EUROPOS
KOMISIJA

Strasbūras, 2023 04 18
COM(2023) 207 final

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI

Kibernetinio saugumo srities talentų trūkumo problemos sprendimas siekiant didinti ES konkurencingumą ir atsparumą bei skatinti jos augimą

(Kibernetinio saugumo įgūdžių akademija)

Kibernetinio saugumo srities talentų trūkumo problemos sprendimas siekiant didinti ES konkurencingumą ir atsparumą bei skatinti jos augimą

(Kibernetinio saugumo įgūdžių akademija)

1. Neatidėliotinas poreikis sumažinti riziką sprendžiant kibernetinio saugumo įgūdžių trūkumo ir spragų problemą

Kibernetinis saugumas yra ne tik piliečių, įmonių ir valstybių narių saugumo dalis. Jis taip pat būtinas siekiant užtikrinti ES politinį stabilumą, jos demokratinių valstybių stabilumą bei mūsų visuomenės ir įmonių klestėjimą. Pastaraisiais metais **grėsmių** kibernetiniam saugumui **situacija** smarkiai pasikeitė ir išryškėjo nerimą kelianti tendencija – kad vis daugiau kibernetinių išpuolių yra nukreipta prieš karinę ir civilinę ypatingos svarbos infrastruktūrą ES. Priešiški subjektai stiprina savo pajėgumus ir atsiranda naujų, hibridinių ir besiformuojančių grėsmių, kaip antai robotų ir dirbtiniu intelektu pagrįstų technologijų naudojimas[1]. Konkrečiai, priešiški subjektai, naudojantys išpirkos reikalavimo programinę įrangą, subjektams nuolat padaro daug finansinės žalos ir žalos reputacijai[2].

Daug kibernetinio saugumo incidentų taip pat buvo nukreipta prieš valstybių narių viešojo administravimo įstaigas ir vyriausybes, taip pat Europos institucijas, įstaigas ir agentūras (EUIBA)[3]. Kibernetiniai išpuoliai taip pat buvo nuolat vykdomi finansų[4] ir sveikatos priežiūros[5] sektoriuose, kurie yra visuomenės ir ekonomikos pagrindas[6]. Dėl geopolitinės įtampos, susijusios su Rusijos agresijos karu prieš Ukrainą, grėsmė kibernetiniam saugumui padidėjo[7] ir gali destabilizuoti mūsų visuomenę. ES **saugumo** negalima užtikrinti be **didžiausio ES turto**: **jos žmonių.** ES skubiai reikia specialistų, turinčių įgūdžių ir gebėjimų užkirsti kelią kibernetiniams išpuoliams, juos nustatyti, nuo jų atgrasyti ir nuo jų apginti ES, įskaitant jos reikšmingiausius ypatingos svarbos infrastruktūros objektus, bei užtikrinti ES **atsparumą**.

Dėl kibernetinio saugumo srities talentų trūkumo mažiau didėja Europos **konkurencingumas** ir **augimas**, kurie labai priklauso nuo strateginių skaitmeninių technologijų (pvz., dirbtinio

---

[1] Europos Sąjungos tinklų ir informacijos apsaugos agentūra (ENISA), 2022 m. grėsmių padėtis — ENISA (europa.eu).

[2] 2021 m. Europolo organizuoto nusikalstamumo internete grėsmės vertinimas (IOCTA). Tokių subjektų veikla grindžiama paslaugos siūlant išpirkos reikalavimo programinę įrangą modeliu. 2022 m. metinės išlaidos įmonėms viršijo 18,4 mlrd. EUR (*Cybereason 2022 Report on the true cost or Ransomware*).

[3] Žr., pavyzdžiui, bendrą ENISA ir Sąjungos institucijų, įstaigų, organų ir agentūrų Kompiuterinių incidentų tyrimo tarnybos (CERT-EU) publikaciją JP-23-01 – „Konkrečių priešiškų subjektų ilgalaikė veikla“ (angl. „Sustained activity by specific threat actors“), TLP:CLEAR, 2023 m. vasario 15 d.

[4] Pavyzdžiui, Vokietijoje 90 proc. sukčiavimo paštu atvejų, apie kuriuos pranešta 2021 m. birželio 1 d.–2022 m. gegužės 31 d., buvo finansinių duomenų viliojimas arba, antai, vykdytas išpuolis prieš finansinio sektoriaus įmonę, kuriame dalyvavo daugiau kaip 20 000 virusu užkrėstų įrenginių iš 125 šalių, The State of IT Security in Germany in 2022, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2023 m. sausio 1 d.

[5] Pavyzdžiui, Prancūzijoje buvo vykdomi išpuoliai naudojant išpirkos reikalavimo programinę įrangą prieš visuomenės sveikatos priežiūros įstaigas, kaip antai „Centre Hospitalier Sud Francilien“, kurių metu priešiški subjektai pažeidė ir paskelbė 11 GB asmens ir medicininių duomenų, taip pat su darbuotojais susijusių duomenų, Panorama de la cybermenace 2022, Agence nationale de la sécurité des systèmes d'information (ANSSI), janvier 2023 .

[6] ENISA, 2022 m. grėsmių padėtis.

[7] Dar žr. CERT-EU – Rusijos karas prieš Ukrainą. vieneri metai kibernetinių operacijų (europa.eu); Rusijos kibernetinės operacijos prieš Ukrainą. Vyriausiojo įgaliotinio deklaracija Europos Sąjungos vardu, 2022 m. gegužės 10 d. ; Vyriausiojo įgaliotinio deklaracija Europos Sąjungos vardu dėl kibernetinės kenkimo veiklos, kurią įsilaužėliai ir įsilaužėlių grupės vykdo Rusijos agresijos prieš Ukrainą kontekste, 2022 m. liepos 19 d.

intelekto, 5G ir debesijos) plėtros ir naudojimo. Kad ES galėtų toliau kurti pagrindines pažangiąsias technologijas pasauliniu mastu, reikia kvalifikuotų kibernetinio saugumo specialistų.

