 NICE rolės (žr. 3.12 pav.). Buvo tik vienas skelbimas, kuris ieškojo siauros specializacijos darbuotojų (NICE rolių kiekis darbo

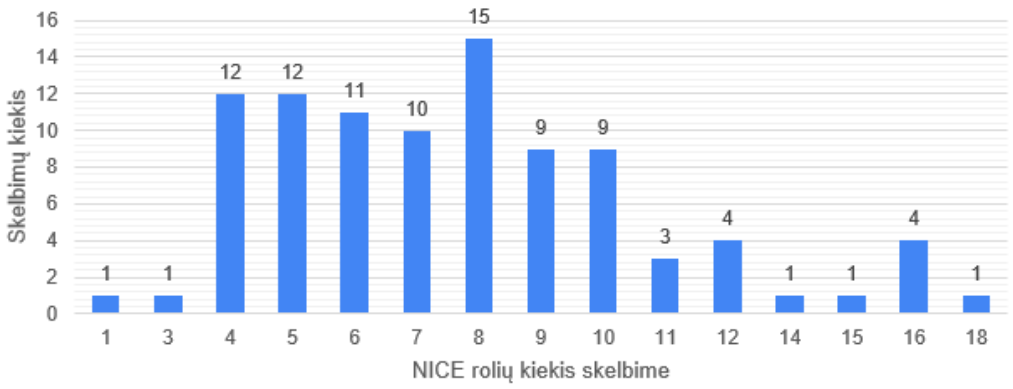
3.28 lentelė. Kaip dažnai darbo skelbimuose minimi industriniai sertifikatai

Sertifikatas	Skelbimų kiekis	Sertifikatas	Skelbimų kiekis
AWS Certified Advanced Networking	2	GCFA	1
AWS Certified Security	1	GCFE	1
AWS Certified Solution Architect	1	GCIA	3
BCMII	1	GCIH	4
CASE	1	GCSA	2
CCSE	1	GIAC	2
CCSP	1	GPEN	1
CEH	**8**	GSLC	1
Certified Kubernetes Security Specialist	1	GWEB	1
CIPM	2	GXPN	1
CIPP/E	2	HBSS	1
CISA	**6**	Internal Seccurity Assesor (ISA)	1
Cisco CCNA Security	1	ISO27001 Lead Auditor/Implementer	1
Cisco Security	2	ISSAP	3
CISM	**10**	ISSEP	1
CISSP	**15**	ISSMO	1
CompTIA Cloud+	1	ITIL	1
CRISC	4	LPT	1
CRTP	2	Network+	2
CSSLP	1	NSA	1
DRII	1	OSCE	1
E|CIH	1	**OSCP**	**6**
ECPC-B DPO	1	OSED	2
eCPPT	2	OSWE	2
eCPTX	2	PCSAE	1
eWPT	2	PNCSE	1
Fortinet FortiGate NSE4	1	Security+	4

skelbime - vienas). Pasitaikė ir tokių įmonių, kurių darbo skelbimuose minimos 16 arba net 18 rolių. Priminsime, kad maksimalus mūsų tyrime naudojamas NICE rolių kiekis yra 41.

> *Lietuvoje kibernetinio saugumo specialistas vidutiniškai turi atlikti aštuonių amerikiečių arba trijų europiečių specialistų funkcijas.*

Pradedantiesiems rolių kiekis įprastai skiriamas mažesnis, nei patyrusiems arba vyriausiesiems. Taip pat pastebėta tendencija, kad kuo didesnė privati įmonė arba kuo daugiau vienu metu ji ieško personalo, tuo siauresnės specializacijos kibernetinio saugumo darbo skelbimai. Ypač tai matyti tuomet, kai įmonė formuoja atskirą kibernetinio ar informacinio saugumo padalinį.



3.12 pav. Kiek NICE rolių turėjo vykdyti pretendentai darbo skelbimuose

3.29 ir 3.30 lentelėse pateiktos dažniausiai ir rečiausiai minimos darbo paieškos skelbimuose NICE rolės. Daugiau nei pusė skelbimų (58 proc.) darbdaviai tikisi iš naujo darbuotojo nuolatinės sistemų saugumo analizės (angl. Systems Security Analyst). Ne ką rečiau (53 proc.) įmonės nori, kad saugumo specialistas kurtų informacinių sistemos saugumą (Information Systems Security Developers). Ši rolė dažniausiai pasitaiko IRT arba finansų sektoriuje, kai bendrovė nuolatos vysto arba diegia naują programinę įrangą.

Neretai iš kibernetinio saugumo specialisto tikimasi, kad jis vertins saugumo riziką (NICE rolė Security Control Assessor, 49 poc.) bei mažiau arba daugiau prisidės prie kibernetinio saugumo politikos ir strategijos kūrimo (angl. Cyber Policy and Strategy Planner, 45 proc. visų darbo skelbimų). Pastaroji rolė skelbimo tekste kartais formuluojama, kaip „pagalba aukštesnei vadovybei strategijos kūrimo klausimais".

Darbo skelbimuose incidentų valdymas (angl. Cyber Defense Incident Responder, 45 proc.) ir pažeidžiamumų vertinimas (angl. Vulnerability Assessment Analyst, 44 proc.) retai išskiriami kaip vienintelės darbuotojo rolės. Tendencija tokia, kad jas norima užkrauti tam pačiam specialistui lygiagrečiai dar kelioms vykdomoms pareigoms. Kitos, irgi dažnai minimos rolės yra sistemų testavimas (angl. System Testing and Evaluation Specialist, 42 proc. darbo skelbimų), grėsmių analizė (angl. Threat/Warning Analyst, 40 proc.), programų saugumo vertinimas (angl. Secure Software Assessor,

38 proc.) bei kibernetinės gynybos infrastruktūros palaikymas (angl. Cyber Defense Infrastructure Support Specialist, 37 proc.).

Remiantis darbo skelbimais, galima padaryti prielaidą, jog dėl šalyje veikiančių įmonių nedidelio dydžio NIST NICE rolių modelis yra per daug detalus ir Lietuvai netinka.

3.29 lentelė. Dažniausiai minimos NICE rolės darbo skelbimuose (bendras skelbimų skaičius – 94)

NICE rolė	Skelbimų kiekis
1. Duomenų ir sistemų administravimo veiklos -> Sistemų saugumo analizė (angl. Systems Security Analyst)	54
2. Saugių produktų ir sistemų kūrimo veiklos -> Sistemų kūrimas: Informacinių sistemų saugumo kūrimas (angl. Information Systems Security Developers)	50
3. Saugių produktų ir sistemų kūrimo veiklos -> Rizikos valdymas: Saugumo priemonių vertinimas (angl. Security Control Assessor)	46
4. Planavimo, vadovavimo ir priežiūros veiklos -> Strateginis planavimas: Kibernetinio saugumo politikos ir strategijos kūrimas (angl. Cyber Policy and Strategy Planner)	42
5. Apsaugos ir gynybos veiklos -> Incidentų valdymas: Reagavimas į incidentus (angl. Cyber Defense Incident Responder)	42
6. Apsaugos ir gynybos veiklos -> Pažeidžiamumų vertinimas ir analizė (angl. Vulnerability Assessment Analyst)	41
7. Saugių produktų ir sistemų kūrimo veiklos -> Testavimas ir vertinimas: Testavimas (angl. System Testing and Evaluation Specialist)	39
8. Apsaugos ir gynybos veiklos -> Grėsmių analizė (angl. Threat/Warning Analyst)	38
9. Saugių produktų ir sistemų kūrimo veiklos -> Programų kūrimas: Programų saugumo vertinimas (angl. Secure Software Assessor)	36
10. Apsaugos ir gynybos veiklos -> Kibernetinės gynybos infrastruktūros palaikymas (angl. Cyber Defense Infrastructure Support Specialist)	35
11. Saugių produktų ir sistemų kūrimo veiklos -> Sistemų architektūra: Saugumo architektūros projektavimas (angl. Security Architect)	34
12. Planavimo, vadovavimo ir priežiūros veiklos -> Kibernetinio saugumo mokymų kūrimas/instruktavimas (angl. Cyber Instructional Curriculum Developer / Instructor / Educator)	32
13. Apsaugos ir gynybos veiklos -> Kibernetinės gynybos analizė - analizuoja įvykius (pagal gautus kitų sistemų duomenis) (angl. Cyber Defense Analyst)	31

Darbo skelbimuose aprašytų NICE rolių analizė taip pat patvirtino jau ne kartą šioje ataskaitoje nagrinėtą kibernetinio saugumo mokslininkų (angl. Researcher, 0 proc.) ir teisininkų (angl. Cyber Legal Advisor, 0 proc.) poreikio trūkumą. Sprendžiant iš CV-Online ir LinkedIn svetainių analizės, įmonės tokių specialistų neieško. Tačiau šios ataskaitos autoriai neatmeta galimybės, kad toks poreikis vis tik Lietuvoje yra ir jį būtų galima identifikuoti ateityje atlikus visapusišką darbo skelbimų analizę, įtraukiant daugiau šaltinių ir apimant visas pramonės ir paslaugų sritis.

Nepopuliari darbo skelbimuose ir technologijų tyrimų ir plėtros rolė (angl. Research and Development Specialist, 2 proc. visų skelbimų). Jos užuominų skelbimo tekste galima rasti, pvz., kai įmonė tikisi, kad darbuotojas „tobulins savo profesines žinias" arba „seks saugumo naujienas", tačiau gilesnių tyrimų iš specialisto nėra reikalaujama.

Darbo skelbimuose retai minimas privatumo reikalavimų palaikymas ir užtikrinimas (angl. Privacy Officer/Privacy Compliance Manager, 2 proc.). Tai indikuoja kibernetinio saugumo sektoriaus Lietuvoje brandos stoką. [2, 53]

3.30 lentelė. Rečiausiai minimos NICE rolės darbo skelbimuose (bendras skelbimų skaičius – 94)

NICE rolė	Skelbimų kiekis
33. Planavimo, vadovavimo ir priežiūros veiklos -> IT investicijų portfelio valdymas (angl. IT Investment/Portfolio Manager)	3
34. Apsaugos ir gynybos veiklos -> Kibernetinė žvalgyba (angl. Cyber Intel Planner)	3
35. Duomenų ir sistemų administravimo veiklos -> Duomenų bazių valdymo sistemų administravimas (angl. Database Administrator)	3
36. Planavimo, vadovavimo ir priežiūros veiklos -> Vadovavimas, privatumo reikalavimų palaikymas ir užtikrinimas (angl. Privacy Officer/Privacy Compliance Manager)	2
37. Planavimo, vadovavimo ir priežiūros veiklos -> Vadovavimas komunikacinių sistemų saugumo klausimais (angl. Communications Security (COMSEC) Manager)	2
38. Saugių produktų ir sistemų kūrimo veiklos -> Testavimas ir vertinimas: Technologijų tyrimai ir plėtra (angl. Research and Development Specialist)	2
39. Planavimo, vadovavimo ir priežiūros veiklos -> Kibernetinio saugumo juridinės konsultacijos (angl. Cyber Legal Advisor)	0
40. Duomenų ir sistemų administravimo veiklos -> Žinių valdymas (angl. Knowledge Manager)	0
41. Saugių produktų ir sistemų kūrimo veiklos -> Moksliniai tyrimai ir inovacijos (angl. Researcher)	0

ENISA ECSF rolės: norima „darbių-devyndarbių"

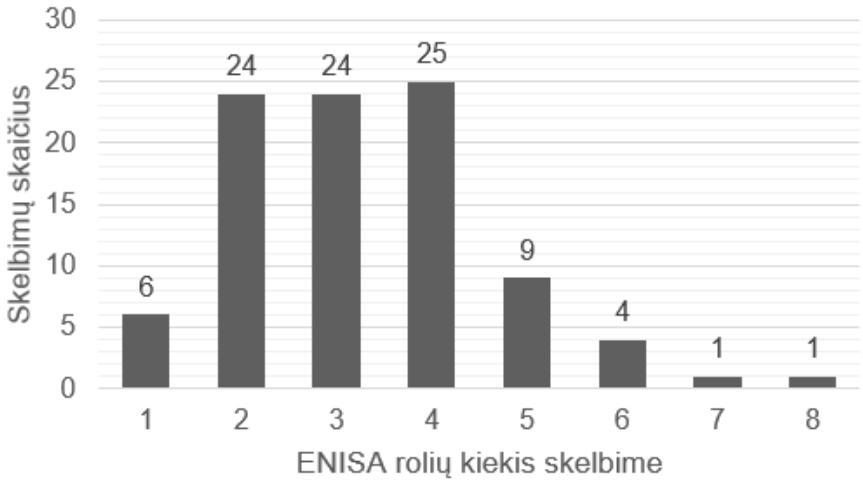
ENISA kuriamas kibernetinio saugumo rolių sąrašas (ECSF, 1.1 lentelė) yra gerokai trumpesnis už NIST NICE sąrašą. 41-a NICE rolė Europos sąjungos erdvei pritaikytame modelyje sutrauktos iki 12-os. Sprendžiant iš darbo skelbimų analizės rezultatų, Lietuvos įmonės KS specializacijų sąrašą norėtų dar labiau sutrumpinti apjungdamas kelias ENISA roles į vieną.

Darbo skelbimuose vienam kibernetinio saugumo specialistui vidutiniškai priskiriama 3,1 ENISA rolė (žr. 3.13 pav.). 77 procentuose skelbimų ieškomas darbuotojas turėjo atlikti nuo dviejų iki keturių ENISA rolių.

ENISA rolių populiarumas koreliuoja su NICE NIST rolėmis. Ieškomiausia ENISA rolė yra vyr. informacijos saugos vadovas (CISO, E1). Ši rolė buvo paminėta 56 proc. visų nagrinėtų darbo skelbimų (žr. lentelę 3.31). Toliau pagal populiarumą seka rizikos vertintojai bei valdytojai (E10, 46 proc.), saugių sistemų įgyvendintojai (E8, 45 proc.), organizacijos saugumo ir procedūrų/procesų auditoriai (E6, 44 proc.) ir aktyvios pagalbos teikėjai (E2, 41 proc.). Tuo tarpu teisės, politikos ir atitikties pareigūnų reikia mažiausiai (E3, 2 proc. visų skelbimų). Įmonės pakankamai retai ieško ir grėsmių žvalgybos pareigūnų (E4, 9 proc.).

Jei tame pačiame darbo skelbime minimos kelios ENISA rolės, ne visos jos turi vienodą svorį. Kai kurios rolės akcentuojamos labiau nei kitos, kai kurios aprašytos nepilnai. 3.14a pav. pateiktas skelbimų skaičius, kuriame ENISA rolės minimos pagrindinių pareiginių funkcijų apraše. Čia irgi „paklausiausia" E1 rolė (CISO, 44 proc.), tačiau toliau seka E6 (organizacijos saugumo ir procedūrų/procesų auditoriai, 34 proc.), o ne E10, kaip buvo galima tikėtis iš lentelės 3.31. E10 rolė kaip pagrindinė minima kiek daugiau nei ketvirtyje (27 proc.) darbo skelbimų. Trečioje vietoje išliko E8 (saugių technologinių ir programinių sistemų įgyvendintojai, 33 proc.).

Įdomiai pasiskirstė ENISA rolės pagal dažnumą antraeilių pareiginių funkcijų aprašymuose (Pav. 3.14b).



3.13 pav. Kiek ENISA rolių paminėta darbo skelbimuose

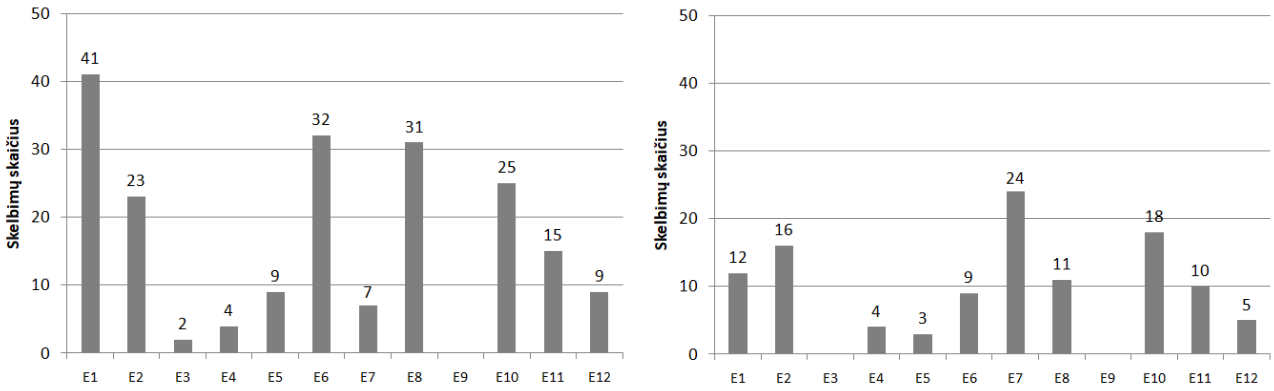
3.31 lentelė. ENISA rolių „populiarumas" (kaip dažnai paminėta) darbo skelbimuose. Bendras skelbimų skaičius – 94

Vieta	ENISA rolė	Skelbimų kiekis
1	E1. Vyr.informacijos saugos vadovas (CISO)	53
2	E10. Rizikos valdytojas	43
3	E8. Saugių sistemų kūrėjas (įgyvendintojas)	42
4	E6. Organizacijos saugumo ir procedūrų/procesų auditorius	41
5	E2. Aktyvios pagalbos teikėjas (incidento metu)	39
6	E7. Kibernetinio saugumo ugdytojas	31
7	E11. Skaitmeninių nusikaltimų tyrėjas	25
8	E12. Organizacijos kibernetinio/fizinio saugumo, perimetro pažeidžiamumų testuotojas	14
9	E5. Saugumo architektas	12
10	E4. Grėsmių žvalgybos pareigūnas	8
11	E3. Teisės, politikos ir atitikties pareigūnas	2

Iš naujų darbuotojų dažniausiai tikimasi, kad jie, be pagrindinių darbų, papildomai mokys kolegas (E7 rolė, 26 proc.), vertins/valdys rizikas (E10, 19 proc.) arba tirs incidentus (E2, 17 proc.).

Jeigu roles grupuotume į dvi kategorijas – labiau netechnines (E1, E3, E6, E10) ir labiau technines (likusios 8 ENISA rolės), tada pamatytume, kad pagal pagrindines roles, organizacijos ieško vienodai netechninių ir techninių specialistų (49,5 proc. netechninių ir 50,5 proc. techninių), tačiau pagal antraeiles roles, dominuoja techninės (iš visų antraeilių rolių, netechninės sudaro tik 35 proc., o techninės – beveik dvigubai daugiau, 65 proc.). Kitaip tariant, yra didelė tikimybė (pagal atliktą analizę, ši tikimybė yra 34 proc.), kad netechninėms rolėms priimamas žmogus papildomai turės atlikti ir techninio specialisto darbą. Tiesą sakant, net iš 25 proc. vadovų (CISO) buvo prašoma papildomai vykdyti kurios nors techninės rolės darbą.

> Remiantis darbo skelbimais, vienas iš keturių aukščiausio lygio kibernetinio saugumo vadovų (CISO) papildomai turi dirbti ir techninio specialisto darbą.



(a) Pagrindinė ENISA rolė

(b) Antraeilė ENISA rolė

3.14 pav. Kaip dažnai ENISA rolės minimos skelbimuose pagrindinių ir antraeilių pareiginių funkcijų aprašymuose. Bendras skelbimų kiekis – 94

3.6.2. Išvados

1. 2022 metų pradžioje Lietuvoje per skelbimų portalus buvo ieškoma beveik 2000 IRT sektoriaus darbuotojų (virš 3,6 proc. nuo visų šiame sektoriuje dirbančiųjų) ir beveik 200 KS specialistų (apie 15 proc. nuo dirbančių KS specialistų).
2. 90 proc. KS skelbimų ieško patyrusių (bent keleto metų darbo patirtį šioje srityje turinčių) specialistų. Remiantis ekspertų interviu, jaunuosius specialistus įmonės pritraukia kitais būdais (pvz., suteikdamos praktikos vietas studentams), arba (remiantis vadovų apklausa) tiesiog permeta šias funkcijas IT specialistams.
3. Privačios įmonės siūlo nuo 15 iki 53 proc. didesnius atlyginimus KS specialistams, negu valstybinės įmonės. Privačios įmonės papildomai siūlo įvairius nefinansinius priedus.

4. Tik pusė KS darbo skelbimų iš pretendentų reikalauja turėti aukštojo mokslo diplomą, ir tik 6 proc. skelbimų reikalauja industrinių sertifikatų. Sertifikatai yra privalumas (įvardijami 54 skirtingi sertifikatai). Jeigu diplomo reikalaujama, tai greičiausiai bus IRT srities bakalauro arba magistro diplomas (85 proc. tarp diplomo reikalaujančių skelbimų). Ekspertai nurodo, kad reikalavimai gali griežtėti ateityje, jeigu į Lietuvą migruos kitų šalių IT specialistai (tai šiuo metu yra tikėtina).
5. Iš KS specialistų tikimasi ne tik gerų techninių žinių, bet ir "minkštųjų" kompetencijų: apie 40 proc. skelbimų reikalauja gerų komunikavimo ir ataskaitų rašymo įgūdžių.
6. Tarptautinės rolių klasifikavimo sistemos (NIST NICE, ENISA ECSF) Lietuvoje netinka. Vienas darbuotojas Lietuvoje vidutiniškai turi vykdyti bent 3 ENISA ECSF rolių arba 8 NICE rolių funkcijas.
7. Įmonės daugiausia ieško vyr. informacijos saugos vadovo (CISO), mažiausiai – kibernetinės teisės pareigūno, ir nė viena neieško kibernetinės srities mokslininko.
8. Organizacijos ieško apylygiai specialistų netechninėms (CISO, Auditoriaus, Rizikos valdytojo, Teisės ar atitikties pareigūno) ir techninėms rolėms, tačiau net trečdalio netechninių specialistų prašoma atlikti ir techninių rolių funkcijas.

4. Kompetencijų žemėlapis

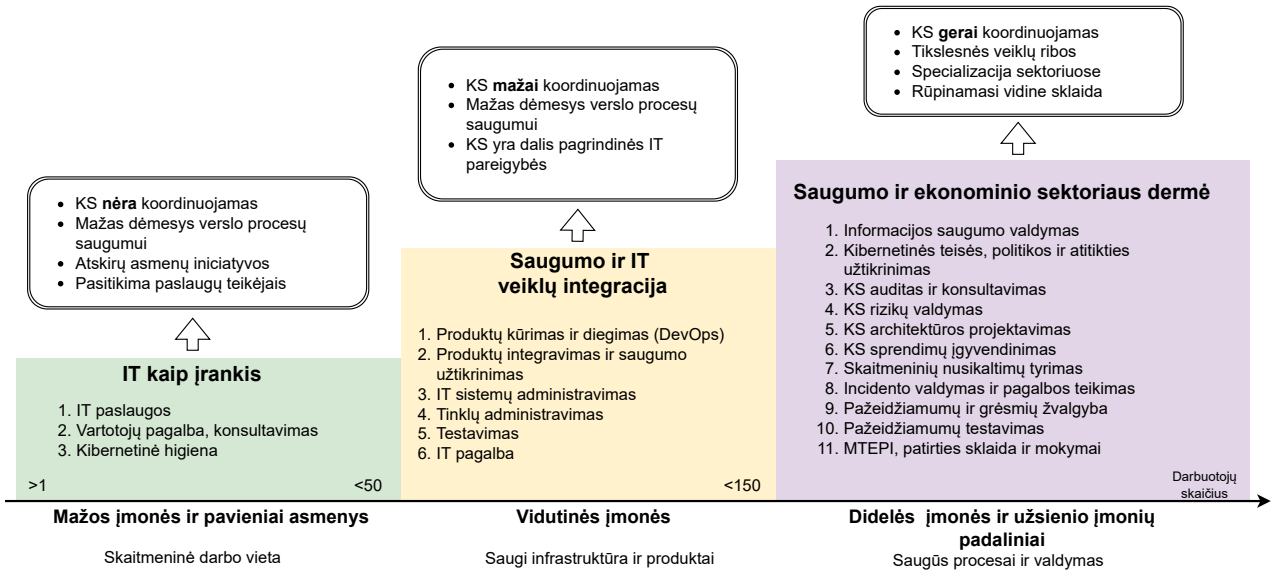
Šiame skyriuje pateikiamos KS žemėlapio komponentai – išskiriamas KS kompetencijų poreikis pagal organizacijas, suformuojamas veiklomis paremtas kompetencijų žemėlapis ir pagal jį pateikiamas kompetencijų padengimas ir poreikis, o pabaigoje nubrėžiamas tipinis KS darbuotojo karjeros kelias.

4.1. KS kompetencijų poreikis pagal organizacijos tipą

Atlikus kokybinius ir kiekybinius nuoseklius KS lauko tyrimus, išskirtini trys organizacijų tipai (žr. 4.1 pav.) pagal KS brandą ir KS kompetencijų poreikius.

Mažos organizacijos ar pavieniai asmenys sudaro pirmąjį lygmenį. Jame pirminė veikla nėra siejama su IT produktų ar IT paslaugų teikimu. KS matomas kaip skaitmeninės darbo vietos dalis. KS tokiu atveju deleguojamas organizacijos viduje esančiam IT specialistui (jei toks yra), organizacijos bendram darbuotojų išprusimui, ar tiesiog pasitikima paslaugų teikėjų pagal nustatytus KS reikalavimus. KS suvedamas į IT raštingumą ir saugaus IT išteklių ar duomenų naudojimo galimybes. KS nėra koordinuojamas organizacijos viduje, galimi verslo proceso saugumo pažeidimai. Šiame lygmenyje mažos organizacijos sulyginamos su pavieniais asmenimis visuomenėje, nes pagrindinis skaitmeninės darbo vietos saugumo parametras yra kibernetinės higienos lygmuo, kurį įtakoja bendrasis supratimas apie KS grėsmes.

Antrąjį lygmenį sudaro *vidutinės įmonės*, kurių pirminė veikla nėra sietina su IRT sektoriumi, ir mažos IT paslaugų įmonės. KS matomas kaip integrali dalis saugioje darbo infrastruktūroje, produktų



4.1 pav. KS samprata ir kompetencijų poreikis organizacijose

naudojimo ir kūrimo procesuose. KS veiklos tokiu atveju deleguojamos įmonės viduje dirbantiems programinių sprendinių kūrėjams ir diegėjams. KS užtikrinimas koncentruojamas organizacijos IT pareigybėse kaip dalis „savaime suprantamų pareigų", apjungiančių kūrimą ir diegimą, pavyzdžiui, angl. programinės įrangos kūrimo ir IT specialisto (angl. (Cyber)DevOps, (Cybersecurity) Development and Operations). KS valdymas ir reguliavimas silpnai koordinuojamas. Reagavimas į incidentus ar kitos KS veiklos taip pat nėra aktualizuojamos organizacijos viduje. Šiame lygmenyje koncentruojamasi į saugios infrastruktūros kūrimą bei užtikrinimą bei produktų, kurie turėtų būti saugūs pagal nutylėjimą, kūrimą.

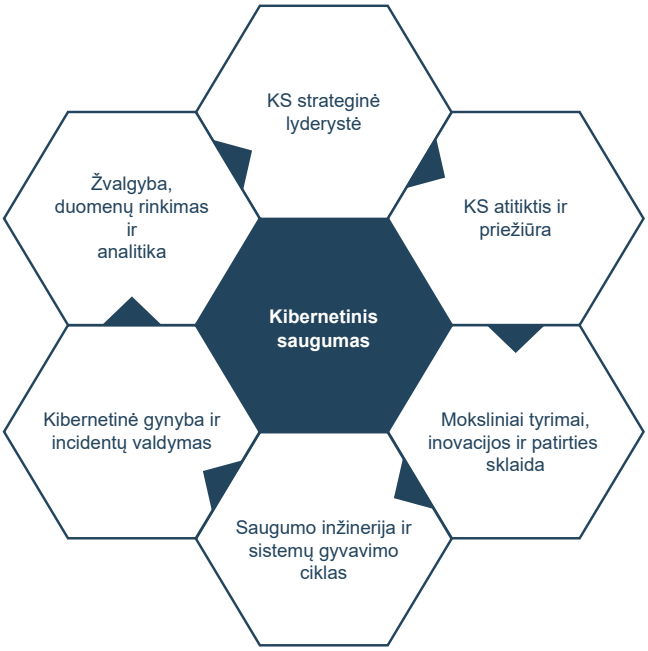
Trečiajame organizacijų lygmenyje KS kompetencijos matomos išreikštinai. Jį sudaro *Didelės įmonės ir užsienio įmonių padaliniai*, įskaitant valstybės įmones ir organizacijas, bei IT ar KS paslaugas teikiančios vidutinės įmonės. Šiame lygmenyje atsiskiria KS veiklos ir joms atlikti reikalingos kompetencijos bei KS specializacijos ar rolės. Veiklų pavadinimai įprastai siejami su atliekamos veiklos turiniu ar jų populiariaisiais analogais, pavyzdžiui, šiame lygmenyje dažniau sutinkamas pažeidžiamumų testuotojas (angl. penetration tester), o ne bendrojo pobūdžio testuotojas. Šio lygmens įmonės įprastai rūpinasi vidine sklaida (mokymais), o KS yra gerai koordinuojamas ir pareigybėse aiškios KS veiklų ribos.

Remiantis Lietuvos statistikos departamento informacija, Lietuvoje smulkios įmonės (iki 50 darbuotojų) sudaro 97 proc. visų įmonių (2022 m. pradžios duomenimis; iki 10 darbuotojų – 84 proc.; tarp 50 ir 150 darbuotojų – 2,2 proc.; o pačios didžiausios, virš 150 darbuotojų – tik 0,8 proc.). Įmonių, kurias mes vadiname "vidurinėmis" (tarp 50 ir 150 darbuotojų) yra 2032, o "didelių" (virš 150 darbuotojų) – tik 788. Vadinasi, Lietuvoje didžiausias poreikis yra IT specialistų, kurie teikia IT paslaugas, konsultuoja vartotojus, ir į kurių darbo funkcijas įeina užtikrinti pagrindinių

KS principų, kurie leistų darbuotojams ir apskritai visuomenės nariams turėti saugią darbo aplinką, įgyvendinimą, besiremiantį kibernetinės higienos gerąja praktika. Specifinės KS rolės atsiranda tik didesnėse organizacijose, tačiau didžioji dauguma KS specialistų atlieka daug skirtingų veiklų vienu metu.

4.2. Veiklomis paremtas kompetencijų žemėlapis

Tyrimai parodė, kad NIST NICE ir net ENISA ECSF kompetencijų sąrangos yra per smulkios, nes Lietuvoje dažniausiai ieškoma universalaus darbuotojo, kuris gali padengti kelias roles ir veiklų sritis. Siekiant vieningo standarto, kai ieškoma darbuotojo ar formuojamas kompetencijų poreikis, reikia subalansuoto kelių abstrakcijos lygmenų kompetencijų žemėlapio. Remdamiesi tyrimų rezultatais, siūlome veiklomis paremto profesinio KS kompetencijų žemėlapio modelį, turintį šešias sritis. Kiekvieną iš sričių grindžiame egzistuojančiais mokslo darbais. Modelio sritys kaip dimensijos pateikiamos 4.2 pav.



4.2 pav. KS dimensijos pagal veiklas

Kibernetinio saugumo strateginė lyderystė. Vyresniosios vadovybės įtraukimas į kibernetinės rizikos mažinimą yra pagrindinis sėkmės veiksnys [12]. Incidentų valdymo procedūrų nustatymas, nuolatinė veiklos stebėsena, darbuotojų motyvavimas ir kitos vadovų sukurtos priemonės ugdo tvarų kibernetinio saugumo supratimą. Todėl ši veiklos sritis yra susijusi su kibernetinio saugumo strateginiu valdymu. Pavyzdžiui, Švedijoje buvo atlikti keli pusiau struktūruoti interviu su respondentais iš šešių organizacijų, veikiančių skirtinguose pramonės sektoriuose, siekiant nustatyti pagrindinius saugumo kultūros kūrimo veiksnius [54]. Tyrimo metu buvo nustatyta, kad vienas iš veiksnių –

kibernetiniu saugumu besidominčio vadovo, turinčio pedagoginį požiūrį, kuris padėtų darbuotojams nuolat keistis ir pereiti prie į saugumą orientuotos kultūros, poreikis. Dhillon moksliniame darbe [20] pasiūlė tris organizacinės kompetencijos lygius, skirtus IT panaudojimui, siekiant įgyti konkurencinį pranašumą – strateginį, naudojimo ir tiekimo. Informacijos saugumas turi būti plėtojamas visuose trijuose organizacijos lygmenyse [21]. Pavyzdžiui, strateginis lygmuo apima kompetenciją aiškiai apibrėžti vaidmenis (grėsmės sumažinamos, kol dar netapo rimtos), o eksploatavimo lygmuo apima kompetenciją vadovauti ir daryti įtaką kitų sąmoningumui (noras "parduoti veiksmų planą"). Todėl patikimi vadovai, atliekantys CISO vaidmenį su visa jo atsakomybe, kuria pasitikėjimą ir gebėjimus organizacijoje [39].

Kibernetinio saugumo atitiktis ir priežiūra. Skaitmeninimo procesai sudarė sąlygas plėtoti kibernetinio saugumo teisinį reguliavimą, siekiant užtikrinti duomenų apsaugą ir stiprinti atsparumą kibernetiniams nusikaltimams. Europos Sąjungoje yra sukurta daug politikos ir reguliavimo priemonių [26], skirtų pagrindinėms teisėms apsaugoti ir apimančių kibernetinius klausimus nepriklausomai nuo teisių. Techninės daugiasluoksnės ekosistemos kelia iššūkių, susijusių su saugumo lygiais ir jų įgyvendinimu verslo sektoriuose [13]; pavyzdžiui, Europos Sąjungoje vis dar trūksta kai kurių reglamentų ir privalomų reikalavimų gamintojui dėl daiktų interneto produktų saugumo. Sprendimai ir strategijos gali sudaryti sąlygas kilti grėsmėms, todėl organizacijos turi vertinti ir analizuoti ne tik savo riziką, bet ir tendencijas visame sektoriuje [40]. Todėl šios žemėlapio srities veiklos padeda laikytis teisės aktų reikalavimų, atlikti auditą ir valdyti riziką, atsižvelgiant į standartus ir reguliavimus.

Moksliniai tyrimai, inovacijos ir patirties sklaida. Mūsų tyrimai parodė, kad kibernetinio saugumo sampratos formavimas yra visų specialistų atsakomybė, o tokių rolių kaip ugdytojas ar mokslininkas dažniausiai neišskyrė. Tačiau visuomenės švietimas bei inovacijų kūrimas yra neatsiejama nacionalinio žemėlapio dalis, jei siekiame užtikrinti strategijos vykdymą. KS švietimas turi prasidėti nuo pirmųjų švietimo pakopų, siekiant išugdyti visuomenės kibernetinę higieną ir tinkamus įpročius. Švedijoje buvo atlikti pusiau struktūruoti interviu su ekspertais, kad nustatytų technologijų kurso vaidmenį vidurinėse mokyklose [45]. Interviu metu ekspertai pabrėžė, kad svarbiau formuoti saugaus elgesio įpročius, o ne rengti piliečius kibernetinio saugumo darbui. Remiantis moksliniais tyrimais, kibernetinio saugumo mokymas ir švietimas yra svarbiausias kibernetinio saugumo kultūros veiksnys [46]. Švietimo įstaigos daugiausia dėmesio skiria švietimui ir moksliniams tyrimams kaip pagrindinei funkcijai, tačiau inovacijos gali būti skatinamos tik pasitelkiant tarpsektorinę partnerystę, įskaitant verslo ir akademinę bendruomenę [59]. Todėl ši žemėlapio sritis sujungia patirties sklaidą kaip švietimą plačiąja prasme (įskaitant vidinius organizacijų mokymus) ir mokslinius tyrimus (akademinė bendruomenę ir verslą), kad leistų apibrėžti nacionalinę inovacijų plėtros kryptį.

Saugumo inžinerija ir sistemų gyvavimo ciklas. Šiandien saugumo priemonių diegimas laikantis standartų yra *pagrindinė higiena* [56], neatsiejama nuo sistemų projektavimo ir kūrimo. Ši žemėlapio sritis padengia bet kokį priemonių taikymą ir sprendimų integravimą, laikomą įgyvendinimu infrastruktūroje arba programinėje įrangoje, pradedant architektūros projektavimu ir baigiant veiklos

palaikymu. Ši sritis remiasi IT sistemų saugumu ir apima visus, su šiomis sistemomis sąveikaujančius objektus [66] atsižvelgiant į kibernetinio saugumo kontekstą. Svarbu pabrėžti, kad projektavimas ir kūrimas neapsiriboja tik IT sistemomis, bet apima ir industrines valdymo sistemas. Be abejo, pavyzdžiui, inžinerijos procesuose [64] reikėtų atsižvelgti į SCADA saugumo ir IT saugumo skirtumus, pavyzdžiui, ryšių protokolus ir atsparumo grėsmėms tolerancijos lygius.

Kibernetinė gynyba ir incidentų valdymas. Reagavimas į incidentus ir incidentų valdymas gali būti laikomas atskira veiklos ir atsakomybių sritimi. Platus paslaugų prieinamumas per internetines sistemas ir išmaniųjų įrenginių naudojimas iš anksto užprogramuoja galimas atakas ir pažeidimus. Pranešimų teikimo nacionaliniams CSIRT procesai iš anksto apibrėžti teisės aktuose, tačiau kai kurios įmonės privalo palaikyti reagavimo į incidentus procedūras, užtikrinti jų parengtį ir darbuotojų mokymus kaip elgtis incidento metu. Informacijos saugos pareigūnai yra atsakingi už procedūrų laikymosi užtikrinimą ir mokymus, o incidentų valdymas apima komandinį darbą. Ši žemėlapio sritis padengia kibernetinę gynybą reagavimo į incidentus požiūriu, įskaitant skaitmeninių nusikaltimų tyrimus, kurie yra reagavimo į incidentus proceso dalis [28].

Žvalgyba, duomenų rinkimas ir analitika. Ši žemėlapio sritis apima duomenų analizę ir sistemų pažeidžiamumų testavimą. Stebėjimo įrankiai generuoja didelius duomenų kiekius, o klausimas, kokia tų duomenų dalis paverčiama sprendimu didinant atsparumą ar išvengiant incidento, išlieka net ir šiandien [56]. Tinkama duomenų analizė suformuoja sistemos kasdienės būklės situaciją ar vaizdą, kurį galima palyginti su išskirtinėmis situacijomis, netipine sistemos elgsena ir specialiose sistemose skelbiamais sistemų kompromitavimo požymiais (angl. indicators of compromise). Organizacijoms gali būti naudinga dalytis informacija ir naudotis turima informacija apie grėsmes. Dalijimosi žvalgybos informacija bendruomenės yra galinga priemonė, padedanti priimti sprendimą, atlikti veiksmus ir išvengti rizikos tapti taikiniu dėl sistemos pažeidžiamumo [44]. Didieli duomenų kiekiai reikalauja technologinių sprendimų ir įrankių, kad būtų galima analizuoti ir aptikti atakų modelius ar pažeidimus sistemose. Taigi ši žemėlapio sritis susijusi su iššūkiais ir poreikiais siekiant nustatyti pažeidžiamumus ir incidentus realiuoju laiku, pavyzdžiui, taikant dirbtinį intelektą.

Remiantis tyrimų rezultatais, pavyzdžiui, poreikiais, ir KS veiklų koreliacija pagal mokslinius darbus ir susidariusią praktiką, kiekvienai žemėlapio sričiai buvo priskirtos kompetencijų grupės ir kompetencijos pagal dominuojančias veiklas (žr. 4.3 pav.). Šis kompetencijų priskirtų veikloms sąrašas nėra baigtinis. Kaip minėta ankstesniuose skyriuose, kompetencijų lygmenys nenuleidžiami iki mokymosi rezultatų ar gebėjimų lygmenų.

Svarbu paminėti, kad žemėlapio struktūra dera su ENISA ECSF kompetencijų sąranga [24]. ENISA ECSF rolės kai kuriose srityse apjungiamos, pavyzdžiui, labai specializuotos Grėsmių žvalgybos pareigūno ir Pažeidžiamumų testuotojo rolės kaip atskiros grupės buvo apjungtos į sritį Žvalgyba, duomenų rinkimas ir analitika. Pagal tyrimo rezultatus, šių rolių reikia mažiau, bet tuo pačiu jos yra specializuotos ir reikalingos kompetencijos ugdomos, kai jau yra pakankamas ekspertizės lygmuo

4.3 pav. Dominuojančių KS kompetencijų žemėlapis

kitose kompetencijų grupėse. Šiame modelyje Įgyvendintojo ir Architekto rolės pakliūna po skėtine sritimi Saugumo inžinerija ir sistemų gyvavimo ciklas, nes saugumo architekto kaip atskiros rolės Lietuvoje ieškoma retai, bet tuo pačiu saugumo architektūra yra kertinis sistemų aspektas padengiamas įgyvendinimo metu, todėl rolės veiklas atlieka įgyvendinimu užsiimantys darbuotojai. Lyginant su ENISA sąranga, konkrečiau – Įgyvendintojo role, mūsų modelyje ši sritis labiau išskaidyta, papildomai atskiriant integravimą ir nuolatinį veiklos palaikymą, nes įgyvendinimas padengia infrastruktūrinį bei programinį lygmenis, taip pat Lietuvoje šioje srityje susitelkęs didžiausias KS ir ypač techninių specialistų blokas.

Strateginės lyderystės bei Atitikties ir priežiūros sritys yra laikytinos mažiau techninėmis sritimis, į kurias atviras kelias iš kitų mokslo ir studijų krypčių nei technologinės ar IT. Tyrimo metu pastebėta, kad mokymas ar mokslas ekspertų ar įmonių vadovų nėra išskiriami kaip svarbios ar aktualios KS sritys, bet tuo pačiu didelės įmonės užsiima darbuotojų KS sampratos ugdymu, o kiekvieno KS specialisto reikalas kažkokiu būdu prisidėti prie vartotojų KS sampratos tobulėjimo. Taigi mūsų modelyje yra išskirta sritis, padengianti mokslinius tyrimus bei ugdymą (patirties sklaidą), o taip pat atskirai – eksperimentinę plėtrą ir inovacijas, nes valstybės strategija taip pat apima inovacijų kūrimą bei KS paslaugų eksportą į užsienio rinkas.

4.3. Lietuvos kompetencijų poreikio žemėlapis

Remiantis atliktais KS lauko tyrimais, apjungus verslo organizacijų perkamų paslaugų apimtis ir specifiką, būsimus poreikius, atsižvelgus į vadovų bei KS specialistų nuomones, įvertinus situaciją aukštajame moksle, įvertinus koreliuojančias KS sritis ir jų veiklas, buvo suformuotas Lietuvos kompetencijų poreikio žemėlapis (žr. 4.4 pav.).

KS sritis	KS veiklos	Verslo įmonės perka išorės paslaugas	Vadovų nuomonė ateityje rekės	KSS nuomonė veikiama KS srityje	KSS nuomonė atlieka veiklas	Darbo skelbimai ieško ENISA rolės	Darbo skelbimai ieško NIST NICE veiklos	AM ir NŠ ugdo
Kibernetinio saugumo strateginė lyderystė	Informacijos saugos valdymas							
Kibernetinio saugumo atiktis ir priežiūra	KS auditavimas							
	KS rizikų valdymas							
	Duomenų sauga							
Moksliniai tyrimai, inovacijos ir patirties sklaida	KS moksliniai tyrimai							
	KS eksperimentinė plėtra ir inovacijos							
	KS patirties sklaida							
Saugumo inžinerija ir sistemų gyvavimo ciklas	KS sprendimų architektūros kūrimas							
	KS įgyvendinimas							
	KS integravimas ir diegimas							
	KS operatyvinis palaikymas ir pagalba							
Kibernetinė gynyba ir incidentų valdymas	KS nusikaltimų tyrimas							
	Pagalba KS incidento metu							
Žvalgyba, duomenų rinkimas ir analitika	Grėsmių žvalgyba ir analitika							
	Pažeidžiamumų testavimas							

4.4 pav. Lietuvos kompetencijų poreikio žemėlapis

Kompetencijų žemėlapio poreikių klasifikatorių priskyrimas žemėlapyje buvo atliekamas eksper-

tiniu vertinimu (ekspertų sutarimo būdu), atsižvelgiant į tyrimų metu gautus statistinius įverčius. Žemėlapiui naudojamas trijų šviesoforo spalvų žymėjimas. Nustatytos probleminės veiklos žymimos raudonai, dalinių problemų veiklos – geltonai ir mažai problemų arba jų nėra – žaliai. Balta žymima, jei veikla atitinkamoje tyrimo dalyje nebuvo pastebėta arba buvo sąlyginai nežymi (labai maža) kitų veiklų atžvilgiu.

Verslo įmonės perka sąlyginai nedaug KS paslaugų iš kitų įmonių, tarp dažniausiai paminėtų buvo pažeidžiamumų testavimas bei auditas. Kitos perkamos paslaugos pažymėtos raudonai – šiuo atveju tai rodo ne tik mažą paklausą, bet ir mažą tokias paslaugas teikiančių įmonių pasiūlą. Grėsmių žvalgyba, saugos valdymas bei moksliniai tyrimai KSS specialistų nebuvo pažymėti. Valdymas yra natūrali vidinė įmonės veikla, tačiau neegzistuojantis grėsmių žvalgybos ir mokslinių tyrimų poreikis rodo žemą brandos lygį. *Vadovų nuomonės* stulpelyje raudonai sužymėtos veiklos, kurių labiausiai reikės ateityje. Čia svarbu atkreipti dėmesį, kad numatomas didelis poreikis Saugumo inžinerijos ir sistemų gyvavimo ciklo grupei (sietina su visu IT sektoriumi) bei KS atitikties ir priežiūros grupėje – auditui ir rizikos valdymui. Pažeidžiamumų testavimas bei KS nusikaltimų tyrimai yra pažymėti žaliai, nes pirmajai veiklai vyrauja tendencija samdyti paslaugą, o antroji rodo (mūsų manymu nepagrįstą) vadovų optimizmą, kad jiems pavyks išvengti incidentų. *KS specialistų nuomonė* apie jų organizacijoje aktualias veiklos sritis (pagal ENISA) ir atliekamas veiklas (pagal NIST NICE) parodė, kad beveik nepadengiami skaitmeninių nusikaltimų tyrimai bei su moksliniais tyrimais susijusi veiklų grupė. Šie stulpeliai rodo, kad įmonės užsiima sistemų kūrimu ir jų saugumo užtikrinimu, o iš kitų stulpelių matosi, kad net ir ateityje šioms veikloms poreikis bus. *Darbo skelbimus* nagrinėjant pagal ENISA ir NIST sąrangas matyti, kad ieškoma saugumo vadovų, viso profilio įgyvendintojų ir gebančiųjų valdyti incidentą (pažymėta raudonai). Aukštajame moksle ir neformaliuoju būdu yra ugdomi KS vadovai, taip pat yra mokslo potencialas (pagal studijų programas ir mokslo rezultatus). IT (arba KS) mokytojų kaip atskiros rengimo programos nėra, nes šiuo metu Lietuvoje yra problema pritraukti mokyklų absolventus į STEM dalykų pedagogiką. Studijų programose mažai padengiami KS specifiniai technologiniai dalykai (nėra specializacijų).

Pagal sudarytą žemėlapį darytinos šios išvados:

- KS paslaugų pasiūlos sektorius nėra išvystytas, nes dauguma KS naudojančių organizacijų orientuojasi į vidinių žmogiškųjų išteklių kūrimą. Ypatingai pastebimas grėsmių žvalgybos ir mokslinių tyrimų trūkumas – įmonės to neatlieka pačios, neperka iš kitų ir neplanuoja poreikio.
- KS specialistų poreikis matomas Saugumo inžinerijos ir sistemų gyvavimo ciklo sričiai dėl tampraus ryšio su IT funkcijomis.
- Poreikio moksliniams tyrimams, inovacijoms ir patirties sklaidai įmonių vadovybė nejaučia kaip svarbioms veikloms, tačiau pastebimas susidomėjimas KS specialistų lygmenyje atlikti sklaidą, tyrimus ir inovacijas. Ši sritis svarbi Lietuvos strategijose, bet įmonės dar šių veiklų neišskiria ir nemato ateityje.
- Aukštosios mokyklos ir neformaliojo švietimo kursai nerengia KS specialistų sklaidai (moky-

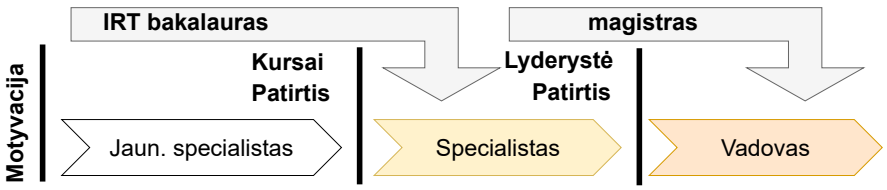
mams), tačiau poreikis viduje organizacijoje užsiimti mokymu ir gerosios praktikos sklaida matomas per skelbimus ir KS specialistų atliekamas veiklas. Svarbu paminėti, kad mokymas skelbimuose dažnai paminėta kaip antrinė specialisto rolė.

4.4. KS karjeros kelias

Vienas iš projekto tikslų buvo identifikuoti KS darbuotojo karjeros kelią. Pagal Lietuvoje taikomą Lietuvos profesijų klasifikatorių [42] yra naudojami šie profesijų lygmenys:

1. **Vadovai**
2. **Specialistai**
3. **Technikai ir jaunesnieji specialistai**
4. Tarnautojai
5. Paslaugų sektoriaus darbuotojai ir pardavėjai
6. Kvalifikuoti žemės, miškų ir žuvininkystės ūkio darbuotojai
7. Kvalifikuoti darbininkai ir amatininkai
8. Įrenginių ir mašinų operatoriai ir surinkėjai
9. Nekvalifikuoti darbininkai
0. Ginkluotųjų pajėgų profesijos

Remiantis kokybinio tyrimo duomenimis, tipinis KS specialisto kelias pagal šiuo metu nusistovėjusį verslo požiūrį, praktiką ar valstybės teisinį reguliavimą (žr. 4.5 pav.) prasideda nuo motyvacijos



4.5 pav. KS specialisto karjeros kelias

ateiti į KS sritį, noro domėtis KS veiklomis bei gebėjimo mokytis savarankiškai. Motyvaciją verslo įstaigos prašo patvirtinti bent vienu iš galimų dviejų alternatyvių pasirinkimų. Pirmoji alternatyva demonstruoti motyvaciją ir pagrįsti domėjimąsi KS yra specializuotų neformalaus švietimo kursų sertifikatų pateikimas arba (retais atvejais) aktyvus dalyvavimas projektinėse veiklose, pvz. atviro kodo kūrimo iniciatyvose. Antroji – studijos aukštojoje mokykloje IRT studijų programose (prioretizuojant kibernetinio saugumo bakalauro programas).

Norint tapti KS specialistu, visų pirma yra būtina įgyti bent kelerių metų darbo patirtį IRT srityje (pageidautina – KS srityje). IRT studijų programose įgytas bakalauro laipsnis yra didelis privalumas (pusė darbdavių to reikalaus), tačiau kaip alternatyvą galima rinktis neformaliojo švietimo ir profesinio

sertifikavimo kursus. Kaip ekspertai pabrėžė, specifinis sertifikatas parodo domėjimosi sritį ir motyvaciją. Versle KS specialistas gali būti užauginamas nepriklausomai nuo išsilavinimo, jeigu įmonė tam skiria resursus (ne visos tą daro, dauguma stengiasi pirkti jau užaugintus specialistus).

Kandidatams, siekiantiems užimti vadovo pareigas, taikomas aukštesnis slenkstis – ne tik ilgesnė darbo patirtis metais, bet ir asmeninės savybės, pavyzdžiui, gebėjimas imtis lyderystės, o viešajame sektoriuje įprasta, kad vadovas privalo turėti magistro mokslo laipsnį kaip apibrėžta kvalifikacijų sąrangoje.

Valstybinės institucijos turi ribotą galimybę įdarbinti nekvalifikuotą techniką ar jaunesnįjį specialistą dėl taikomų kvalifikacinių apribojimų. Taip pat valstybės institucijos laikosi aukštojo mokslo kvalifikacijų sandaros ir dėl to karjeros atitikmenys tiesiogiai rišami su studijų programų baigimu, tiksliau – laipsnio įgijimu. Pavyzdžiui, pastebima, kad valstybinio sektoriaus aukštos kvalifikacijos specialistai norėdami užimti vadovaujantį postą apsisprendžia studijuoti magistro pakopos studijų programose (remiamasi universitetų patirtimi).

5. Išvados

Tyrimo pradžioje kėlėme hipotezę, kad KS specialistų trūkumą galima būtų spręsti pritraukiant kitų, ne IRT, sričių išsilavinimą turinčius specialistus. Pagal visuomenės nuomonę, KS yra technologinių ir fizinių mokslų sritis. Šiuo metu KS ekspertai mato kaip pagrindą tik bendrąsias IRT žinias, o darbo rinkoje dominuoja technologinių kompetencijų poreikis. Bendrosios kompetencijos versle įprastai minimos kaip bendrosios kompetencijos ir asmeninės savybės nesiejant su išsilavinimu ar darbuotojo profiliu. Pastebima, kad kalbėdami apie KS specialistą, valstybinio sektoriaus vadovai IRT žinias akcentuoja labiau, nei verslo vadovai. Tačiau apklausose ir per ekspertų interviu buvo pastebėta, kad į kibernetinio saugumo gali ateiti bet koks specialistas, kuris turi motyvacijos ir bazines IRT žinias, įgytas formaliuoju ar neformaliojo švietimo būdu.

Kibernetinis saugumas dar nėra visiškai savarankiška specialistų rengimo kryptis. Darbo rinkoje KS funkcijos ir darbuotojų poreikis glaudžiai susiję su IRT sektoriumi. Remiantis oficialia Lietuvos statistika IRT sektoriuje dirba apie 40–50 tūkst. IT specialistų, o remiantis išvestiniais duomenimis (paieška LinkedIn profesiniame tinkle) save KS specialistais įvardinančių yra apie 1 – 1,5 tūkst. (KS specialistai sudaro apie 2,5 proc. nuo IRT darbuotojų). Didelė dalis IRT specialistų pagal nusistovėjusią praktiką vykdo KS veiklas nors to neįvardina.

Ateityje, KS specialistų trūkumas numatomas visose KS srityse, mažiausias dėmesys numatomas skaitmeninių nusikaltimų tyrimams, o didžiausias – sistemų palaikymui. Per ateinančius 5 metus organizacijos, kuriose dirba daugiau nei 50 darbuotojų, ieškos bent 800 naujų KS specialistų. Šios organizacijos sudaro tik 3 proc. nuo visų Lietuvos įmonių. Todėl tikėtina, kad skaičius 800 yra labai konservatyvi prognozė. Galima teigti, kad specialistų pozicijų skaičius padvigubės per ateinančius

5 metus. Juos paruošti yra didelis iššūkis.

Kibernetinio saugumo srities brandos lygis Lietuvoje yra pakankamai žemas.

- Visuomenė linkusi KS specialistą identifikuoti kaip IT sistemų administratorių.
- Įmonių vadovai taip pat mano, kad paprastas KS funkcijas gali atlikti IT specialistas.
- Didžioji dalis Lietuvos įmonių neturi savo KS specialisto, nesamdo KS paslaugų iš išorės ir net neplanuoja ateityje tai daryti.
- KS specialistai mažai specializuoti, nes dauguma samdomų KS specialistų turi atlikti daug skirtingiems vaidmenims tenkančių veiklų.

Brandos lygis įtakoja ir inovacijų skvarbą bei įmonių specializaciją:

- Tyrimai rodo, kad inovacijas kuriančių KS įmonių yra vienetai. Darbo skelbimuose nebuvo nė vienos užuominos apie KS mokslinius tyrimus ar eksperimentinės plėtros poreikį versle. Verslo įmonės nesikoncentruoja į mokslo tyrimų ir eksperimentinės plėtros, kaip kokybiškai naujų paslaugų kūrimą, o į KS specialistus žiūri tik kaip į veiklos funkcijų užtikrintojus.
- Mokslo tyrimų grupės didžiuosiuose akademiniuose centruose turi potencialą augti ir kurti naująsias technologijas prisidedant prie verslo sektoriaus KS inovacijų kūrimo bei valstybės žmogiškųjų išteklių papildymo.

Valstybinis sektorius šiuo metu negali konkuruoti su verslu:

- Versle taikomas 15 – 53 proc. didesnis atlygis už tos pačios KS pozicijos darbą.
- Verslo organizacijos siūlo papildomų motyvacinių paketų, pvz., lankstus darbo grafikas, sporto kompleksai, papildomas sveikatos draudimas ir t.t.
- Valstybės įmonės ir organizacijos laikosi kvalifikacinių lygmenų, kurie apriboja ankstyvą jaunųjų (mažiau kvalifikuoti ar nekvalifikuotų) bet motyvuotų jaunesniųjų specialistų ar technikų įdarbinimą KS veikloms atlikti (pvz., studentas dar neturintis bakalauro laipsnio valstybinėse įstaigose laikomas nekvalifikuotu darbuotoju).
  Valstybiniame sektoriuje IT specialistų klasifikacijoje taikomas profesijų klasifikatoriaus nėra lankstus ir neskatina IT specialistams judėti labiau specializuotu (horizontalioji karjera) ar į kitas susijusias veiklas karjeros keliu. Vertikalioji karjera (vadovavimo atsakomybės) gali sėkmingai klostytis, jeigu IT specialistas pasižymi bendraisiais (minkštaisiais) gebėjimais ir asmeninėmis savybėmis, kurie yra perkeliami į kitas sritis. Vertikalus judėjimas valstybiniame sektoriuje vyksta lėčiau nei verslo sektoriuje ir siejamas su kvalifikacijų pagrįstumu.
- 80 proc. specialistų privačiame sektoriuje turi geras sąlygas kelti kvalifikaciją, o panašias sąlygas turi mažiau nei 50 proc. viešojo sektoriaus KS specialistų.

Remiantis reprezentatyvios visuomenės apklausos duomenimis, požiūris į kibernetinius šauktinius (nedetalizavus šios savokos apibrėžimo) yra patrauklus šaukiamojo amžiaus jaunuoliams. Nepriklausomai nuo pasirinktos "Kibernetinių šauktinių" panaudojimo strategijos, jie yra puiki galimybė spręsti specialistų trūkumo problemą. Nauda gali pasireikšti skirtingais būdais.

- Visų pirma, padaugėja pritrauktų į KS sritį jaunuolių skaičius.
- Antra, tarnybos metu gali būti dalinai patenkintas trūkstamų KS specialistų valstybinėse institucijose poreikis.
- Trečia, po tarnybos, dalis specialistų gali tęsti karinę profesionalią tarnybą, o likusieji su patirtimi papildyti darbo rinką valstybiniame ar privačiame sektoriuje.

Amžius, lytis ar darbuotojo profilis nėra kliūtis įsilieti į KS sritį. Vidutinio amžiaus Lietuvos gyventojai pozityviai žiūri į moterų KS specialisčių didėjimą darbo rinkoje, o pačios specialistės mato daug galimybių ir perspektyvą, nes svarbios ne tik technologinės žinios, bet ir bendrieji gebėjimai, pavyzdžiui, lyderystė, gebėjimas dalintis informacija, projektų valdymas, gebėjimas nuolat mokytis ir tobulėti.

Amerikietiškas NIST NICE standartas, aprašantis virš 40 skirtingų KS specialisto rolių, netinka Lietuvos įmonėms, nes yra per daug detalus atsakomybių ir vykdomų veiklų požiūriu. Net ir 12 rolių turinti ENISA ECSF kompetencijų sąranga neatitinka Lietuvos situacijos, nes darbuotojas atlieka kelių rolių veiklas, o į įgyvendintojo rolę patenka dauguma KS technologinių specialistų. Mūsų siūlomas veiklomis pagrįstas kompetencijų žemėlapis galėtų būti naudojamas Lietuvoje apibrėžti egzistuojančias ir būsimas darbo vietas keliais lygmenimis, pradedant nuo aukščiausio abstraktaus, sudaryto iš 6 sričių, kurių kiekviena pajungia labiausiai susijusias veiklas.

6. Rekomendacijos

Reikminio tyrimo metu nustatytos ir apibendrintos rekomendacijos tiesiogiai išplaukiančios iš tyrimo duomenų ir ar netiesiogiai iš ekspertinio visuminio vertinimo.

- Keisti KS specialybės įvaizdžio modelį, naudojant šiuolaikinio „gerojo" KS specialisto įvaizdį. Geriau aiškinti KS karjeros kelio pradedantiesiems, laužant nusistovėjusius stereotipus, demonstruojant sektinus pavyzdžius ir pasirinkimus, derinant su IT sektoriaus ar kitomis giminingomis studijų programomis.
- Atnaujinti ir tobulinti Lietuvos profesijų klasifikatorių [42], papildant kibernetiniam saugumui tinkamomis profesijomis ir atitinkamais aprašais bei suderinant su Europos komisijos naudojamu ESCO klasifikatoriumi [62],[61].
- Valstybinio sektoriaus specialistams mažinti atlyginimo atotrūkį nuo kolegų versle numatant specialistų, vidurinės grandies vadovų ir vadovų karjeros kelius organizacijos viduje, papildomą jų ugdymą, kitas motyvacijos priemones.
- Siekiant griauti lyčių stereotipus ir pritraukti daugiau moterų į KS sritį, svarbu pasitelkti sėkmės istorijų ar sektinus pavyzdžius (angl. role models) ir inicijuoti projektus, kuriuose būtų ne tik vienai grupei (moterims) pristatomos karjeros galimybės KS srityje, bet ir pačios moterys galėtų aktyviai dalyvauti visuomenės švietime nuo formalaus ugdymo pradžios.
- Mentorystės ir koučingo programos galėtų būti platforma, kurioje sėkmingai daugelį metų KS srityje dirbančios moterys padėtų pradedančiosioms sklandžiau įsilieti į KS sritį. Mentorystei ir koučingui svarbūs konsultavimo gebėjimai buvo įvardinti kaip iš kitų sričių atsinešta sukaupta patirtis. Mentorystė galėtų vykti formalizuotoje tinklaveikoje, kuri buvo išskirta kaip žinių ir dalinimosi informacija būdas. Žinių dalinimasis tinklaveikoje identifikuotas kaip svarbus

faktorius veiklos pradžioje, nes KS srityje vis dar nepakankama specializuotų žinių sklaida.

- Valstybinio sektoriaus organizacijoms sukurti strategiją dėl IRT ir KS dirbančių specialistų pritraukimo, jų išlaikymo ir jų karjeros kelio numatymo.
- Didinti kibernetinio saugumo raštingumą darbdavių terpėje, aiškiau formuluojant darbuo-tojų roles pagal ieškomo specialisto lygį ir tikėtinas kompetencijas, siejant su numatomu karjeros keliu ar specializacija.
- Skatinti ir kurti aplinkas mokslo tiriamosios ar eksperimentinės plėtros ir inovacijų KS rezultatų perdavimui verslo subjektams tokiu būdu demonstruojant alternatyviuosius karjeros kelius bei kuriant naujas darbo vietas KS inovatyvių paslaugų kūrimui.
- Diegti KS kultūrą nuo mažens, papildant IT įgūdžių ir raštingumo temomis bendrojo ugdymo programas. Bendrojo ugdymo programos IT raštingumo dalyje rasti galimybių aptarti saugaus elgesio (kibernetinės higienos) elementus, tokiu būdu sukuriant saugesnę bręstančią visuomenę.
- Didinti mokymosi visą gyvenimą KS programų apimtis, visuomenę šviesti tinkamai suprojektuotomis priemonėmis, nepaliekant švietimo funkcijos vien žiniasklaidai.
- Atnaujinti Informatikos mokslų studijų krypčių aprašą papildant tinkamomis saugumo kompetencijomis pagal kvalifikacijos lygmenis.
- Skatinti KS studijų programų ar KS modulių kūrimą profesinio bakalauro, bakalauro, magistro lygio ir IT SP specializavimą bakalauro lygiu, sudarant sąlygas IRT sektoriaus studentams koncentruotis į KS tematikas ir specializuotis į KS sritį.
- Apsvarstyti Lietuvos kariuomenės „kibernetinio šauktinio" sistemos sukūrimą. Greito ugdymo cikluose dalyvaujantys šauktiniai galėtų užimti trūkstamų *jaunesnių* specialistų vietas nišinėse valstybinio sektoriaus struktūrose, o po tarnybos — panaudoti savo patirtį versle (žr. 3.1.
- Gerinti mokslininkų, podoktorantūros stažuotojų, doktorantų pritraukimą darbui (projektai, inovacijų perdavimo projektai) su KDS sietinose mokslinėse tematikose ypač IRT sektoriuje.
- Skatinti ankstyvas studentų integracijas į daugiadisciplinius mokslo darbus skatinant naujų KS technologijų kūrimą.
- Lietuvoje skatinti standartizuotą KS specialistų identifikavimą ar profiliavimą (darbo skelbimų aprašuose, formuojant komandas, pareigybinėse instrukcijose), nurodant jų atliekamas dominuojančias veiklas pagal mūsų pateiktą kompetencijų žemėlapį (4.3 pav.), ir atkreipiant dėmesį į glaudžiai susijusias veiklų grupes siekti mažinti persidengiančių rolių kiekį vienam KS darbuotojui.

Literatūros sąrašas

Knygos ir jų skyriai

[4] Vida Beresnevičiūtė, Arūnas Poviliūnas ir Rūta Žiliukaitė. *Profesinės veiklos lauko tyrimo metodika*. Vilnius: VU, 2011. ISBN: 978-9955-526-81-0. Žiniatinklyje: http://www.esparama.lt/es_parama_pletra/failai/ESFproduktai/2011_Profesines_veiklos_lauko_tyrimo_metodika.pdf (žr. psl. 27).

[33] International Labour Office. *International standard classification of occupations: ISCO-88*. Printed y International Labor Office, Geneva, Switzerland, 2012. ISBN: 978-92-2-125927-2 (žr. psl. 18).

[38] Declan Kennedy. *Writing and using learning outcomes: a practical guide*. University College Cork, 2006. ISBN: 978-0-9552229-6-2 (žr. psl. 28).

[47] I. Nai Fovino ir kt. *European Cybersecurity Centres of Expertise Map : Definitions and Taxonomy*. Publications Office of the European Union, Luxembourg, 2018. DOI: 10.2760/622400 (žr. psl. 15, 23).

[58] Lior Tabansky ir Isaac Ben Israel. "The National Cyber-Strategy of Israel and the INCB". Konferencijos leidinyje: *Cybersecurity in Israel*. Cham: Springer International Publishing, 2015, 49–54 psl. ISBN: 978-3-319-18986-4. DOI: 10.1007/978-3-319-18986-4_7 (žr. psl. 9).

Straipsnių rinkinių dalys

[16] P. Colaizzi. "Psychological research as a phenomenologist views it". Konferencijos leidinyje: *Existential Phenomenological Alternatives for Psychology*. Open University Press: New York, 1978, 6 psl. (žr. psl. 35).

[21] Gurpreet Dhillon, Kane Smith ir Karin Hedström. "Ensuring Core Competencies for Cybersecurity Specialists". Konferencijos leidinyje: *Cybersecurity Education for Awareness and Compliance*. IGI Global, 2019, 121–133 psl. DOI: 10.4018/978-1-5225-7847-5.ch007 (žr. psl. 86).

[26] Gloria González Fuster ir Lina Jasmontaite. "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights". Konferencijos leidinyje: *The Ethics of Cybersecurity*. Cham: Springer International Publishing, 2020, 97–115 psl. ISBN: 978-3-030-29053-5. DOI: 10.1007/978-3-030-29053-5_5 (žr. psl. 86).

[28] Cem Gurkok. "Chapter 41 - Cyber Forensics and Incidence Response". Konferencijos leidinyje: *Computer and Information Security Handbook (Third Edition)*. Red. John R. Vacca. Third Edition. Boston: Morgan Kaufmann, 2017, 603–628 psl. DOI: https://doi.org/10.1016/B978-0-12-803843-7.00041-7 (žr. psl. 87).

[44] Allan Liska. "Chapter 8 - CERTs, ISACs, and intelligence-sharing communities". Konferencijos leidinyje: *Building an Intelligence-Led Security Program*. Red. Allan Liska. Boston: Syngress, 2015, 139–151 psl. ISBN: 978-0-12-802145-3. DOI: https://doi.org/10.1016/B978-0-12-802145-3.00008-9 (žr. psl. 87).

Žurnaliniai straipsniai

[1] Saleh AlDaajeh ir kt. "The role of national cybersecurity strategies on the improvement of cybersecurity education". Konferencijos leidinyje: *Computers & Security* 119 (2022), 102754 psl. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2022.102754 (žr. psl. 23).

[5] Agnė Brilingaitė, Linas Bukauskas ir Aušrius Juozapavičius. "A framework for competence development and assessment in hybrid cybersecurity exercises". Konferencijos leidinyje: *Computers & Security* 88 (2020), 101607 psl. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2019.101607 (žr. psl. 11).

[12] Dave Chatterjee. "Should executives go to jail over cybersecurity breaches?" Konferencijos leidinyje: *Journal of Organizational Computing and Electronic Commerce* 29.1 (2019), 1–3 psl. DOI: 10.1080/10919392.2019.1568713 (žr. psl. 85).

[13] Pier Giorgio Chiara. “The IoT and the new EU cybersecurity regulatory landscape”. Konferencijos leidinyje: *International Review of Law, Computers & Technology* 36.2 (2022), 118–137 psl. DOI: 10.1080/13600869.2022.2060468 (žr. psl. 86).

[14] Noman H. Chowdhury, Marc T.P. Adam ir Timm Teubner. “Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures”. Konferencijos leidinyje: *Computers & Security* 97 (2020), 101931 psl. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2020.101931 (žr. psl. 11).

[20] Gurpreet Dhillon. “Organizational competence for harnessing IT: A case study”. Konferencijos leidinyje: *Information & Management* 45.5 (2008), 297–303 psl. DOI: https://doi.org/10.1016/j.im.2008.01.008 (žr. psl. 86).

[30] George Hatzivasilis ir kt. “Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees”. Konferencijos leidinyje: *Applied Sciences* 10.16 (2020). ISSN: 2076-3417. DOI: 10.3390/app10165702 (žr. psl. 11).

[32] Samuel C. Yang. “A meta-model of cybersecurity curriculums: Assessing cybersecurity curricular frameworks for business schools”. Konferencijos leidinyje: *Journal of Education for Business* 96.2 (2021), 99–110 psl. DOI: 10.1080/08832323.2020.1757594 (žr. psl. 11).

[39] Richard Klimoski. “Critical Success Factors for Cybersecurity Leaders: Not Just Technical Competence”. Konferencijos leidinyje: *People & Strategy* 39.1 (2016), 14–19 psl. (žr. psl. 86).

[40] In Lee. “Cybersecurity: Risk management framework and investment cost analysis”. Konferencijos leidinyje: *Business Horizons* 64.5 (2021), 659–671 psl. ISSN: 0007-6813. DOI: https://doi.org/10.1016/j.bushor.2021.02.022 (žr. psl. 86).

[49] William Newhouse ir kt. “National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework”. Konferencijos leidinyje: *NIST Special Publication* 800-181 (2017), 144 psl. DOI: 10.6028/NIST.SP.800-181. Žiniatinklyje: https://doi.org/10.6028/NIST.SP.800-181 (žr. psl. 10, 16).

[56] Uma Somayajula. “What went wrong with Cyber Security?” Konferencijos leidinyje: *SSRN* (2022). DOI: http://dx.doi.org/10.2139/ssrn.4012355 (žr. psl. 86, 87).

[59] Karen Teh ir kt. “Singapore’s cybersecurity ecosystem”. Konferencijos leidinyje: *Communications of the ACM* 63.4 (2020), 55–57 psl. DOI: http://dx.doi.org/10.1145/3378552 (žr. psl. 86).

[64] Darshana Upadhyay ir Srinivas Sampalli. “SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations”. Konferencijos leidinyje: *Computers & Security* 89 (2020), 101666 psl. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2019.101666 (žr. psl. 87).

[66] Ricardo Villalón-Fonseca. "The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity". Konferencijos leidinyje: *Computers & Security* 120 (2022), 102805 psl. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2022.102805 (žr. psl. 87).

Tarptautinių renginių leidiniai

[29] Joanne L. Hall ir Asha Rao. "Non-Technical skills needed by cyber security graduates". Konferencijos leidinyje: *2020 IEEE Global Engineering Education Conference (EDUCON)*. 2020, 354–358 psl. DOI: 10.1109/EDUCON45650.2020.9125105 (žr. psl. 10, 69).

[35] Johanna Jacob ir kt. "Is the Nice Cybersecurity Workforce Framework (NCWF) Effective for a Workforce Comprising of Interdisciplinary Majors?" Konferencijos leidinyje: *Proceedings of the 16th International Conference on Scientific Computing (CSC'18). Las Vegas, USA*. 2018. Žiniatinklyje: https://par.nsf.gov/biblio/10095246 (žr. psl. 11).

[46] Emilia N. Mwim ir Jabu Mtsweni. "Systematic Review of Factors that Influence the Cybersecurity Culture". Konferencijos leidinyje: *Human Aspects of Information Security and Assurance*. Red. Nathan Clarke ir Steven Furnell. Cham: Springer International Publishing, 2022, 147–172 psl. DOI: 10.1007/978-3-031-12172-2_12 (žr. psl. 86).

[50] Allen Parrish ir kt. "Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-Discipline". Konferencijos leidinyje: *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*. ITiCSE 2018 Companion. Larnaca, Cyprus: Association for Computing Machinery, 2018, 36–54 psl. ISBN: 9781450362238. DOI: 10.1145/3293881.3295778 (žr. psl. 10).

[52] Federica Polo ir Jussi Kantola. "Tomorrow's Digital Worker: A Critical Review and Agenda for Building Digital Competency Models". Konferencijos leidinyje: *Advances in Human Factors, Business Management and Leadership*. Red. Jussi Ilari Kantola, Salman Nazir ir Vesa Salminen. Cham: Springer International Publishing, 2020, 107–115 psl. ISBN: 978-3-030-50791-6. DOI: 10.1007/978-3-030-50791-6_14 (žr. psl. 10).

[55] Reijo M. Savola. "Current Level of Cybersecurity Competence and Future Development: Case Finland". Konferencijos leidinyje: *Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings*. ECSA '17. Canterbury, United Kingdom: Association for Computing Machinery, 2017, 121–124 psl. ISBN: 9781450352178. DOI: 10.1145/3129790.3129804 (žr. psl. 10).

[65] Andrey Vybornov, Natalia Miloslavskaya ir Alexander Tolstoy. “Designing Competency Models for Cybersecurity Professionals for the Banking Sector”. Konferencijos leidinyje: *Information Security Education. Information Security in Action*. Red. Lynette Drevin, Suné Von Solms ir Marianthi Theocharidou. Cham: Springer International Publishing, 2020, 81–95 psl. ISBN: 978-3-030-59291-2. DOI: 10.1007/978-3-030-59291-2_6 (žr. psl. 10).

[67] Franz E Weinert. “Begabung und Lernen. Zur Entwicklung geistiger Leistungsunterschiede”. Konferencijos leidinyje: *Werte schulischer Begabtenförderung. Begabung und Leistung*. 2012, 23–34 psl. DOI: 10.25656/01:9029 (žr. psl. 10).

Techninės ataskaitos

[2] Miguel Eiras Antunes, Jean Gil Barroca ir Daniela Guerreiro de Oliveira. *Urban Future With a Purpose*. 2021. Žiniatinklyje: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Public-Sector/deloitte-urban-future-with-a-purpose-study-set2021.pdf Lankytasi: 2022-07-24 (žr. psl. 78).

[23] ENISA. *Diversity in Cybersecurity*. techreport. 2021. Žiniatinklyje: https://ecsc.eu/about/diversity-flyer-online.pdf (žr. psl. 43).

[31] Martin Hurt ir Tiia Sõmer. *Cyber Conscription: Experience and Best Practice from Selected Countries*. 2021. Žiniatinklyje: https://icds.ee/wp-content/uploads/2021/02/ICDS_Report_Cyber_Conscription_Hurt_Somer_February_2021.pdf Lankytasi: 2022-07-20 (žr. psl. 25).

[36] Joint Task Force on Cybersecurity Education. *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. techreport. New York, NY, USA: ACM/IEEE/AIS-SIGSEC/IFIP WG 11.8, 2017. DOI: 10.1145/3184594. Žiniatinklyje: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf (žr. psl. 16, 40).

[24] European Union Agency for Cybersecurity, ENISA. *European Cybersecurity Skills Framework Role Profiles*. Available online at: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles. [accessed November 18, 2022]. 2022-09 (žr. psl. 15, 16, 87).

Žiniatinklio ištekliai

[3] Vilius Benetis. *Kibernetinio saugumo įmonių Lietuvoje žemėlapis*. 2022. Žiniatinklyje: https://github.com/vibenas/Cybersecurity-Lithuania-Map Lankytasi: 2022-07-14 (žr. psl. 23, 24).

[6] Linas Bukauskas ir kt. *Lietuvos įmonių darbo skelbimų kibernetiniame saugumo rolėse tyrimas [Duomenų rinkinys]*. 2022. DOI: 10.18279/MIDAS.CIBERSEK_JOB_ADDS_LT.188854 (žr. psl. 70).

[7] Linas Bukauskas ir kt. *Lietuvos įmonių vadovų ir specialistų apklausa kibernetinio saugumo klausimais [Duomenų rinkinys]*. 2022. DOI: 10.18279/MIDAS.CIBERSEK_CEO_HR_CSS_LT.188843 (žr. psl. 47).

[8] Business Finland. *Cybersecurity from Finland*. 2020. Žiniatinklyje: https://www.businessfinland.fi/49ed06/contentassets/9d10aa6fff2c469d905e61b3507dd6f0/finnish_solutions_for_cyber_security_web.pdf (žr. psl. 24).

[9] Aapo Cederberg. *Comprehensive Cyber Security Approach – The Finnish Model*. 2020. Žiniatinklyje: https://www.cyberwatchfinland.fi/wp-content/uploads/2020/07/A-COMPREHENSIVE-CYBER-SECURITY-APPROACH-%E2%80%93-THE-FINNISH-MODEL.pdf (žr. psl. 24).

[10] Studijų krypčių vertinimo centras. *Įsakymas dėl Informatikos mokslų studijų krypčių grupės aprašo patvirtinimo*. 2021. Žiniatinklyje: https://www.e-tar.lt/portal/lt/legalAct/e1bb60c053e211eb9dc7b575f08 (žr. psl. 17).

[11] Studijų krypčių vertinimo centras. *Studijų krypčių aprašai*. 2022. Žiniatinklyje: https://www.skvc.lt/default/lt/kokybes-uztikrinimas/krypciu-aprasai (žr. psl. 17).

[15] *CyberPhish*. Žiniatinklyje: https://cyberphish.eu/ (žr. psl. 23).

[17] Deloitte. *The future market for cybersecurity in Denmark*. 2018. Žiniatinklyje: https://innovationsfonden.dk/sites/default/files/2018-07/thefuturemarketforcybersecurityindenmark.pdf (žr. psl. 24).

[18] Lietuvos statistikos departamentas. *Lietuvos statistikos duomenų bazė — Gyventojai ir socialinė statistika – Užimtos darbo vietos*. 2022. Žiniatinklyje: https://osp.stat.gov.lt/statistiniu-rodikliu-analize?indicator=S3R534#/ Lankytasi: 2022-07-13 (žr. psl. 69).

[19] Lietuvos Statistikos Departamentas. *Lietuvos statistikos metraštis*. 2019. Žiniatinklyje: https://osp.stat.gov.lt/lietuvos-statistikos-metrastis/lsm-2019/mokslas-ir-technologijos/informacines-technologijos Lankytasi: 2022-07-10 (žr. psl. 69).

[22] *ECHO*. Žiniatinklyje: https://echonetwork.eu/ (žr. psl. 23).

[25] Eurostat. *Employed ICT specialists — total (dataset ISOC_SKS_ITSPT)*. 2022-04. Žiniatinklyje: https://ec.europa.eu/eurostat/databrowser/view/ISOC_SKS_ITSPT/default/table?lang=en&category=isoc.isoc_sk.isoc_sks.isoc_skslf Lankytasi: 2022-07-13 (žr. psl. 69, 70).

[27] The Danish Government. *The Danish National Strategy for Cyber and Information Security*. 2021. Žiniatinklyje: https://en.digst.dk/media/27024/digst_ncis_2022-2024_uk.pdf (žr. psl. 24).

[34] IT Professionalism Europe (ITPE). *The European e-Competence Framework (e-CF)*. Žiniatinklyje: IT%20Professionalism%20Europe%20(ITPE) (žr. psl. 16).

[37] Aušrius Juozapavičius. *Lietuvos visuomenės nuomonės apie kibernetinio saugumo specialistus tyrimas [Duomenų rinkinys]*. 2022. DOI: 10.18279/MIDAS.OMNIBUS_CYBERSEC_LT.188817 (žr. psl. 41).

[41] *Lietuvos kibernetinių nusikaltimų kompetencijų ir tyrimų centras*. Žiniatinklyje: https://l3ce.eu (žr. psl. 15).

[42] Lietuvos Respublikos ekonomikos ir inovacijų ministerijos Žmogiškųjų išteklių plėtros skyrius. *Lietuvos Profesijų klasifikatorius*. 2022. Žiniatinklyje: http://www.profesijuklasifikatorius.lt (žr. psl. 18, 91, 97).

[43] Lietuvos Respublikos švietimo ir mokslo ministerija. *Dėl studijų krypčių ir krypčių grupių, pagal kurias vyksta studijos aukštosiose mokyklose, sąrašo, jo keitimo tvarkos, kvalifikacinių laipsnių sąrangos ir studijų programų pavadinimų sudarymo principų patvirtinimo*. 2017. Žiniatinklyje: https://www.e-tar.lt/portal/lt/legalAct/ae5d5730b7c211e693eea1ef35f20da9 (žr. psl. 16).

[45] Wafaa Mushtaq. *Cybersecurity in the Technology Subject from the Swedish Perspective : Investigation, Analysis, and Evaluation Tool*. Dissertation. 2020. Žiniatinklyje: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-283112 (žr. psl. 86).

[48] Ieva Namavičiūtė. *Pasaulinių kibernetinio saugumo (KS) industrijos tendencijų ir KS specialistų padėties Lietuvoje apžvalga*. Kurk Lietuvai. 2018. Žiniatinklyje: http://kurklt.lt/wp-content/uploads/2018/04/Esamos-situacijos-ap%5C%C5%5C%BEvalga-FINAL.pdf (žr. psl. 10).

[51] Rodney Petersen ir kt. *Workforce framework for cybersecurity (NICE framework)*. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD. 2020. DOI: 10.6028/NIST.SP.800-181r1. Žiniatinklyje: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=931370 (žr. psl. 10, 16).

[53] Office of the Privacy Commissioner of Canada. *Privacy and Cyber Security: Emphasizing privacy protection in cyber security activities*. 2015-02-12. Žiniatinklyje: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/cs_201412/ Lankytasi: 2022-07-24 (žr. psl. 78).

[54] Emma Ryttare. *Change Management: A Key in Achieving Successful Cyber Security : A Multiple Case Study of Organizations in Sweden*. 2019. Žiniatinklyje: http://urn.kb.se/resolve?urn=urn:nbn:se:ltu:diva-74788 (žr. psl. 85).

[57] *SPARTA*. Žiniatinklyje: https://www.sparta.eu/ (žr. psl. 23).

[60] The Council of the European Union. *The European Qualifications Framework*. 2017. Žiniatinklyje: https://europa.eu/europass/en/european-qualifications-framework-eqf (žr. psl. 17).

[61] The European Commission. *ESCO Skill-Occupation Matrix Tables*. 2021. Žiniatinklyje: https://esco.ec.europa.eu/system/files/2021-07/en_ESCO%5C%20Skill-Occupation%5C%20Matrix%5C%20Tables%5C%20Technical%5C%20Report.pdf Lankytasi: 2022-07-18 (žr. psl. 18, 97).

[62] The European Commission. *ESCO Skill-Occupation classifier*. 2022. Žiniatinklyje: https://esco.ec.europa.eu/en/classification/occupation_main Lankytasi: 2022-07-18 (žr. psl. 97).

[63] The European Parliament and The Council of the European Union. *General Data Protection Regulation (GDPR)*. 2022. Žiniatinklyje: https://gdpr.eu/tag/gdpr/ (žr. psl. 15).

[68] Women4Cyber Lietuva. *Moterys griauna mitus apie kibernetinį saugumą: Lietuvoje be darbo neliks*. 2021. Žiniatinklyje: https://www.15min.lt/verslas/naujiena/mokslas-it/moterys-lietuvoje-griauna-mitus-apie-kibernetini-sauguma-nauju-tikslu-reikia-siekti-naudojant-naujus-metodus-1290-1515246 (žr. psl. 43).

A. Priedai

A.1. Omnibus: Visuomenės požiūrio į kibernetinį saugumą apklausa

Reprezentatyvi Lietuvos gyventojų apklausa buvo atlikta 2021 metų rugsėjo 17 – spalio 3 d. pagal su užsakovu suderintą klausimyną apklausą atliko Lietuvos – Didžiosios Britanijos rinkos ir viešosios nuomonės tyrimų kompanija „Baltijos tyrimai“. Tyrimo metu buvo apklausti 1004 Lietuvos gyventojai (18 metų ir vyresni).

A.1.1. KSS Klausimyno dalis

Klausimai apie kibernetines grėsmes

K1. Ką jūs manote apie visuomenės švietimą kibernetinių grėsmių klausimu? Nurodykite vieną atsakymą, kuris labiausiai atitinka jūsų nuomonę. (Skaityti atsakymų variantus. Tik vienas atsakymas)
   (a) Per daug jau mokymų ta tema – daugiau nieko nereikia
   (b) Žiniasklaida apie tai rašo pakankamai, tegu ir toliau tai daro
   (c) Šia tema galėtų būti daugiau mokymų mokyklose ir universitetuose
   (d) Informacijos apie kibernetines grėsmes nepakanka – reikėtų daugiau viešai prieinamų šaltinių ir mokymų ta tema
   9. (Neskaityti) Nežino, neatsakė

K2. Kokias funkcijas, jūsų nuomone, atlieka kibernetinio saugumo specialistas? Nurodykite vieną atsakymą, kuris labiausiai atitinka jūsų nuomonę. (Skaityti atsakymų variantus. Tik vienas

atsakymas)

(a) Stebi kompiuterinių sistemų veiklą ir reaguoja į iškilusius saugumo įvykius
(b) Kuria žiniatinklio svetaines, puslapius, informacines sistemas
(c) Prižiūri kompiuterių tinklus, administruoja kompiuterius
(d) Kuria telefonams skirtas programėles ir / ar kompiuterinius žaidimus
9. (Neskaityti) Nežino, neatsakė

K3. Pasakykite, ar jūs visiškai sutinkate, greičiau sutinkate, greičiau nesutinkate ar visiškai nesutinkate su šiais teiginiais apie galimybę tapti kibernetinio saugumo specialistu? (Skaityti teiginiais. Klausti ir žymėti apie kiekvieną)

	Visiškai sutinku – Visiškai nesutinku	N/N
Kibernetinio saugumo specialistu įmanoma tapti persikvalifikavus iš bet kurios kitos profesijos	1 – 4	9
Kibernetinio saugumo specialistu gali būti bet kurio amžiaus asmuo	1 – 4	9
Kibernetinio saugumo specialistu įmanoma tapti mokantis savarankiškai	1 – 4	9

K4. Kaip jūs manote, ar tokios mokslo sritys yra svarbios, ruošiant kibernetinio saugumo specialistus bei dirbant šioje srityje? Apie kiekvieną iš pateiktų sričių pasakykite, ar ji yra labai svarbi, greičiau svarbi, greičiau nesvarbi ar visiškai nesvarbi? (Skaityti teiginiais. Klausti ir žymėti apie kiekvieną)

	Visiškai sutinku – Visiškai nesutinku	N/N
Gamtos mokslai (fizika, informatika, matematika)	1 – 4	9
Technologiniai mokslai (informatikos ir elektronikos inžinerija)	1 – 4	9
Humanitariniai mokslai (istorija, filologija, filosofija)	1 – 4	9
Socialiniai mokslai (komunikacija ir informacija, teisė, politikos mokslai, psichologija)	1 – 4	9

K5. Kaip jūs manote, kokia dalis procentais tarp kibernetinio saugumo specialistų turėtų būti moterys? (Perskaityti atsakymų variantus. Tik vienas atsakymas)

(a) Iki 30 procentų
(b) Nuo 30 iki 60 procentų
(c) Nuo 60 iki 90 procentų
(d) Daugiau nei 90 procentų

9. (Neskaityti) Nežino, neatsakė

K6. Jeigu jus pakviestų tarnauti į Lietuvos Kariuomenę, ar jūs norėtumėte tarnauti kaip "kibernetinio saugumo šauktinis" - dirbti su kompiuteriu ir mokytis ginti kompiuterines sistemas? (**Šis klausimas užduotas tik tiems, kurie patenka į amžiaus 18–25 metų grupę**).

(a) Taip

(b) Ne

9. (Neskaityti) Nežino, neatsakė

Omnibus: Survey on public attitudes towards cybersecurity

Lithuanian population survey September 2021. A representative survey of the Lithuanian population was carried out on 17 September - 3 October 2021 by the Lithuanian - British market and opinion research company **UAB Baltijos tyrimai**, according to a questionnaire agreed. The survey covered 1004 X country residents (aged 18 and over).

Questions

Questions for general population from OMNIBUS related to understanding of Cybersecurity

K1. What do you think about educating the public about cyber threats? Please give one answer that best fits your opinion. (Read the answer choices. Only one answer)
   (a) Too much training on the subject already - nothing more needed
   (b) The media have written enough about it, let them continue to do so
   (c) There could be more training in schools and universities on this topic
   (d) Not enough information on cyber threats — need more publicly available sources and training on cyber threats
   9. (Not marked) Don't know, did not answer

K2. What do you see as the role of a cybersecurity professional? Please select the one answer that most closely matches your opinion. (Read the answer choices. Only one answer)
   (a) Monitor the performance of computer systems and respond to security incidents
   (b) Creates web sites, pages, information systems
   (c) Maintain computer networks, administer computers
   (d) Developing applications and/or computer games for phones
   9. (Not marked) Don't know, did not answer

K3. Please tell whether you completely agree, rather agree, rather disagree or completely disagree with the following statements about the possibility of becoming a cybersecurity professional? (Read the statements. Ask and tick about each)

	Strongly agree – Strongly disagree	N/N
It is possible to become a cyber security professional by retraining from any other profession	1 – 4	9
You can be a cybersecurity professional at any age	1 – 4	9
It is possible to become a cybersecurity professional through self-study	1 – 4	9

K4. Do you think that such scientific fields are important for the training and work of cyber security

professionals? For each of the following areas, please tell us whether it is very important, rather important, rather unimportant or not important at all? (Read in statements. Ask and mark for each)

	Strongly agree – Strongly disagree	N/N
Natural sciences (physics, computer science, mathematics)	1 – 4	9
Technological sciences (computer and electronic engineering)	1 – 4	9
Humanities (history, philology, philosophy)	1 – 4	9
Social sciences (communication and information, law, political science, psychology)	1 – 4	9

K5. What percentage of cyber security professionals do you think should be women? (Read the answer choices. Only one answer)
   (a) Up to 30 percent
   (b) Between 30 and 60 percent
   (c) Between 60 and 90 percent
   (d) More than 90 percent
   9. (Not marked) Don't know, did not answer

K6. If you were tasked to serve in the X Country Armed Forces, would you like to serve as a "cyber security conscript" - working with computers and learning how to defend computer systems? (**This question is only asked to those in the 18–25 age group**).
   (a) Yes
   (b) No
   9. (Not marked) Don't know, did not answer

A.2. Organizacijų vadovų tyrimas

A.2.1. Klausimynas

Klausimyno struktūra ir klausimai, kurie pateikti Lietuvos organizacijų sprendimų priėmėjų apklausai.

Trumpas prisistatymo puslapis.

Sveiki,

Reikminio tyrimo projektui Kibernetinio saugumo kompetencijų modelio kūrimas finansavimą skyrė Lietuvos mokslo taryba (LMTLT), Nr. P-REP-21-2. Projekte atliekamas kibernetinio saugumo kompetencijų lauko tyrimas siekiant ištirti kibernetinio saugumo srities ir joje dirbančių specialistų specifiką Lietuvos įmonėse ir organizacijose. Projektą vykdo Vilniaus universitetas ir Generolo Jono Žemaičio Lietuvos karo akademija, o organizacijų apklausą įgyvendina UAB Rinkos tyrimų centras. Tyrimo metu bus apklausti IT padalinių vadovai, IT ir kibernetinio saugumo specialistai iš privačių ir valstybinių įmonių visoje Lietuvoje. Apklausa anoniminė. Anketos trukmė – 15 min.

"Kibernetinio saugumo" sąvoka mes suprantame tokius dalykus kaip: rūpinimasis įmonės informacinių technologijų ir duomenų saugumu, pažeidžiamų sričių analizė ir prevencija, IT konsultacijos ir auditas, BDAR (angl. GDPR), kibernetiniai tyrimai ir pan. Jūsų nuomonė mums yra itin svarbi. Dėkojame už Jūsų atsakymus!

Pradėti apklausą adresu: http://www..

Pagarbiai

Esamos situacijos vertinimas

Kiek apskritai aktuali ir svarbi Jūsų įmonės veiklai yra kibernetinio saugumo problema? „Kibernetinio saugumo“ sąvoka mes suprantame tokius dalykus kaip: rūpinimasis įmonės informacinių technologijų ir duomenų saugumu, pažeidžiamų sričių analizė ir prevencija, IT konsultacijos ir auditas, GDPR, kibernetiniai tyrimai ir pan.

A1. Kibernetinio saugumo svarba/aktualumas Jūsų įmonei/organizacijai:

1. labai aktuali sritis
2. aktuali sritis
3. vidutiniškai aktuali
4. mažai aktuali
5. visiškai neaktuali sritis
6. nežinau / sunku pasakyti

A2 . Kiek jūsų įmonėje/organizacijoje yra darbuotojų, kurie atlieka darbus, susijusius su kibernetiniu įmonės saugumu (t.y. jų pagrindinė arba viena iš funkcijų yra įmonės kibernetinis saugumas) ?

1. (įrašykite skaičių)
2. Tokių nėra (PEREITI PRIE KL. A4)

A3. Ar Jūsų įmonėje yra išskirtos ir aprašytos kokios nors kibernetinio saugumo specialisto pareigybinės funkcijos?

1. Taip, yra aiškiai aprašyta
2. Taip, iš dalies
3. Ne, tokio aprašo nėra
4. Nežinau/ sunku pasakyti

A4. Ar Jūsų įmonė samdo išorinius paslaugų teikėjus kibernetinio saugumo darbams? 1.Taip 2.Ne 3.Nežinau

A5. Ar per paskutinius 2-5 metus kibernetinio saugumo klausimams įmonėje pradėjote skirti didesnį dėmesį, pavyzdžiui daugiau finansinių ar žmogiškųjų resursų?

1. Skiriame dėmesio daugiau
2. Skiriame dėmesio tiek pat
3. Skiriame mažiau dėmesio
4. Nežinau/ sunku pasakyti

#.

. . . . . .

A6. Ar per ateinančius 2-5 metus kibernetinio saugumo klausimams planuojate skirti didesnį dėmėsį?

1. Taip, skirsime dėmesio daugiau
2. Skirsime dėmesio tiek pat
3. Skirsime mažiau dėmesio
4. Nežinau/ sunku pasakyti

#.

. . . . . .

A7. Kiek tikėtina, kad per ateinančius 2-5 metus įmonėje bus įdarbinti papildomi specialistai darbui (pilnai ar iš dalies) kibernetinio saugumo srityje?

1. Labai tikėtina
2. Tikėtina
3. Mažai tikėtina
4. Nežinau/ sunku pasakyti

#.

. . . . . .

A8. Jūsų nuomone, ar trūksta Lietuvoje kibernetinio saugumo specialistų (KSS)?

1. Trūkumas yra labai didelis
2. Šiek tiek trūksta
3. Netrūksta
4. Nežinau/ sunku pasakyti

#.

. . . . . .

A9. Vieni mano, kad geram KS specialistui yra svarbiausia gilios techninės žinios, kiti gi linkę manyti, kad itin svarbu „minkštosios“ kompetencijos (pvz., vadybos žinios, užsienio kalbos, noras mokytis ir tobulėti, bendravimas su klientais, teisinės žinios, komandinis darbas ir t.t.). Jei Jūs ieškotumėte KSS, kiek kreiptumėte dėmesį į vienas ir kiek į kitas kompetencijas?

Dėmesys išskirtinai techninėms kompetencijoms	1—2—3-...-8—9—10	Dėmesys išskirtinai „minkštosioms“ kompetencijoms

A10. Jūsų nuomone, ar IT specialistas gali atlikti ir kibernetinio saugumo specialisto (KSS) funkcijas?

1. Taip, vienas ir tas pats specialistas gali tuo pilnai pasirūpinti
2. Taip, šių sričių specialistų funkcijos iš dalies persidengia
3. Kibernetinio įmonės saugumo ir IT sritimi turėtų rūpintis skirtingi darbuotojai
4. Nežinau/ sunku pasakyti

įrašykite: #. . . . . .

A11. Toliau pateiksime keletą skirtingų veiklų ir funkcijų, kurias įvairiose įmonėse atlieka KSS. Pagalvokite, apie ateinančius 2-5 metus, ir pasakykite, kuriose iš šių sričių Jūsų įmonei/organizacijai gali būti reikalingos šios KSS kompetencijos ir žinios. Vertinkite 5 balų skalėje, kur 1 reiškia, kad tokio poreikio greičiau nebus, o 5 reikštų, kad tokios kompetencijos labai tikėtina, kad bus tikrai reikalingos.

Veikla	Aprašymas	Poreikis
1. Saugumo sistemų kūrimas ir vystymas	Rizikų valdymas, programų kūrimas, saugumo priemonių vertinimas, programavimas, technologijų tyrimas ir plėtra, sistemų architektūra, testavimas ir vertinimas ir pan.	1-2-3-4-5
2. Saugumo sistemų ir operacijų palaikymas	Duomenų ir sistemos administravimas, pagalba vartotojams, technikos ir programų diegėjas ir prižiūrėtojas, duomenų analitikas saugumo užtikrinimo tikslais, tinklo planavimas, diegimas ir priežiūra	1-2-3-4-5
3. Vadovavimas ir priežiūra	Strateginis KS planavimas, teisinė pagalba KS klausimais, privatumo palaikymas, duomenų saugos inspektavimas, mokymai KS temomis, KS personalo atranka, KS investicijų planavimas ir KS auditas	1-2-3-4-5
4. Apsauga ir gynyba	Kibernetinės gynybos analizė, incidentų valdymas, pažeidžiamumų vertinimas	1-2-3-4-5
5. Duomenų surinkimas ir analizė	Grėsmių, įsibrovimų analizė, „etiškas“ įsibrovėlis, kalbų specialistas kibernetinėms grėsmėms, duomenų surinkimo operacijos, „visų šaltinių“ analizė	1-2-3-4-5
6. Kibernetiniai tyrimai	Kibernetinių nusikaltimų tyrimai	1-2-3-4-5

įvertinkite visus : ..... #.

Demografinė informacija

Pabaigas keletas klausimų apie Jūsų įmonę/organziciją:

D1. Sektorius: 1. Viešas 2.Privatus ..... #.

D2. Įmonės dydis(darbuotojų skaičius):

D2A. 1. iki 10 darbuotojų 2. 11-50 3. 51-250 4. virs 251 darbuotojų

D3. Metinė įmonės apyvarta:

1. 0–145 000 Eur.
2. 145 000–1 000 000 Eur
3. 1 000 000–5 000 000 Eur
4. 5 000 000–10 000 000 Eur
5. Virš 10 000 000 eur
6. Nežinau / negaliu pasakyti

D4. Pagrindinės įmonės (organizacijos) veiklos sritys: (įrašyti)

D5. Jūsų pareigos:

1. Vadovas
2. Personalo vadovas
3. Padalinio/filialo/skyriaus vadovas
4. IT specialistas
5. Kita

Dėkojame už Jūsų atsakymus!

A.2.2. The questionnaire

The structure of the questionnaire and the questions for the survey of decision-makers in Lithuanian organisations. The survey of organisations is implemented by the marker research expert company **UAB Rinkos tyrimų centras**. A short introduction page.

Dear respondent,

The project studies the field of cybersecurity competences in order to investigate the specifics of the cyber security field and the professionals working in it in Lithuanian companies and organisations. The project is carried out by Vilnius University and the General Jonas Žemaitis Military Academy of Lithuania, and the survey of organisations is implemented by UAB Rinkos tyrimų centras. The survey will interview IT department managers, IT and cybersecurity professionals from private and public companies across Lithuania. The survey is anonymous. The duration of the questionnaire is 15 minutes. The funding for the research project Development of a Cyber Security Competence Model was granted by the Research Council of Lithuania (RCL), No. P-REP-21-2.

"Cybersecurity is defined as: taking care of the company's IT and data security, analysis and prevention of vulnerable areas, IT consulting and auditing, GDPR, cyber investigations, etc.

Your opinion is very important to us. Thank you for your answers!

Start the survey at: http://www....

Sincerely

Assessment of the current situation

How relevant and important is cyber security to your company's operations in general? By "cyber security" we mean things such as: taking care of the company's IT and data security, analysis and prevention of vulnerable areas, IT consulting and auditing, GDPR, cyber investigations, etc.

A1. importance/relevance of cybersecurity for your company/organisation:

1. A very relevalnt area for
2. important area
3. moderately relevant
4. low relevance
5. not relevant at all
6. don't know / difficult to say

A2. How many employees in your company/organisation are involved in cybersecurity-related work (i.e. cybersecurity is their main or one of their functions) ?

1. (please enter the number)
2. None (MOVE TO QUESTION A4.)

A3. Do you have any specific job functions for a cyber security specialist in your company?

1. Yes, it is clearly described
2. Yes, partially
3. No, there is no such description
4. Don't know/difficult to say

A4. Does your company use external service providers for cyber security work? . . . . . 1.Yes 2.No 3.Don't know

A5. In the last 2-5 years, have you started to pay more attention to cybersecurity issues in your company, e.g. more financial and human resources vise?

1. Paying more attention
2. Paying as much attention as previous
3. Pay less attention
4. Don't know/difficult to say

#.

. . . . . .

A6. Do you plan to increase your focus on cybersecurity in the next 2-5 years?

1. Yes, we will pay more attention
2. We'll pay the same amount of attention
3. We will pay less attention
4. Don't know/difficult to say

#.

. . . . . .

A7. How likely is it that the company will recruit additional specialists to work (fully or partially) in the field of cyber security in the next 2-5 years?

1. Very likely
2. Likely
3. Unlikely
4. Don't know/difficult to say

#.

. . . . . .

A8. In your opinion, is there a shortage of cyber security professionals in the Country?

1. The shortfall is very high
2. Slightly lacking
3. Not missing
4. Don't know/difficult to say

#.

. . . . . .

A9. Some believe that deep technical knowledge is the most important for a good cybersecurity professional, while others tend to think that soft competences (e.g. management knowledge, foreign languages, willingness to learn and develop, communication with clients, legal knowledge, teamwork, etc.) are crucial. If you were looking for a cybersecurity spcialits, how much would you focus on one set of competences and how much on the others?

Focusing exclusively on technical competences	1—2—3-...-8—9—10	Focusing exclusively on "soft" competences

A10. In your opinion, can an IT professional also act as a Cyber Security Specialist?

1. Yes, one and the same specialist can take full care of it
2. Yes, there is some overlap between these professionals
3. Different people should be involved in cyber security and IT
4. Don't know/difficult to say

write other: #. .....

A11. Bellow are some of the different activities and functions performed by Cybersecurity specialist in companies. Think about the next 2–5 years and tell us which of the following areas your company/organisation might need the competences and knowledge of these Cybersecurity specialists. Please rate on a 5-point scale, where 1 means that there is unlikely to be a need, and 5 means that there is very likely to be a real need for these competences.

Activities	Description	Need
1. Security Systems Design and Development	Risk Management, Application Development, Security Tool Evaluation, Programming, Technology Research and Development, System Architecture, Testing and Evaluation, etc.	1-2-3-4-5
2. Security Systems and Operations Support	Data and system administration, user support, technical and application installer and maintainer, data analyst for security purposes, network planning, installation and maintenance	1-2-3-4-5
3. Management and Supervision	Strategic QA planning, legal support for QA issues, privacy support, data security inspections, QA training, QA staffing, QA investment planning and QA audit	1-2-3-4-5
4. Security and Defence	Cyber Defence Analysis, Incident Management, Vulnerability Assessment	1-2-3-4-5
5. Data Collection and Analysis	Threat, Intrusion Analysis, "ethical" intruder, cyber threat language specialist, data collection operations, "all-source" analysis	1-2-3-4-5
6. Cyber Investigations	Cybercrime Investigations	1-2-3-4-5

please rate all : . . . . . #.

Demographic information

Finally, some questions about your company/organisation:

D1. Sector: 1. Public 2.Private . . . . . #.

D2. Company size (number of employees): . . . . . #.

D2A. 1. up to 10 employees 2. 11–50 3. 51–250 4. over 251 employees . . . . . #.

D3. Annual turnover:

1. 0–145 000 EUR.
2. 145 000–1 000 000 EUR
3. 1 000 000–5 000 000 EUR
4. 5 000 000–10 000 000 EUR
5. Above EUR 10 000 000
6. Don't know / can't say

. . . . . #.

D4. Main activities of the enterprise/organisation: (insert) . . . . . #.

D5. Your responsibilities:

1. Manager
2. Personnel Manager
3. Head of Unit/Branch/Division
4. IT Specialist
5. Other

. . . . . #.

Thank you for your answers!

A.2.3. Aprašomoji informacija

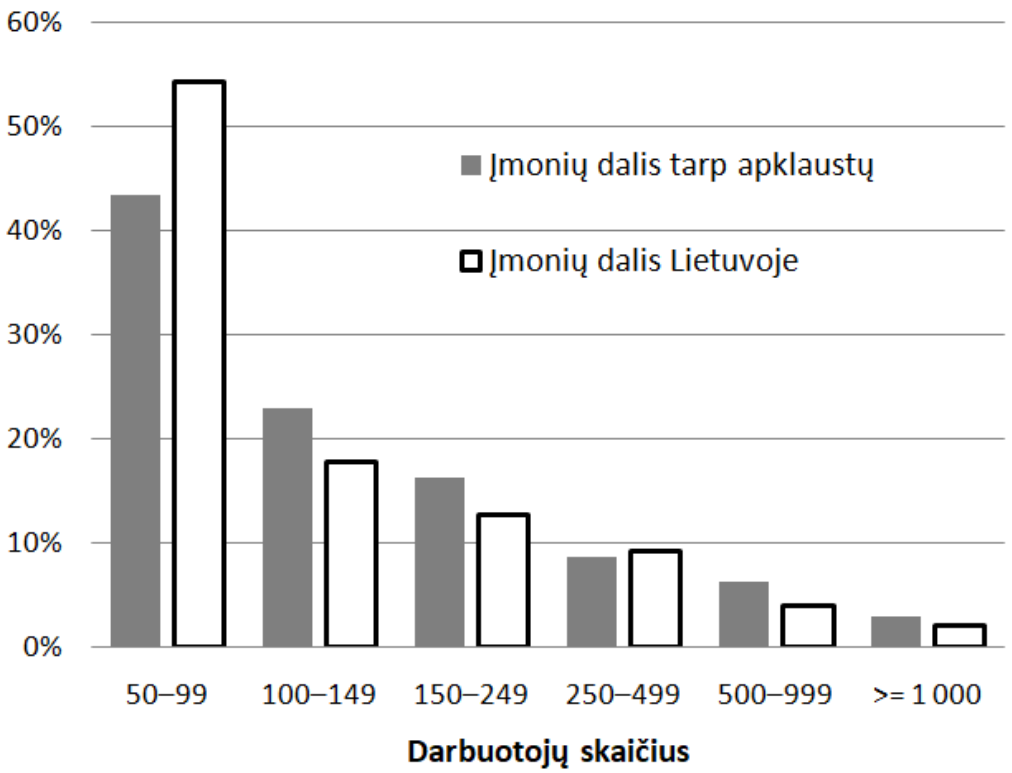
Lentelėje A.1 pateiktas respondentų pasiskirstymas pagal pareigas ir sektorius.

A.1 lentelė. Respondentų pareigų pasiskirstymas pagal sektorius

Sektorius (D1)	Pareigos (D5)	Dažnis	Proc.	Suminis proc.
Privatus	IT specialistas	2	0,935	0,935
	Kita	20	9,346	10,280
	Personalo vadovas	105	49,065	59,346
	Skyriaus vadovas	16	7,477	66,822
	Vadovas	71	33,178	100,000
	Iš viso	214	100,000	
Viešas	IT specialistas	0	0,000	0,000
	Kita	4	12,5	12,5
	Personalo vadovas	10	31,25	43,75
	Skyriaus vadovas	4	12,5	56,25
	Vadovas	14	43,75	100,000
	Iš viso	34	100,000	

Lentelėje A.2 pateikti agreguoti atsakymai į klausimą A10 (ar KS funkcijas gali atlikti IT specialistas).

Papildomas duomenų validumo vertinimas: apklausoje dalyvavusių įmonių dydis nuosekliai auga kartu su apyvarta, kaip ir reikia tikėtis (Lentelėje A.3 neįtrauktos 57 eilutės, kuriose nepateikta apyvarta). Analogiškai: personalo vadovų skaičius auga kartu su įmonės dydžiu. Apklausa buvo tikslingai nukreipta į didesnes įmones. Imant tik tas įmones, kuriose dirba 50 darbuotojų arba daugiau, apklausoje sudalyvavusių įmonių pasiskirstymas tiksliai atkartoja įmonių pasiskirstymą Lietuvoje (pagal 2022 metų pradžios Lietuvos statistikos departamento stat.gov.lt duomenis), žr. A.1.



A.1 pav. Įmonių, kuriose dirba 50 ar daugiau darbuotojų, pasiskirstymas

A.2 lentelė. Ar KS funkcijas gali atlikti IT specialistas

Pareigos (D5)	Ar IT spec gali dirbti kaip KS (A10)	Dažnis	Proc.	Suminis proc.
Vadovas	1: Taip	20	23,53	23,53
	2: Dalinai	48	56,47	80,00
	3: Ne	11	12,94	92,94
	4: Sunku pasakyti	6	7,06	100,00
	Iš viso	85	100,00	
Personalo vadovas	1: Taip	25	21,74	21,74
	2: Dalinai	66	57,39	79,13
	3: Ne	20	17,39	96,52
	4: Sunku pasakyti	4	3,48	100,00
	Iš viso	115		
Skyriaus vadovas	1: Taip	6	30,00	30,00
	2: Dalinai	13	65,00	95,00
	3: Ne	0	0,00	95,00
	4: Sunku pasakyti	1	5,00	100,00
	Iš viso	20	100,00	
IT specialistas	1: Taip	0	0,00	0,00
	2: Dalinai	1	50,00	50,00
	3: Ne	1	50,00	100,00
	4: Sunku pasakyti	0	0,00	100,00
	Iš viso	2	100,00	
Kita	1: Taip	9	37,50	37,50
	2: Dalinai	11	45,83	83,33
	3: Ne	2	8,33	91,67
	4: Sunku pasakyti	2	8,33	100,00
	Iš viso	24	100,00	

A.3 lentelė. Įmonių dydis pagal apyvartą (tik 190 įmonių nurodė savo apyvartą)

	Dydis (D2A)				
Apyvarta (M€)	1: <0,145	2: 0,145-1	3: 1-5	4: 5-10	5: >10
Kiekis	13	36	70	36	35
Įm.dydis (Vidurkis)	1,231	2,306	2,857	3,056	3,371
Stand.deviacija	0,599	0,856	0,490	0,333	0,598
Min.	1,000	1,000	1,000	2,000	2,000
Maks.	3,000	4,000	4,000	4,000	4,000

A.3. KS specialistų apklausa

A.3.1. Klausimynas

Klausimyno struktūra ir klausimai, kurie pateikti viešos nuomonės apklausai.

Trumpas prisistatymo puslapis.

Sveiki,

Reikminio tyrimo projektui Kibernetinio saugumo kompetencijų modelio kūrimas finansavimą skyrė Lietuvos mokslo taryba (LMTLT), Nr. P-REP-21-2. Projekte atliekamas kibernetinio saugumo kompetencijų lauko tyrimas siekiant ištirti kibernetinio saugumo srities ir joje dirbančių specialistų specifiką Lietuvos įmonėse ir organizacijose. Projektą vykdo Vilniaus universitetas ir Generolo Jono Žemaičio Lietuvos karo akademija, o organizacijų apklausą įgyvendina UAB Rinkos tyrimų centras. Tyrimo metu bus apklausti IT padalinių vadovai, IT ir kibernetinio saugumo specialistai iš privačių ir valstybinių įmonių visoje Lietuvoje. Apklausa anoniminė. Anketos trukmė – 15 min.

"Kibernetinio saugumo" sąvoka mes suprantame tokius dalykus kaip: rūpinimasis įmonės informacinių technologijų ir duomenų saugumu, pažeidžiamų sričių analizė ir prevencija, IT konsultacijos ir auditas, BDAR (angl. GDPR), kibernetiniai tyrimai ir pan. Jūsų nuomonė mums yra itin svarbi. Dėkojame už Jūsų atsakymus!

Pradėti apklausą adresu: http://www..

Pagarbiai

Keletas klausimų apie Jūsų įmonę/organizaciją (pažymėkite/įrašykite)

D1. Sektorius . . . . . 1. Viešas 2. Privatus

D2. Įmonės dydis: (darbuotojų skaičius): 1. <10 2. <50 3. <250 4. >250 . . . . . .

D3. Pagrindinės įmonės (organizacijos) veiklos sritys:

D4. Jūsų pareigos: a1=1. Padalinio(IT)/filialo/skyriaus vadovas a2=2. IT specialistas, a3=3. Kita...įrašykite a1 a2 a3

D5. Kiek jūsų įmonėje/organizacijoje yra darbuotojų, kurie atlieka darbus, susijusius su kibernetiniu įmonės saugumu (t.y. jų pagrindinė arba viena iš funkcijų yra įmonės kibernetinis saugumas) (įrašykite skaičių)?

D6. Ar Jūsų įmonė samdo išorinius paslaugų teikėjus kibernetinio saugumo darbams? a1=1. Taip,a2=2. Ne (PEREITI PRIE KL D7), a3=3. Nežinau (PEREITI PRIE KL D7) a1 a2 a3

D6.1 Kurioms KS sritims ar darbams yra samdomi išoriniai paslaugų teikėjai (pasirinkti kelias)?

1. Organizacijos informacinių technologijų, tinklų bei kitų sistemų saugumo priežiūra ir valdymas
2. Teisinis reguliavimas, formalioji duomenų apsauga ir veiklos BDAR užtikrinti
3. Saugumo technologiniai architektai, saugių technologinių ir programinių sistemų kūrėjai
4. Kibernetinio saugumo srities moksliniai tyrimai, inovacijos, mokymai
5. Incidento valdymas ir technologinė pagalba incidento metu
6. Kibernetinių incidentų/nusikaltimų tyrimai
7. Organizacijos kibernetinio/fizinio saugumo, perimetro gynybos testavimas
8. Organizacijos saugumo ir procedūrų/procesų auditavimas
9. Rizikos vertinimas bei valdymas
10. Kita: ...

D7. Ar jūsų įmonėje reikalaujama ar tikimasi iš kibernetinio saugumo specialistų kokių nors diplomų ar sertifikatų? a1=1. Taip, a2=2. Ne (PEREITI PRIE KL D8), a3=3. Nežinau (PEREITI PRIE KL D8) a1 a2 a3

D7.1 Kokių diplomų ar sertifikatų reikalaujama?

D8. Pažymėkite, kurios kibernetinio saugumo veiklos atliekamos jūsų įmonėje/organizacijoje?

1. Organizacijos informacinių technologijų, tinklų bei kitų sistemų saugumo priežiūra ir valdymas
2. Teisinis reguliavimas, formalioji duomenų apsauga ir veiklos BDAR užtikrinti
3. Saugumo technologiniai architektai, saugių technologinių ir programinių sistemų kūrėjai
4. Kibernetinio saugumo srities moksliniai tyrimai, inovacijos, mokymai
5. Incidento valdymas ir technologinė pagalba incidento metu
6. Kibernetinių incidentų/nusikaltimų tyrimai
7. Organizacijos kibernetinio/fizinio saugumo, perimetro gynybos testavimas
8. Organizacijos saugumo ir procedūrų/procesų auditavimas
9. Rizikos vertinimas bei valdymas
10. Kita: ...

D9. Vieni mano, kad geram KS specialistui svarbiausios gilios techninės žinios, kiti linkę manyti, kad svarbios „minkštosios“ kompetencijos (pvz., vadybos žinios, užsienio kalbos, noras mokytis ir tobulėti, bendravimas su klientais, teisinės žinios, komandinis darbas ir t.t.). Jei Jūs ieškotumėte KS specialisto, kiek atkreiptumėte dėmesį į vienas ir kiek į kitas kompetencijas?

Dėmėsys išskirtinai techninėms kompetencijoms	1—2—3—4 ... 7—8—9—10	Dėmesys išskirtinai „minkštosioms“ kompetencijoms

D10. Pažymėkite Jūsų organizacijoje atliekamas planavimo, vadovavimo ir priežiūros veiklas, susijusias su kibernetiniu saugumu:

1. Kibernetinio saugumo juridinės konsultacijos (angl. Cyber Legal Advisor)
2. Vadovavimas, privatumo reikalavimų palaikymas ir užtikrinimas (angl. Privacy Officer/Privacy Compliance Manager)
3. Duomenų apsaugos pareigūnas (angl. Data Protection Officer)
4. Kibernetinio saugumo mokymų kūrimas/instruktavimas (angl. Cyber Instructional Curriculum Developer / Instructor / Educator)
5. Vadovavimas informacinių sistemų saugumo klausimais (angl. Information Systems Security Manager)

6. Vadovavimas komunikacinių sistemų saugumo klausimais (angl. Communications Security (COMSEC) Manager)
7. Strateginis planavimas: Kibernetinio saugumo personalo plėtra (angl. Cyber Workforce Developer and Manager)
8. Strateginis planavimas: Kibernetinio saugumo politikos ir strategijos kūrimas (angl. Cyber Policy and Strategy Planner)
9. Lyderystė: Vizijos kūrimas ir sprendimų priėmimas (angl. Executive Cyber Leadership)
10. Vadovavimas IT projektams (angl. IT Project Manager)
11. Vadovavimas palaikant produktą - rūpinasi, kad sistemos veiktų (angl. Product Support Manager)
12. IT investicijų portfelio valdymas (angl. IT Investment/Portfolio Manager)
13. IT programų auditavimas (angl. IT Program Auditor)
14. Kita: ...

D11. Pažymėkite Jūsų organizacijoje atliekamas apsaugos ir gynybos veiklas, susijusias su kibernetiniu saugumu:

1. Kibernetinės gynybos analizė - analizuoja įvykius (pagal gautus kitų sistemų duomenis) (angl. Cyber Defense Analyst)
2. Kibernetinės gynybos infrastruktūros palaikymas (angl. Cyber Defense Infrastructure Support Specialist)
3. Incidentų valdymas: Reagavimas į incidentus (angl. Cyber Defense Incident Responder)
4. Pažeidžiamumų vertinimas ir analizė (angl. Vulnerability Assessment Analyst)
5. Kita: ...

D12. Pažymėkite Jūsų organizacijoje atliekamas duomenų rinkimo ir analizės veiklas, susijusias su kibernetiniu saugumu:

1. Grėsmių analizė (angl. Threat/Warning Analyst)
2. Etiškas įsibrovimas (angl. Exploitation Analyst)
3. Visų informacijos šaltinių analizė (kibernetinio saugumo klausimais) (angl. All-Source Analyst)

4. Kibernetinė žvalgyba (angl. Cyber Intel Planner)
5. Kibernetinių nusikaltimų tyrimai (angl. Cyber Defense Forensics Analyst)
6. Kita: ...

D13. Pažymėkite Jūsų organizacijoje atliekamas duomenų ir sistemų administravimo veiklas, susijusias su kibernetiniu saugumu:

1. Duomenų bazių valdymo sistemų administravimas (angl. Database Administrator)
2. Duomenų analizė (angl. Data Analyst) - kuria algoritmus, procesus ir atvaizdžius sudėtingiems duomenims modeliavimo ar duomenų gavybos tikslais
3. Žinių valdymas (angl. Knowledge Manager) - siejamas su intelektinio kapitalo ir informacinio turinio valdymo įrankiais
4. Techninės pagalbos vartotojams teikimas (angl. Technical Support Specialist)
5. Tinklo sistemų ir paslaugų planavimas, diegimas ir priežiūra, įskaitant virtualią aplinką (angl. Network Operations Specialist)
6. Sistemų administravimas - technikos ir programų diegimas ir priežiūra, paskyrų valdymas (angl. System Administrator)
7. Sistemų saugumo analizė (angl. Systems Security Analyst)
8. Kita: ...

D14. Pažymėkite Jūsų organizacijoje atliekamas saugių produktų ir sistemų kūrimo veiklas, susijusias su kibernetiniu saugumu:

1. Rizikos valdymas: formali atsakomybė už sistemą (angl. Authorizing Official/Designating Representative)
2. Rizikos valdymas: Saugumo priemonių vertinimas (angl. Security Control Assessor) - vertina tiek vadybos, tiek technines priemones
3. Programų kūrimas: Programavimas (angl. Software Developer)
4. Programų kūrimas: Programų saugumo vertinimas (angl. Secure Software Assessor)
5. Sistemų architektūra: IT architektūros projektavimas (angl. Enterprise Architect)

6. Sistemų architektūra: Saugumo architektūros projektavimas (angl. Security Architect)
7. Testavimas ir vertinimas: Technologijų tyrimai ir plėtra (angl. Research & Development Specialist)
8. Reikalavimų sistemoms planavimas: Reikalavimų sistemoms planavimas (angl. Systems Requirements Planner) - paverčia funkcinius reikalavimus į techninius
9. Testavimas ir vertinimas: Testavimas (angl. System Testing and Evaluation Specialist)
10. Sistemų kūrimas: Informacinių sistemų saugumo kūrimas (angl. System Testing and Evaluation Specialist) - kiekviename etape rūpinasi, kad kuriamos sistemos būtų saugios
11. Sistemų kūrimas: Integruotų sistemų kūrimas (angl. Systems Developer)
12. Moksliniai tyrimai ir inovacijos (angl. Researcher)
13. Kita: ...

D15. Kokių sričių KS specialistų labiausiai trūksta jūsų įmonei ar Lietuvos rinkai apskritai?

D16. Kiek, Jūsų nuomone, skiriama dėmesio kibernetinio saugumo specialistų kvalifikacijos kėlimui Jūsų organizacijoje?

1. Daugiau nei pakankamai
2. Pakankamai
3. Beveik pakankamai
4. Per mažai
5. Visa neskiriama
6. Negaliu atsakyti

D17. Jūsų pasiūlymai / pageidavimai kibernetinio saugumo specialistų rengimui (kompetencijos,

atsakomybės, funkcijos, problemos ar pan.).

_____

_____

Dėkojame už Jūsų atsakymus!

A.3.2. Questionire

The structure of the questionnaire and the questions put to the opinion poll. The survey of specialists is implemented by the marker research expert company **UAB Rinkos tyrimų centras**.

A few questions about your company/organisation (please tick/type)

D1. Sector . . . . . 1. Public 2. Private

D2. Company size: (number of employees): 1. <10 2. <50 3. <250 4. >250 . . . . . .

D3. The main activities of the company/organisation:

D4. Your job title: a1=1. Head of department(IT)/branch/unit a2=2. IT Specialist, a3=3. Other...please enter a1 a2 a3

D5. How many employees in your company/organisation are involved in work related to the cybersecurity of the company (i.e. cybersecurity of the company is one of their main or one of their roles) (please enter the number)?

D6. Does your company outsource cybersecurity work? a1=1. Yes, a2=2. No (MOVE TO QUESTION D7), a3=3. Don't know (MOVE TO QUESTION D7) a1 a2 a3

D6.1 For which areas or works of the QA are external service providers hired (select a few)?

1. Maintenance and management of the security of the organisation's information technology, networks and other systems
2. Regulatory, formal data protection and GDPR compliance activities
3. Security technology architects, developers of secure technology and software systems
4. Cybersecurity research, innovation, training
5. Incident management and technological support during an incident

6. Cyber Incident/Crime Research
7. Cyber/physical security, perimeter defence testing
8. Auditing of organisational security and procedures/processes
9. Risk assessment and management
10. Other: ...

D7. Does your company require or expect any diplomas or certifications from cybersecurity professionals? a1=1. Yes, a2=2. No (MOVE TO QUESTION D8), a3=3. Don't know (MOVE TO QUESTION D8) a1 a2 a3

D7.1 What diplomas or certificates are required?

D8. Please tick which cybersecurity activities are carried out in your company/organisation?

1. Maintenance and management of the security of the organisation's information technology, networks and other systems
2. Regulatory, formal data protection and GDPR enforcement activities
3. Security technology architects, developers of secure technology and software systems
4. Cybersecurity research, innovation, training
5. Incident management and technological support during an incident
6. Cyber Incident/Crime Research
7. Cyber/physical security, perimeter defence testing
8. Auditing of organisational security and procedures/processes
9. Risk assessment and management
10. Other: ...

D9. Some consider that deep technical knowledge is the most important for a good cybersecurity professional, while others tend to consider "soft" competences (e.g. managerial knowledge, foreign languages, willingness to learn and develop, communication with clients, legal knowledge, teamwork, etc.) important. If you were looking for a Cybersecurity professional, how much would you pay attention to one set of competences and how much to the other?

Attention on purely technical competences	1—2—3—4 ... 7—8—9—10	Focusing exclusively on "soft" competences

D10. Please tick the planning, management and oversight activities related to cybersecurity in your organisation:

1. Cyber Legal Advisor
2. Privacy Officer/Privacy Compliance Manager
3. Data Protection Officer
4. Cyber Instructional Curriculum Developer / Instructor / Educator
5. Information Systems Security Manager
6. Communications Security (COMSEC) Manager
7. Strategic Planning: Cyber Workforce Developer and Manager
8. Strategic Planning: Cyber Security Policy and Strategy Planner
9. Leadership: Executive Cyber Leadership
10. IT Project Manager
11. Product Support Management — keeping systems running (Product Support Manager)
12. IT Investment/Portfolio Manager
13. IT Program Auditor
14. Other: ...

D11. Please tick the protection and defence activities related to cyber security in your organisation:

1. Cyber Defence Analyst — analyses events (based on data received from other systems)
2. Cyber Defence Infrastructure Support Specialist

3. Incident Management: Cyber Defence Incident Responder
4. Vulnerability Assessment Analyst
5. Other: ...

D12. Please tick the data collection and analysis activities related to cybersecurity in your organisation:

1. Threat/Warning Analyst
2. Exploitation Analyst
3. All-Source Analyst (Cybersecurity)
4. Cyber Intel Planner
5. Cyber Defense Forensics Analyst
6. Other: ...

D13. Please tick the cybersecurity-related data and systems administration activities in your organisation:

1. Database Administrator
2. Data Analyst — develops algorithms, processes and representations for complex data for modelling or data mining
3. Knowledge Manager — associated with intellectual capital and information content management tools
4. Technical Support Specialist (Technical Support Specialist)
5. Network Operations Specialist — Planning, implementation and maintenance of network systems and services, including virtual environments
6. System Administration — installation and maintenance of hardware and applications, account management (System Administrator)
7. Systems Security Analyst
8. Other: ...

D14. Please tick the cybersecurity-related activities in your organisation to develop secure products and systems:

1. Risk management: formal responsibility for the system (Authorizing Official/Designating Representative)
2. Risk Management: Security Control Assessor - assesses both management and technical measures
3. Software Development: Software Developer
4. Software Development: Secure Software Assessor
5. Systems Architecture: IT Architecture Design (Enterprise Architect)
6. Systems Architecture: Security Architect
7. Test & Evaluation: Technology Research & Development Specialist
8. Systems Requirements Planner: Systems Requirements Planner - translates functional requirements into technical requirements
9. Testing and Evaluation Specialist
10. Systems Development: Information Systems Security Development (System Testing and Evaluation Specialist) - at each stage, ensures that the systems being developed are secure
11. Systems Developer: Integrated Systems Development
12. Research and Innovation (Researcher)
13. Other: ...

D15. What are the main specialists of cybersecurity in your company or in the XCountry market in general you are lacking?

D16. In your opinion, how much attention is paid to the qualification of cyber security professionals in your organisation?

1. More than enough
2. Sufficient
3. Almost enough
4. Too little
5. Not allocated at all
6. Cannot answer

D17. Your suggestions/requests for the training of cyber security professionals (competences, responsibilities, roles, problems, etc.).

Thank you for your answers!

A.3.3. Respondentų pageidavimai KS specialistų rengimui

1. Praktinės patirties, pripažįstamų pasaulyje sertifikatams prilyginamų žinių.
2. Turėti nustatytą politiką bei strateginius planus pasiimti junior lygio specialistą ir ruošti pagal įmonėj reikalingą kryptį. Keliami per dideli reikalavimai samdant KS specialistus, t.y. aukšti lūkesčiai kompetencijoms, tačiau mažas atlyginimas.
3. Jei kalbame apie kibernetinio saugumo specialistą, kurie dirba labiau su technine puse - tokiu atveju apskritai trūksta specialistų su giliomis IT techninėmis žiniomis (tinklai, tinklo įrenginių specifikos, programavimo žinios, Linux OS, pažeidžiamumų paieškos proceso supratimas). Jei imame kibernetinio saugumo specialistą plačiąją prasme (pvz. kaip saugos architektą, CISO ar rizikų specialistą, DPO) - trūksta mokymų aukštesnio lygio specialistams (šiuo metu didžioji dalis orientuoti į pradedančiuosius). Lietuvoje trūksta/nėra informacijos/mokymų susijusių su industrija.
4. Rinkoje matomas didelis KS specialistų trūkumas, tad iš universitetų tikimasi, jog jie paruoš kuo daugiau bendrų KS žinių turinčių studentų, o įmonės vėliau galės juos profiliuoti detaliau bei suteikti specifines žinias. Viena iš didžiausių problemų, jog studentai nesidomi KS specifika, perspektyvomis ir eina lengviausiu, programuotojo ar projektų vadovo karjeros keliu.

A.4. Pusiau struktūrizuoti ekspertų interviu

Prieš interviu buvo paruošti pusiau strūktūrizuoto inteviu klausimai ekspertams:

1. Kas gi Tavo supratimu yra kibernetinio saugumo specialistas (*KSS*) (t.y. ką jis daro, ką jis moka daryti, t.y. kompetencijų klausimas)?
2. Kaip tokiu tapti? T.y. ką pasakyti jaunam (ir gal net ir nejaunam) žmogui, ir ką pasakyti universitetui/kolegijai, t.y. ką mokytis/mokinti. Koks yra teisingas kelias į KS sritį?
   Alternatyvios intervencijos:
   (a) Ką rinktis mokyklos abiturientui?
   (b) Ar įmanoma įsivaizduoti kibernetinį saugumą be IT žinių?
   (c) Ką siūlytum mokiniui - eiti į universitetą, ar iškart dirbti?
   (d) Ar samdote *junior* (red. pradedančiuosius) ir mokinate?
   (e) Kiek verti sertifikatai ir ar jie reikalingi?
   (f) Kiek reikalingas versle aukštasis išsilavinimas?
   (g) Koks yra požiūris į darbuotojo amžių?
   (h) Koks Tavo paties buvo/yra kelias?
   (i) Priklausomai nuo srities (technologijų ar valdymo) turbūt bus ir atitinkami keliai į jas. Ar IT žinios *governance* (red. strateginio vadovavimo) srityje privalomos?
   (j) Ką patartum mokiniui kelyje į *KS*?
   (k) Kas vertingiau - ar eiti studijuoti, ar iškart dirbti?
3. Įžvalgos apie rinką – ar tikrai trūksta KS specialistų? Nes atrodo, kad nėra daug darbo pasiūlymų, jei išanalizavus CVonline (ar LinkedIn... kiti).
4. Apskritai ar *soft skills* (red. „minkštosios" kompetencijos) labai svarbios? Ar iš LinkedIn galime susidaryti nuomonę apie trūkstamas pozicijas? Nes pozicijų su raktažodžiu *cyber* (red. kibernetinis) nėra tiek daug.

Žemiau pateiktų interviu kalba nėra taisyta.

A.4.1. Interviu nr. 1

Kas gi Tavo supratimu yra KSS (t.y. ką jis daro, ką jis moka daryti, t.y. kompetencijų klausimas)?

Jei specialistas, tai reiškia *senior* (red. vyriausiasis) žmogus, kuris jau daug žino. Priklauso nuo srities: gali būti tinklo specialistas, kuris prižiūri tinklo saugumą, tvarko ugniasienes; gali būti infrastruktūros saugumą užtikrinantis žmogus; gali būti vadybininkas politikos formuotojas, ypač jei aukštesnio rango įmonės vadovas; gali būti pažeidžiamumų testuotojas (pentester) - įvairių sistemų ar produktų. Daug šakų. Aš nesu *cyber security specas* (red. KSS), negaliu atsakyti, nes IT specialistas ir *cyber security* (red. KS) specialistas persidengia, nėra aiškios ribos tarp jų. Jeigu esi

savo srities IT specialistas, kuris suvokia apie kibernetines grėsmes ir taikai metodus jų prevencijai, tai automatiškai jau gali save vadinti ir *cyber security specu*.

2. Kaip tokiu tapti? T.y. ką pasakyti jaunam (ir gal net ir nejaunam) žmogui, ir ką pasakyti universitetui/kolegijai, t.y. ką mokytis/mokinti. Koks yra teisingas kelias į KS sritį?

Skaityti, žiūrėti, praktikuotis. Pradžiai reikia norėti. Nebijoti daug mokytis, domėtis ta sritimi. Jei esi bet kurioj IT srity geras *specas*, tai saugumo žinios ateis tarsi natūraliai. Pvz., galima rasti informaciją, kad *DB portas* (red. duomenų bazės prievadas) neturi būti pasiekiamas iš išorės. Tačiau bet kuris DB administratorius ir taip tą žino, jam tos žinios per patirtį atėjo. Jei toks nesi, tada turi daugiau skaityti ir aiškintis (kompensuoti patirties trūkumą).

Ką rinktis mokyklos abiturientui?

Kokioje 11 ar 12 klasėje jau žmogus turėtų būti pats pasidomėjęs ir turėti supratimą apie tai, kas jį labiau traukia. Kai studijavau KTU, tai buvo 4 sritys IT - tinklai, programavimas, grafika, geležis. Dabar jau žinau yra kažkokių kursų.

Ar įmanoma įsivaizduoti KS be IT žinių? Pvz., jei kalbame apie vadybą ar teisę?

Manau, kad net ir vadyboje dabar turėtų būti duodamas kažkoks supratimas apie IT ir saugumą, nes be to supratimo įmonių vadovai vėliau negali užtikrinti įmonės saugumo, kaip jau ne kartą yra nutikę Lietuvoje. O dėl IT studijų, tai galėtų būti programos, kuriose žmogus pasimokytų įvairių sričių (apie infrastruktūrą, programų kūrimą, tinklus), o tada nuspręstų, kad gilins KS žinias kažkurioje specializuotoje srityje. Galima aišku ir Udemy (nors ten daug prastų kursų, bet yra ir vertų) pasižiūrėjus susidaryti bent minimalų supratimą apie galimas sritis, pvz., įrangos tiekėjai (vendoriai) dažnai daro nemokamus kursus apie savo produktus, pvz., Fortigate. Taip gautum supratimą, ką reikia žinoti, kad galėtum valdyti tinklus ar formuoti jų saugumo politiką.

Ką siūlytum mokiniui - eiti į universitetą, ar iškart dirbti?

Šiais laikais, jei turi valios ir dvasios stiprybės, tai gali pats labai daug išmokti – internete pakanka informacijos ir kursų, nors tikrai būtų gerai, jei kas nors galėtų *paguidint'ų* (red. nurodytų kryptį ar mentroriautų). Nelabai dabar žinau, kur stoti, bet girdėjau, kad Vilnius Coding School dabar kažkokią saugumo programą siūlo.

Ar samdote *junior* (red. pradedančiuosius) ir mokinate?

Mes – ne. Ieškome jau mokančių, nes mokymams reikia skirti savus resursus, mes to nedarome. Teoriškai tada reiktų organizuoti kažkokią *cyber* akademiją, ir geriausius sau pasilikti. Didesnėse

> įmonėse aišku galima tą daryti, kai ant kaklo nekaba tas mokinys.
>
> > Kiek verti sertifikatai ir ar jie reikalingi?
>
> Labai jau skirtingų yra sertifikatai - jie viens kitam nelygu. Jei neturi diplomų ir patirties, tai bent jau sertifikatą parodyk. Aišku, neretai būna pirkimų reikalavimai įmonėms, kai būtina turėti tam tikrą kiekį sertifikuotų žmonių (dėl formalių reikalavimų).
>
> > Tai kiek reikalingas versle aukštasis išsilavinimas?
>
> Žinok, kuo toliau, tuo mažiau. Vis daugėja specializuotų kursų. Suprask - jie darosi svarbesni, nei diplomas.
>
> > Kaip dėl darbuotojo amžiaus?
>
> *Senior* specialistas tikrai nebus 20 ar 21 metų, lygiai kaip ir 50+ irgi dar retai būna. Nors daug žinių yra fundamentalios - nežiūrint į tai, kad viskas IT pastoviai keičiasi, tad su laiku vyresnių specialistų daugės. Dar keletas minčių apie savo augimą - tai sako, kad neretai mokosi kursuose (Udemy), po to išsilaiko egzaminą, gauna sertifikatą. Kai kuriose didelėse įmonėse sertifikatai savo CV yra svarbūs - padeda atsijoti tave nuo daugybės kitų konkurentų.
>
> > Ar diplomas yra svarbus?
>
> Lietuvoje gal taip, užsienyje manau mažiau. Kiek susiduriu su darbo skelbimais - tai arba reikia darbo patirties, arba sertifikato, arba abiejų, bet apie diplomus mažiau kalbos eina (kokioj septintoj vietoj, bet lietuviškas universiteto pavadinimas mažai ką reikš).

> 3. Įžvalgos apie rinką – ar tikrai trūksta KS specialistų? Nes atrodo, kad nėra daug darbo pasiūlymų, jei išanalizavus CVonline (ar LinkedIn... kiti).

> Tiesiog gerų specialistų trūksta visose srityse, ne vien *cyber*. IT sektorius vis auga, todėl ir trūksta. Per darbo skelbimus beveik neįmanoma surasti gerų specialistų, ypač jei neturi *HR* (red. žmogiškųjų išteklių) skyriaus, kuris būtent tuo *head-huntinimu* (red. "galvų medžioklė") išskirtinai užsiimtų, todėl mes ieškome per pažintis ir rekomendacijas. Todėl ir nėra tiek daug tų skelbimų, nes jie neveikia. Štai reikėjo gero *devops* (red. programinės įrangos kūrimo ir IT) specialisto, tai geri neaplikuoja. Aplikuoja tie, kurie per Google visus tavo skelbimo raktažodžius ir akronimus išsiaiškino (nors realiai neišmano).

A.4.2. Interviu nr. 2

1. Kas gi Tavo supratimu yra KSS (t.y. ką jis daro, ką jis moka daryti, t.y. kompetencijų klausimas)?

Kaip tik dabar darom atrankas į savo komandą ir ieškom 3 srityse: 1. *Cyber defence*, t.y. saugoti ir vartotojus, ir infrastruktūrą. 2. *Log management/SIEM* (red. saugumo informacija ir įvykių valdymas), 3. *Identity/access management* (red. tapatybės ir prieigos valdymas), kur turi žinoti oauth, octa ir t.t., nes neturim *active dir* (red. Microsoft Active Directory). Dauguma ateina tokie, kurie moka *next*, *next*, *installed* (red. kitas, kitas, diegti). Mes ieškom tokių, kurie gali paimti *open source* (red. atviro kodo) įrankius ir suintegruoti. Padaryti *identity aware proxy* (red. į tapatybę atsižvelgiantis tarpinis serveris) (yra panašūs pas Google). Labai mažai kas moka scriptinti ir programuoti, bent minimaliai, kad mokėtų skaityti kodą (bent daugmaž). Dauguma atsako, kad nemoka programuoti ir nelabai nori išmokti. Dabar nebepakanka tokių *adminų* (red. administratorių) kaip anksčiau, nes darosi infrastruktūra kaip kodas, arba keliasi viskas į *cloud'ą* (red. debesų kompiuteriją), kur viskas yra per *API* (red. programavimo sąsaja). Ko reikia *specui*, tai kad nebijotų mokytis - nereikia būti *developeriu*, bet programavimo įgūdžių jau reikia dabar ir ateity reikės vis daugiau. Nereikia gilaus koncentravimosi į kažkokią vieną sferą, bet reikia plačiai žinoti įvairių dalykų bazines žinias (protokolus, SQL kalbą ir pan.) ir mokėti susikurti savo įrankius. Pvz., yra didelis kelių šimtų *MB log* (red. žurnalas) failas po incidento ir jo su Notepad neatsidarysi. Reikia greitai ką nors išsitraukti iš jo, tai be paprastų komandinės eilutės žinių (grep, regexp) neišsiversi ir spręsti klausimą greitai, neperkant kokių brangių specializuotų įrankių. Kitas dalykas yra mokėti paklausti, t.y. *Soft skills*. Dauguma galvoja, kad jei aš *pentesteris* (red. pažeidžiamumų testuotojas) tai visą dieną praleisiu sistemas lauždamas, bet virš 60% laiko yra ataskaitų rašymas ir pristatymas *stakeholder'iams* (red. akcininkams/suinteresuotosioms šalims). Labai trūksta gebėjimo gerai parengti ataskaitą, paversti techninę kalbą į *biznio* (red. verslo) kalbą. Čia visiems aktualu, jei nori augti. Mūsų supratimu *incident response* (red. pagalbos teikimas po incidento) yra pirmas laiptelis, kur gesini gaisrus (pvz., nuo *phishingo* (red. informacijos rinkimo atakos)), čia ateina tie, kurie prieš tai yra dirbę sistemų administravime, pabūna *incident response* komandoje kokius metus, ir jei turi potencialo tampa *security engineer* (red. saugumo inžinierius), kuris jau diegia saugumo sistemas, nes turi supratimą apie incidentus. Bet net ir tam pirmam laiptelyje, kad būtum geras *incident responderis*, turi turėti *soft skills* - tarkim trūksta tinklo *logų*, turi juos išprašyti iš *tinklisto* (red. kompiuterinio tinklo administratorius). Jei esi inžinierius ir diegi *SIEMą*, kur nori rinkti visų sistemų *logus* - tai reikia eiti ir bendrauti su visom komandom (net ir programuotojais), kad jie suteiktų prieigą. Vienas pats nieko nepadaryti. Ko trūksta, tai mokėjimo dirbti komandoje. Yra tokių, kurie užsidarę dirba, bet *security* reikalauja bendradarbiavimo. Kitas pavyzdys: *SRE (software reliability engineer* (red. programinės įrangos patikimumo inžinierius)) rūpinasi daugiausia *availability* (red. prieinamumu), kad sistemos veiktų, o *confidentiality* (red. konfindecialumas) yra tik *"nice to have"* (red. privalumas), tad mes (*security*) turime rūpintis, kad gautume *logus*. Turime susitarti su programuotojais, kad jie įmontuotų *loginimą*, o *SRE* juos atiduotų. Visą laiką turime derėtis su visom komandom, turim paaiškinti kokią naudą jie gaus

ir kad nenukentės. Pvz., *EDR (end point detection and response* (red. kenkėjiškos programinės įrangos aptikimo ir reagavimo įrankių)) diegimo visi bijo, nes pakenks sistemos *performance'ui* (red. našumui), sulėtins kompus (red. kompiuterius). Pamatuoji, gauni 5% *CPU impact* (red. poveikis), išaiškini naudas kaip koks pardavėjas, ir tada jie patys susidiegia. Skaičiau knygą *"Building modern security policy"* (red. "Šiuolaikinės saugumo politikos kūrimas") - mintis yra *scalint'is* (red. augti) kitų komandų rankomis, nes *security* yra visos įmonės reikalas. Tad reikia pastoviai komunikuoti, kelti *awareness* (red. suvokimą), kad saugumas priklauso nuo mūsų visų. Rašinėju dažnai kitom komandom tokius "bits and bytes" (red. trumpus patarimus), pvz., "naudokitės *password manageriais* (red. slaptažodžių tvarkyklėmis)" ir pan. Nes pradžioj įmonės darbuotojų supratimas yra toks, kad va yra *security* žmogus, jis visą saugumą ir padarys.

> Kokios tavo pareigybės?

Security engineer. Bet kaip sakau, nepakanka vien techninių žinių, reikia ir *soft*. Nebūsi kaip tikras pardavėjas, kuris *story tellingu* (red. istorijų pasakojimu) ištisai užsiiminėja, bet visą laiką reikia stengtis ir ta kryptimi judėti. Turiu ant stalo *"how to make friends and influence people"* (red. "Kaip susirasti draugų ir daryti įtaką žmonėms"), nes yra daug dalykų, kuriuos gali padaryti minkštais būdais. Jei ateisi ir pasakysi kaip kirviu, kad turime kažkokią saugumo sistemą dabar visiems įdiegti, tai iškart bus atstūmimo reakcija. Turi prieš tai pagrįsti poreikį ir išaiškinti naudą. Pvz., iš pradžių dariau saugos auditą, tada švelniai ėjau su rekomendacijomis, kaip jie galėtų pataisyti savo produktus, tai priėmė labai teigiamai. Galėjau vietoj to piktai pareikšti, kokias jie klaidas daro, tai nieko būčiau nepešęs. Dabar kaip tik mėginu per Kubernetes konteinerius vieną saugumo sprendimą diegti - tai iš pradžių darau *proof of concept* (red. koncepcijos įrodymą), pats testuoju, tada einu pas *SRE* - bet jis paims tik jeigu aš išsiaiškinsiu kokius įrankius naudoti, kokias komandinės eilutės komandas, kad jiems nebūtų daug papildomo darbo. Ir tada jau jie įdiegs, t.y. padarysiu jų rankomis, jeigu gerai pateiksiu.

> 2. Kaip tokiu tapti? T.y. ką pasakyti jaunam (ir gal net ir nejaunam) žmogui, ir ką pasakyti universitetui/kolegijai, t.y. ką mokytis/mokinti. Koks yra teisingas kelias į KS sritį?

Mokykloj per karjeros dienas taip aiškinau: nueiti į Github, susirandi patinkantį produktą, randi jų problemas (*issues*) ir bandai prisidėti pataisyti tą problemą – mokaisi programavimo ir *kolaboravimo* (red. bendradarbiavimo), ir tai tau nieko nekainuoja. Kitas dalykas - dalyvauti visuomeninėje veikloje, pvz., nepelno siekiančiai organizacijai sukurti *web* (red. žiniatinklio) puslapį (yra feisbuke (red. "Facebook") web profesionalų grupė, kur dažnai ieško tokių). Tam mokyklinukui ar studentui bus jau realus įrašas į CV apie realią patirtį (kad ir šleivai padarytą). Rodo, kad darei, komunikavai su kitais, valdei laiką ir pasiekei rezultatą. Baigus studijas - pirmas dalykas susitvarkyti CV ir LinkedIn, nes darbdaviai labai žiūri. Jei gauni įsidarbindamas namų darbą, tai padaryk gerai.

Nusimesk aroganciją. Dažnai pastato save ant pjedestalo, nors nežiba žiniomis, reiktų šiek tiek save ant žemės pastatyti. Ir jei eini į *security*, tai visą laiką turėsi mokytis. Vieną įrankį išmokęs negalėsi ilgai su juo sėdėti. Dabar visiems reikia Kubernetes *devops*'ų ir *dev-sec-opsų*, bet neaišku kas kitas bus populiarus po kelių metų. Turi būti *jack of all trades, master of none* (red. visų amatų žinovas, nė vieno iš jų meistras). Arba: *inch deep, mile wide* (red. colio gylio, mylios pločio) (apie žinias). Tiems kandidatams, kurių iškart nepakviečiam, duodu 5 knygų sąrašą:

1. Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd Edition, 2021,
2. Michal Zalewski, The Tangled Web: A Guide to Securing Modern Web Applications, 2011,
3. Evi Nemeth, Garth Snyder, Trent Hein, Ben Whaley, Dan Mackin, UNIX and Linux System Administration Handbook, 2017,
4. Thomas Limoncelli, Christina Hogan, Strata Chalup, Practice of System and Network Administration, The: Volume 1: DevOps and other Best Practices for Enterprise IT, 2017,
5. Thomas Limoncelli, Practice of Cloud System Administration, The: Designing and Operating Large Distributed Systems, Volume 2: DevOps and SRE Practices for Web Services, Volume 2, 2014

Ir buvo atvejis, kai per pusę metų žmogus iš esmės pasikeitė ir vėl atėjo - panašu, kad mes jį priimsime.

> Kaip dėl bakalauro/magistro?

Naudos duos, nes savamokslis gal ir turės techninių žinių, bet neturės bendro išprusimo. Vėliau aišku reikės pačiam mokytis. Informacijos daug, reikia atsirinkti ką mokytis. Visi nori būti *pentester*'iais ir *red-team*'eriais, bet nesupranta, kad 60-70% laiko rašys ataskaitas ir sistemose nebus tiek pažeidžiamumų, kiek mato žaisdami Hackthebox.

> 3. Įžvalgos apie rinką – ar tikrai trūksta KS specialistų? Nes atrodo, kad nėra daug darbo pasiūlymų, jei išanalizavus CVonline (ar LinkedIn... kiti).

Natūralu, kad *senior* nėra tiek daug. Iš *junior* problema ta, kad kažkas turi auginti. Kaip minėjau, vienam daviau literatūros ir jis per pusmetį pats patobulėjo, tai tokie labai faini. O viduje iš pradžių žmogus keliauja į *incident response* - jis nemato viso vaizdo, nes yra daug komandų (*tinklistai*, programuotojai), jis turi išmokti greitai gauti informaciją iš kitų komandų, t.y. komunikacija ir turi išmokti iš kur pasiimti informacijos (pvz., neturi prieigos prie sistemų, bet gali išprašyti, kad *log*'us atsiųstų), turi išmokti valdyti laiką, pvz., kas 15 min teikti (net ir nepilną) info, kad kitos komandos galėtų atitinkamai judėti į priekį. Jei tiems žmonėms dega akys, tai su laiku duodi jiems projektuoti kokią (*cybersec*) sistemą.

> Sertifikatai aktualūs?

Taip. Man pačiam - jie nurodo labai aiškų tikslą, be jo mokytis nėra taip įdomu. Yra sertifikatai kaip Offensive Security ar RedHat, kur turi praktiškai ką nors padaryti per egzaminą, ir yra testai, kaip CEH, CISP. Tai visi yra *cool* (red. šaunu), rodo žmogaus motyvaciją, parodo, kad *basic* (red. pagrindinę) info jau žino. Žodžiu, *nice to have*.

> Ar CV online ir LinkedIn rodo vaizdą, kiek žmonių ieško?

Mačiau statistiką, kad JAV į 7 darbo pozicijas yra 1 pretendentas. Dabar gal dar blogiau. Todėl ir daro visokius renginius, kad daugiau jaunimo pritrauktų, pvz., CTF, didina jų premijas, kad būtų dėmesys didesnis. PawnToOwn - jei įveiki, gauni tą daiktą.

> Bet Lietuvoje įmonės ieško gana nedaug, ar ne?

Sakyčiau, kad anksčiau ieškojo mažiau. Po visokių CityBee skandalų vis daugiau susivokia, kad mums reikia kokio saugos įgaliotinio. Vieni ieško dėl *compliance* (red. reikalo), dėl popierinio lygio. Kiti jau realių sprendimų ieško. Ir yra trečia kategorija, kuri jau labai nori gerai susitvarkyti viską. Viena įmonė pasamdė CISO, kuris po to buvo mane pasiėmęs, kad techniškai jo planus įgyvendinčiau.

> Ar nuo įmonės dydžio priklauso?

Taip. Koks bankas ims dėl *compliance* (PCI DSS) jiems tikrai reikia saugos įgaliotinio, *startup*'ui (red. pradedančiąjai įmonei) ar mažai įmonei viskas per brangu, o vidutinė - jei mąsto, tai ims *hands-on* (red. praktinį) žmogų. Bendrai paėmus, tai kai darom atrankas, tai liūdnas vaizdas su pretendentais.

> O kiek atrenkate?

Pradžioj *HR* pagal CV filtruoja, tada pokalbis su mumis apie *tech* (red. technines) žinias, jei *ok* (red. gerai) tai duodam namų darbą - nelimituojam laiko. Pvz., iš pcap turi nustatyti kas įvyko, tada iš *log*'o gabalo nustatyti kas vyko, tada *mail transfer log*'as XML'u (red. pašto perdavimo žurnalas XML formatu), kurį turi savo norima kalba pasirašęs *script*'ą *išparsinti* (red. apdoroti) į json, ir atlikti analizę, gauna ten URL, ten randa PHP scriptą, kurį turi *reverse engineer*'inti (red. pasitelkti atvirkštinę inžineriją), kad suprastų ką darė. Padaro aprašymą, jei *ok*, tada kviečiam aptarimui. Būna tokių, kur kažkas kitas už juos darbus padaręs. Pats žiniom nespindi, o aprašymas žiba. Jei praeina, tada dviem dienom kviečiame į *try-out* (red. bandomąjį laikotarpį), t.y. žiūrim *culture-fit* (red. kultūrinį tinkamumą, kai darbuotojas sugeba prisitaikyti prie darbovietės vertybių ir kolektyvo). Po tų dviejų dienų turi pristatyti kažkokios duotos problemos sprendimą, t.y. žiūrim

kaip rinko informaciją iš kolegų, ir kaip tinkame viens kitam. Buvo atvejis, kai lyg viskas *ok*, bet netiko per *try-out*, nes sprendimus siūlė, bet negalėjo paaiškinti argumentuotai, kaip juos mėgintų diegti. Reiktų ilgai jį dar mokyti. Yra nemažai žmonių, kurie net ir ilgai dirbdami *security* savo žiniomis nespindi. Kurie neprisitaiko, ir vis dar nori daryti *next-next*, tai liks paraštėse.

Kaip dėl amžiaus?

Dauguma iki 30. Yra virš 40, bet jie lėtesni. Man jauni tuo patinka, kad turi daugiau lankstumo, nebijo "šauti" – kad ir ne visada pataiko. Tie, kurie daugiau gyvenimo matę, nori ramiai.

A.4.3. Interviu nr. 3

1. Kas gi Tavo supratimu yra KSS (t.y. ką jis daro, ką jis moka daryti, t.y. kompetencijų klausimas)?

KS bendrai klausiant yra per platus terminas, priklauso nuo srities. Jei nuo aukštai žiūrėtume, tai galima skirstyti į dvi grupes: procesai ir procedūros (*governance*) ir techninė sritis (inžinerija). Bent pas mus taip yra. Galima aišku žiūrėti į įvairius *framework*'us (red. karkasus).

Pas mus inžinerija tada skaldosi į: infrastruktūrą; prieigos valdymą (*access management*); incidentų valdymą (*incident response*) - nors čia nebūtinai vien tik į inžinerijos pogrupį patenka; *pentester*'iai/*RedTeam*'eriai. Ne visos šios sritys yra griežtai inžinerija, bet jos labiau techninės.

Procesų srityje gali būti lygiai tos pačios rolės, bet jau iš valdymo (*governance*) pusės. Pvz., pažeidžiamumų valdyme (*vulnerability management*) techninis žmogus gali skenuoti sistemas, rinkti informaciją apie IT resursus (*IT assets*), bet jam reikalingas vadovas, kuris šiuos veiksmus koordinuotų. Kiekvienoj minėtoj srity gali rasti dublerį, kurie prižiūri iš labai skirtingų pusių - vieni iš procesų pusės, kiti "*hands-on*". Kalbant apie šias roles – ar yra kažkokia universali jų sistema, ar priklauso nuo įmonės? Priklauso nuo įmonės, bet anksčiau ar vėliau atsiremsi į bendras gerąsias praktikas (koks nors ISF ar CISO *security controls* (red. saugumo kontrolė)), ar ką diktuoja reguliatoriai. [kiti standartai: SOGP 2000; NIST Cybersecurity framework; CIS top 20 security controls; PCI DSS; ISO/IEC 27002:2013; COBIT 5 for information securty]. Kokią metodologiją paimsi, yra specifika, bet visos jos turi bendrus taškus. Svarbu suprasti, ką nors apsaugoti. Jei įmonė *on-prem* (red. vietoje), tai specialistai visai kitaip dirbs, nei su *cloud* sistemomis, bet principai panašūs.

2. Priklausomai nuo srities (*tech* ar *governance*) turbūt bus ir atitinkami keliai į jas. Ar IT žinios *governance* srityje privalomos?

Privalomos ne, tačiau labai praverčia. Paprastai šnekant, kad tau IT specialistai "neprikabintų makaronų". Turi su jais sugebėti susišnekėti. Tu nebūtinai turi būti žmogus, kuris tą daro pastoviai, bet turi suprasti, kaip tai yra daroma. Panašiai kaip statybose - architektas betono nelieja, bet turi suprasti kaip tas daroma ir koks jo atsparumas.

> Ką patartum moksleiviui kelyje į *KS*?

Sėkmės. Vienas kelias – išmokt programuoti. Kitas - diegti sistemas. Trečias - atlikti sistemų analizę, nors tam jau tiesa reikia išmokt programuot ar pan.

> Ar eiti studijuoti, ar iškart dirbti?

Universitetas yra gerai, nes pateiks platesnę žinių paletę, nei bet kokia įmonė - gausi nuo programavimo pagrindų iki projektų valdymo, o įmonėje kur pasodins, ten ir sėdėsi. Gerai yra derinti ir nuo kažkelinto kurso pradėti dirbti, kad gautum ir kažkokią praktiką. Universitetas pateiks plačiai, bet negiliai; įmonė - giliau.

> O kaip sertifikatai?

Pradžioj – labai gerai, nes pasako tiksliai, ką tu žinai. Aišku, sertifikatų yra visokių.

> 3. Įžvalgos apie rinką – ar tikrai trūksta KS specialistų? Nes atrodo, kad nėra daug darbo pasiūlymų, jei išanalizavus CVonline (ar LinkedIn... kiti).

Jaunesniųjų specialistų (*junior*) trūksta mažiau, norinčių į tokias pozicijas yra. Ko labiausiai trūksta, tai patyrusių specialistų. Bet panašiai kaip visur. Aišku, talentų rinkinukas *cyber sec*'e yra siauresnis, nei kitur. Tarkim, bendrai paėmus programuotojų specialistų yra gerokai daugiau. Kaip pasidarai *cyber specu*? Priklauso nuo to, kas tam žmogui įdomu. Yra pozicijų, kur tiesiog darbovietėje jis pastatomas į tam tikrą poziciją ir ten jį išmoko. Bet yra kitokių atvejų. Tarkim, daug kas mėgsta “hakinimą”, krapštosi toje srityje, mėgina rasti spragas, tai natūraliai ir nukeliauja į tą sritį. Bet žmonės įvairūs, kai kuriems mokykloje daugiau patinka matematika, o kitiems kalbos.

> O ar yra perspektyva *KS* tiems, kurie į kalbas linkę?

Manau, kad taip. Jie labiau galėtų į procesų roles eiti. Nors tai klausimas, kuris išlenda iš *cyber sec* rėmų: surask, kur esi stiprus, o jau po to atsiskleis, ar čia *cyber sec* tinka, ar ne. Man buvo jau 10 klasėj aišku, ko noriu. Stojau į informatiką KTU. Po to jau yra profiliavimas, bet manau, kad reikia žiūrėti į išvardintas sritis ir žiūrėti, ką žmogus gali padengti. Tarkim, moterys yra kruopštesnės ir tarsi tiktų procesus valdyti. Bet jeigu nesuprasi srities, bus vistiek sunku. Nereiškia, kad moteris

turi būti sistemų administratore, bet kažkokius kursus galėtų apie tai išklausyti. Tokia sritis, kaip *awareness* (darbuotojų lygio kėlimas) atrodo itin tinkama sritis moterims.

> Kaip bendrai, ar *soft skills* labai svarbūs?

Dažniausiai *geek*'ai (red. moksliukai) turės vadovą, kuris "moka kalbėti", bet jokia grupė nėra visiškai izoliuota nuo kitų.

> Ar iš LinkedIn galime susidaryti nuomonę apie trūkstamas pozicijas? Nes pozicijų su žodžiu *cyber* nėra tiek daug.

Taip. Tačiau tos pozicijos aktualios didelioms įmonėms. *Awareness* žmogaus maža įmonė tikrai neturės. Bet *pentester*'is jau gali būti ir mažesnėje, tik nebūtinai taip bus pavadintas, gali būti QA (*quality assurance*) ar testuotojas. Laikyčiausi pozicijos, kad *cyber sec* neturėtų būti centralizuota vieno žmogaus funkcija, ji turi būti visų darbuotojų galvoje. Žinoma, yra specifinių technologijų, *threat hunter* (red. pavojų medžiotojas), *security engineer*, *incident response* yra išskirtinės pozicijos (kur SOC užsiima). Reguliuojamose įmonėse ir mažesnėse privalo būti tarkim informacinės saugos vadovas, pagal įstatymą. Jis, pvz., turi sudaryti (saugumo) planą, bet eigoje gali pamatyti poreikį ir kokiam inžinieriui.

> Ar Jūs savo įmonėje mėginate auginti specialistus?

Paprastai ieškom *specų*. Kai jau turi kelis *specus*, jau gali imti ir *junior*. Bet pirmiausiai reikia specialisto, negali būti vien vadovas, reikia ir *hands-on* žmonių. Mes *incident response* traktuojam kaip pradinę poziciją, ten žmogus su incidentais susipažįsta, kaip į juos reaguot, plečia žinias, pamažu pereina į inžinierius. Kitas dalykas - reikia žmonių, kurie užtikrintų *compliance* (red. reikalavimų atitikimą), kurie prižiūrėtų *vendor*'ius (red. tiekėjus), praeit ir patikrint, koordinuoti. Ten galėtų ir teisininkas atsirasti, su šiek tiek IT žinių. Atitinkamai ir *privacy* - įdomi ir labai svarbi sritis.

> Ar informacijos saugumas yra KS?

Nesiginčysiu dėl terminų. *Privacy* – yra su info sauga susiję, tik tikslas kiek kitas. Kaip ir su sauga, tie patys principai: CIA. Informacijos saugumo tikslas - apsaugoti įmonės interesus, o *privacy* tikslas – apsaugoti asmenų interesus, kad įmonė nepiktnaudžiautų. Principai panašūs, tik tikslas kiek skiriasi. Manau tai karšta tema, nes specialistų reikės daug, reguliavimas vienas griežčiausių, niekur nedingsi.

> Kiek laiko reikia kol tapsi KSS?

Amžius tiksliai to nepasako - vienas nuo 12 metų pradės, kitas vėliau, vienas mokysis ir laisvalaikiu,

kitas ne.

> Ar turi būti jaunas, kad būtum lankstus ir tiktum KS?

Labai priklauso nuo asmenybės. Pagal pasiskirstymą vyresnio amžiaus specų yra daugiau, nei jaunų. Prieš 10 metų GDPR nebuvo, tad po 10 metų tikrai bus daugiau specialistų. Nes ir poreikiai jau kiti, tarkim *DB admin*'ui jau reikia atsižvelgti į GDPR, nes jei duomenų netrinsi, gręsia bauda. Programuotojas sakys - negaliu. Tad atsiranda poreikis tarpininkams, kurie susišnekės su abiem. Tad su laiku daugės ir vyresnių, ir šiaip daugės. Nes *cyber specų* nėra daug, tad jų algos didesnės, nei tarkim analogiškos patirties programuotojų. O laikui bėgant įmonėse specialistai arba pereina į vadovaujančias pareigas, arba lieka tais vyresniaisiais, kurie sugeba susišnekėti su specialistais ir su vadovybe.

Kai padarysite analizę, parodykite, duokite paskaityti (pakritikuoti).

> Būtinai!

A.4.4. Interviu nr. 4

> 1. Kas Tavo manymu yra kibernetinio saugumo specialistas Lietuvoje?

Iš pirmo žvilgsnio – bet kas, kas susijęs su IT (mokslas/darbas/abu-jei idealiu atveju) - nes užtikrina *availability*. Kuo *cyber* skiriasi nuo "pliko" IT: *compliance* - auditai, konsultacijos; techninis saugumas (*pentester*, *vulnerab analyst*, SOC specialistas, kuris stebi pažeidžiamumus, bet kur baigiasi *admin*/kur prasideda *security*? Nes jei žmogus prižiūri MS Exchange ar Azure platformą, tai tuo pačiu rūpinasi ir jų saugumu, bet paprastai nesivadina *cyber sec* specialistu. Siūlo skirstyti į 4 tipus:

1. IT specialistai, kurie tuo pačiu ir saugumu rūpinasi - čia patenka daugelis Lietuvos specialistų.
2. Analitikai (*analyst*), pvz., Pažeidžiamumų analitikai, SOC specialistai; dar gali būti žmonės, kurie rūpinasi *quality assurance*.
3. Gilių techninių žinių specialistai, pvz., *pentester*'iai, *secure coding reviewers* (red. saugaus kodavimo recenzentai), Azure *security specialists*, Fortigate, AWS, tinklų *security* (tam reikia jau didelės įmonės, tokių gal 10 Lietuvoje, kur atskiras žmogus būtų; dažniausiai būna vienas *tinklistas*, kuris viskuo rūpinasi, o ne atskirai *security*, t.y. Patenka į 1. skiltį)
4. *Consultancy*, GDPR, sertifikavimas, auditas, ISO-27001/2, COBIT; taip pat čia eitų *compliance*, t.y. CISO - pats nėra labai techninis *specas*, bet supranta tą.

Kitaip paversta mintis: jei užsiimi IT, ir dar mėgsti "hakinti", tai pirmas laiptelis yra būti analistu, o tada jei patinka kokia sudėtingesnė techninė sritis - eiti į *pentester*'ius; o jeigu norisi mažiau gilintis į siaurą techninę sritį, gali eiti į labiau "*soft*" sritį – consultancy (red. konsultacijos

sritį).

Kaip dėl teisininkų? Atitiktis teisiniams reikalavimams reikalingas dalykas, bet ar tą galime vadinti *security*?

Pvz., CISO dar turi eiti prie *compliance* - *ownership*'ą *security* (red. saugumo valdymą) turi kažkas imti, tai tam CISO atsiranda (jis yra saugos vadovas - detaliai nežino techninės srities, bet žino, ko reikia laikytis); jam patinka vadyba, organizavimas ir sauga (dažniausiai baigia IT studijas, bet nenori dirbti techninio darbo).

2. Kokias jis turi turėti kompetencijas/gebėjimus?

Gatavi labai brangūs; stengiamės auginti; stengiamės imti arba techninį žmogų: *technical* arba *consultancy*; paskutinių metų studentą arba ką tik baigusį. Svarbiausia žmogaus požiūris ir žmogaus noras mokytis, jie turi *basic*'us (firewall, ..., it) - iš tokio analistas geras, *pentester*'is išauga; *pentester*'ius pervilioja (jei būtų jau paruoštų, tai imtų, bet neparuošia kol kas niekas), atsiremiama į žmogaus norą mokytis (IT bakalauras, nori mokytis, *hacker*'io perspektyva); mokina per platformas: Udemy Pluralsight career path, ko trūksta - *windows*'istui (red. žmogui, kuris naudoja Windows operacinę sistemą) duoda linux ir tinklus, o tada specialius mokymus, kurių nemažai, kad pasimokytų (turi *subscriptions* (red. prenumeratas)), tuo pačiu duoda realius darbus, pvz., konfigūruoti įrangą klientams ar koordinuoti pažeidžiamumų valdymą (Qualys); konsultanto keliui - darbo su kliento patirtimi, nebijo eiti šnekėti, *security* išmokyti gali beveik visus, o ne laisvo bendravimo su klientais; vyresnius samdo, bet dažnai nudegęs, nes jie sako noro mokytis yra, bet realiai nebūna - čia jei virš 50 metų. Tie, kur virš 30 metų paprastai nori didelės algos, tad dauguma darbuotojų iki 30 metų. (Amžius šiaip nesvarbu, apmokysime per metus mokėdami apie 1,5 tūkst. - paskui 2 tūkst., *pentester*'is 2.5 tūkst.- 3 tūkst., konsultantas 3 tūkst.- 3.5 tūkst. į rankas). Sėkmingiausi skiria ir savo asmeninio laiko; įmonė finansuoja kursus, jei nėra ciongo - kišk nekišęs; konsultanto kelyje pradžioje daro mažas užduotis, auditui, skaito ataskaitas, augimo kelias, žmonės su patirtimi gali jungtis į auditą iš karto.

Kiek Jūsų įmonė dabar ieškotų žmonių?

Lietuvoje: 2-3 žmones. Įmonės mastu (tarptautinė įmonė, 80 darbuotojų per visą Europą) 20 "mokinių" priimtų per visas šalis (Italija, UK, Airija, Ukraina).

Kaip įvertini norą mokytis?

Šneki, tada bandomasis laikotarpis - apie pusė praeina jį sėkmingai.

O kaip klausimai apie specialistų ruošimą?

Pvz., CISO - geriau kad būtų ne vadyba, o IT magistras su vadybos kažkiek žinių. Jei būtų *security*+vadyba - išvis būtų gerai. Jei ruošti žmones nuo pradžių, bakalauro studijose, tai geriau tegu visko pačiupinėja, jam reikia duoti visko plačiai, tinklas, serveriai, *cloud*, *docker*'iai, kaip daiktus valdyti, kad suprastų administravimą, tada jau galima galvoti apie *security*. T.y. *security* turėtų būti bet kurios medžiagos paskutinė dalis. Pvz., išmoksti Exchange administruoti, o tada pažiūri į tai per *security* prizmę. Plačiau pačiupinėjus, vadybos principus išmokus, tada supras kur širdis linksta: ar *technical security* ar *management of security* (red. saugomo valdymas).

3. Ar ieškote darbuotojų? Kokių? Kaip sekasi? Kokiais kanalais? Ar CVonline/LinkedIn atitinka realybę (t.y. Kiek procentų darbdavių ieško per tas sistemas)?

Linkedin labiausiai tinka, Lietuvoje dažnai ir CVonline. HR atrenka, daro *personality* testus, peržiūri pagal technines žinias, vertybės turi atitikti, *manager*'io interviu. *Technical knowledge* (red. Techninių žinių) studentas gali neturėti, bet ne *senior* pozicijai. *Senior* pozicijos darbuotojų medžioja iš kitų įmonių. Dėl auditorių - su iso daug kas dirbo, tai iš tokio kito tipo auditorių išauginame (PCI DSS - apmokėjimo kortelių).

Moterys: CISO ir auditorius - tikrai moterys gali ateiti, iš 30 - 2 yra; trūksta drąsos, techninių žinių, galvoja, kad baigė programavimą, bet bijo kad gal *security* nežino, dažniausiai ateina iš IT; kai įtraukiame *legal* tada daugiau bus teisininkių; pačios nesigilina į *tech* saugą; gal dėl to, kad toks yra įvaizdis, kad *hacker*'iai sėdi naktimis rūsyje iki 5 ryto, tai tada netechninę saugumo sritį galima lengviau "parduoti", rūsyje sėdėti nereikia. Reikia moterims saugos pagrindų, vadybos pagrindų, technologijų pagrindų, kad *firewall*'o neišsigąstų, kad galėtų skaityti ataskaitas (saugos vadyba - padengia, kad bus žinių ir apie ugniasienes); *governance of security*.

4. Papasakokite apie Jūsų įmonės specifiką.

Mažoje įmonėje žmogus viską daro, o dabar populiarėja CISO *as a service*. Ne Lietuvos kapitalas lemia, bet įmonės dydis lemia – nuo 100 žmonių jau supranta rizikas, kad skaudės, jeigu pames duomenis. Vadovai turi matyti objektyviau, pastebėti ir *security* rizikas, juk net ir lentpjūvės robotai gali būti pažeidžiami. Garsios istorijos Lietuvoje pakelia kibernetinio saugumo supratimo brandą – plastinė chirurgija, Citybee, jei kažką į užsienį eksportuoja, tada klientai užsienyje dažnai reikalauja laikytis standartų – nes užsienio įmonės (kaip taisyklė – didelės ar vidutinės) tokiu būdu valdo savo rizikas. Kitoms įmonėms Lietuvoje labai priklauso nuo vadovo brandos ir požiūrio.

A.4.5. Interviu nr. 5

PASTABA: Šis interviu nebuvo įrašinėjamas, nes taip pageidavo jo dalyvis, todėl pateikiami perfrazuoti ir sutrumpinti atsakymai.

Ar trūksta Lietuvoje kibernetinio saugumo specialistų (KSS)?

Specialistų visada trūksta. Jaunų pasiūla šiek tiek dar yra, patyrusių – labai maža.

Su jaunais taip: nors ir gana daug tokių CV gauname (t.y. apie 10), bet patirties tarp jų tikrai mažai. Bet blogiausia, kad ir užsispyrimo mažai. Kai daviau dviems dienoms namų darbą (panarplioti techninę užduotį), tai du iškart atkrito (atseit gavo kitą darbo pasiūlymą – bet per vieną dieną mažai tikėtina, kad gavo pasiūlymą, kuris jau garantuotas).

Jei reikia pačiam užsiauginti *KSS*, tai lengviausia iš IT administratorių, geriausia iš tinklo *admin*'ų.

Ar trūksta kibernetinio saugumo specialistų?

Reikėtų pakeisti klausimą ir pasakyti, kad specialistų trūksta nedaug, tačiau labiausiai trūksta specialistų už gerą kainos ir kokybės santykį.

Ir trūksta būtent techninių, o ne vadybinių specialistų, kurie gebėtų remdamiesi kompanijos saugumo politika atitinkamai pakeisti sistemų parametrus (*config*'us). Panašiai kaip ir programuotojų atveju - jų netrūksta, bet trūksta gerų. Patikslinčiau, kad mielai įdarbinčiau (į "*junior*" poziciją) ir žmones be didelės patirties ir be jokio diplomo, jeigu žmonės būtų motyvuoti, tinkamo nusiteikimo, kurie nuoširdžiai domėtųsi ta sritimi. Mėginimai testuoti technologijas savo namų laboratorijoje būtų vertesnis dalykas, nei universitetinis diplomas. Tiesa, įmonių skausmas visada susijęs su tuo, kad apmokyti jauni specialistai lengvai perperkami į kitas įmones.

Daug *KSS* yra susišlavę taip vadinami "centrai", t.y. didelės užsienio įmonės, kaip kad buvo Barclays, ar dabar yra Danske, SwedBank skyriai. Juose atlygis kiek didesnis, tačiau darbas nuobodesnis – labiau mechaninis. Bet galima įžiūrėti tokių centrų pliusą, kadangi žmonės įgyja patirties su sistemomis, kurios Lietuvoje gali būti retos (dėl to, kad mažai didelių įmonių). Ekspertas tikisi, kad su laiku tie žmonės su siaura, bet gilia patirtimi galės jungtis į *startup*'us ir kurti produktus užsieniui, tada bus nauda. Tie centrai susirinko talentus iš Lietuvos verslo, o verslas tada savo ruožtu susirinko iš valstybinių įmonių, tad jei ieškoti *KSS* trūkumo, tai jis tikrai lengviausiai būtų pastebimas valstybiniame sektoriuje. Teigia, kad tie centrai Lietuvoje laikosi ne tiek dėl didelio mūsų *KSS* žinių bagažo, kiek dėl santykinai mažų algų, tačiau algos kyla ir tikėtina, kad neužilgo tie centrai bėgs iš Lietuvos. Tada yra tikimybė, kad bus tam tikras šokas *KSS* rinkai Lietuvoje - bus kurį laiką perteklius. Tuo pačiu InfoBalt įmonės šiuo metu vykdo lobizmą, kad joms leistų įdarbinti skurdesnių šalių specialistus – iš Baltarusijos, Ukrainos. Tai numuštų KSS algas, padidintų konkurenciją tarp jų.

Ar sutiktumete su teiginiu, kad per CVonline, LinkedIn daugiau ieškoma vadybininkų KS srityje, o ne techninių specialistų.

Iš dalies. Bet pats per CV banką negavau nei vienos paraiškos, tik per LinkedIn, tad organizacijos galbūt specialistų ieško per vidinius savo kanalus (pvz., uždarą Cyberthreat Google grupę), o ne per CV bankus. *Head hunter*'iams nesiseka rasti tinkamų *KSS*. Kalbant apie LinkedIn, tai gavome 90% paraiškų iš trečių šalių, nes skelbimas matomas visame pasaulyje, nors regionas ir nurodytas (t.y. Ieškoma tik Baltijos šalyse). Beje, ieškojome trijose šalyse, bet Latvijoje surasti *KSS* dar sunkiau, nei Lietuvoje.

O kaip klausimai apie specialistų ruošimą?

Lietuvoje dar vyrauja žmogaus-orkestro modelis, kai įmonė turi sistemų administratorių, kuris tuo pačiu atsako ir už *KS*. Nemanau, kad tai geras principas, bet suprantu, kad tai yra pagrįsta lėšų taupymu - tik didelės įmonės gali leisti sau specializuotus *KSS*.

Ateityje reikės daug informacinio saugumo specialistų (dėl BDAR). CityBee atvejis aktyvavo įmonių auditus ir rūpestį šiuo klausimu, nors valstybė kol kas per daug rūpinasi vartotojų sutikimais visokiuose naujienlaiškiuose, o ne realių asmens duomenų apsaugos klausimais. Tikiu, kad ateityje įsigalios ir kitas EU reglamentas NIS (*Network Infrastructure and Security*), kuris šiuo metu taikomas tik kritinei infrastruktūrai, ir tada prireiks daugiau ir *KSS*.

Kas, tavo manymu, turėtų ugdyti daugiau? Universitetai ar kolegijos?

Kolegijos, nes jos galėtų greičiau ir tikslingiau tą padaryti, suteikti daugiau praktinių įgūdžių. Bet svarbiausia visgi, kad žmogus būtų nusiteikęs mokytis, motyvuotas, nebijantis iššūkių ar nesėkmių (užsispyręs, neišlepęs).

Įžvalgos apie rinką – koks šiuo metu KS specialistų atlyginimas?

Junior KSS į rankas iki 900 €, *Mid level* (turintis virš 2 metų įvairios patirties, pažįstantis daugelį sistemų, galintis daugelį dalykų daryti savarankiškai) 1500-2200 €, *Senior* 2500-5000 €.

Kalbant apie moterų ir merginų pritraukimą į KSS, kaip jūsų organizacijoje?

Sutinku, kad moterų dar labai mažai, tačiau jau visur atsiranda ir tendencija teigiama.

O kaip dėl amžius. Ar turi įtakos?

Amžiaus atžvilgiu – Lietuva yra jaunuolių kraštas, nes užsienyje tikrai daugiau sutinka ir 40-mečių ir net 60-mečių *KSS*. Jie anksčiau priėmė mokymosi visą gyvenimą kultūrą. Lietuvoje vyresnio amžiaus specialistai irgi galėtų pereiti į KS, tačiau galbūt trūksta drąsos.

A.5. Fokus grupės dialogo gairės

Klausimai:

1. Bendrais bruožais apibūdinkite savo patirtį KSS. Kaip apibūdintumėte savo pareigybę ir kokios veiklos į ją įeina?:
2. Kas Jums yra kibernetinis saugumas vienu sakiniu, fraze, siejant su darbu ar bendrai sritimi?
3. Kokios aplinkybės nulėmė, kad šiandien dirbate KSS ir siejate su KSS savo ateitį?
4. Kokios turimos kompetencijos Jums padeda įeiti į KSS?
5. Jūsų nuomone, kokių kompetencijų Jums trūksta ir kaip jas galėtumėte įgyti?
6. Kuo moterims gali būti patrauklus darbas KSS? Ko reikia, kad moterų daugiau atsirastų KSS? Kokie moterų gebėjimai gali būti išskirtiniai ir užtikrinantys aukštą konkurencingumą šioje srityje?
7. Kokį matytumėte savo karjeros kelią ateityje?
8. Baigiant pokalbį, ar liko kuo norėtumėte pasidalinti iš savo profesinio kelio patirties?

Kibernetinio saugumo laboratorija

Informatikos institutas,

Vilniaus universitetas

Didlaukio g. 47, LT-08303 Vilnius

Lietuva

Tel. 8 5 219 5002

cyberlab@mif.vu.lt