Siekiant pasiruošti šioms kintančioms grėsmėms ir į jas atsižvelgti, taip pat siekiant skatinti ES konkurencingumą, pastaraisiais metais ES kibernetinio saugumo politikos srityje buvo padaryta didelė pažanga, kurios rezultatas – priimtos kelios iniciatyvos, kaip antai Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategija[8], peržiūrėta Tinklų ir informacinių sistemų saugumo direktyva (TIS 2 direktyva)[9], ES sektorių kibernetinio saugumo srities teisės aktai[10], ES kibernetinės gynybos politika[11], Kibernetinio atsparumo aktas[12] ir Kibernetinio solidarumo aktas – pasiūlymą dėl jo Komisija teikia kartu su šiuo komunikatu. Tačiau šiais teisės aktais juose numatytų tikslų nebus pasiekta be kvalifikuotų darbuotojų, kurie galėtų šiuos teisės aktus įgyvendinti. Nors visuomenei stengiamasi suteikti pagrindinių žinių kibernetinio saugumo srityje pagal iniciatyvas, kuriomis siekiama ugdyti bendruosius įgūdžius, reikalingus gyvenimui visuomenėje[13], tačiau, **siekiant įvykdyti tuos teisinius ir politikos reikalavimus kibernetinio saugumo srityje**, būtini kvalifikuoti darbuotojai ir viešajame, ir privačiajame sektoriuose, įskaitant standartizacijos organizacijas, tiek nacionaliniu, tiek ES lygmeniu.

Taigi, ES saugumas ir konkurencingumas priklauso nuo kvalifikuotų kibernetinio saugumo specialistų. Tačiau ES patiria itin didelį kvalifikuotų kibernetinio saugumo specialistų trūkumą, todėl ES, jos valstybėms narėms, įmonėms ir piliečiams kyla kibernetinio saugumo incidentų rizika. 2022 m. Europos Sąjungoje trūko **nuo 260 000**[14] **iki 500 000**[15], kibernetinio saugumo specialistų; buvo apskaičiuota, kad ES reikalinga 883 000 kibernetinio saugumo specialistų, o tai rodo[16], kad esami darbuotojų gebėjimai neatitinka darbo rinkai reikalingų gebėjimų. Kibernetinio saugumo specialistų skaičiui neigiamą poveikį taip pat daro klaidingas supratimas, susijęs su šios specialybės techniniu įvaizdžiu; į šią sritį toliau

[8] Bendras komunikatas Europos Parlamentui ir Tarybai „Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategija“, JOIN(2020) 18 *final*.

[9] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva).

[10] Pavyzdžiui, finansų sektoriuje – 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011 (DORA reglamentas).

[11] Bendras komunikatas Europos Parlamentui ir Tarybai, ES kibernetinės gynybos politika, JOIN(2022) 49 *final*.

[12] Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams, kuriuo iš dalies keičiamas Reglamentas (ES) 2019/1020, COM/2022/454 *final*.

[13] Kai kurios svarbios iniciatyvos, skirtos gyventojų bendriesiems skaitmeniniams įgūdžiams: Europos socialinių teisių ramsčio veiksmų plane numatytas tikslas iki 2030 m. pasiekti, kad 80 proc. gyventojų turėtų pagrindinius skaitmeninius įgūdžius, Skaitmeninės politikos kelrodis, 2021–2027 m. skaitmeninio švietimo veiksmų planas, Skaitmeninės kompetencijos programa, pasiūlymas dėl Tarybos rekomendacijos dėl skaitmeninių įgūdžių ugdymo švietimo ir mokymo srityje gerinimo.

[14] (ISC)² (Tarptautinis informacinių sistemų saugumo sertifikavimo konsorciumas) Kibernetinių įgūdžių vertinimas remiantis Europos kibernetinio saugumo įgūdžių sistema (angl. *Assessing Cyber Skills on the basis of the ECSF*), ENISA internetinis seminaras, 2023 m. vasario 16 d.

[15] Remiantis Europos kibernetinio saugumo organizacija (ECSO), kaip nurodyta bendrame komunikate Europos Parlamentui ir Tarybai, ES kibernetinės gynybos politika, JOIN(2022) 49 *final*.

[16] (ISC²) Kibernetinių įgūdžių vertinimas remiantis Europos kibernetinio saugumo įgūdžių sistema (ECSF), ENISA internetinis seminaras, 2023 m. vasario 16 d.

nepavyksta pritraukti **moterų** – jos sudaro 20 proc. kibernetinio saugumo studijų absolventų[17] ir 19 proc. informacinių ir ryšių technologijų specialistų[18]. Siekiant spręsti šią problemą Europos **2030 m. Skaitmeninio dešimtmečio politikos programoje**[19] nustatytas tikslas iki 2030 m. padidinti IRT specialistų skaičių iki 20 milijonų, kartu pasiekiant lyčių konvergenciją. Be to, naujai ES politikai įgyvendinti reikalingas pakankamas skaičius reikiamą kvalifikaciją turinčių darbuotojų. Pavyzdžiui, daugiau kaip 42 proc. aukštesniųjų IT vadovų finansinių paslaugų sektoriuje kibernetinio saugumo įgūdžių ir žinių trūkumą nurodė kaip pagrindinį sunkumą, su kuriuo jų verslas susidurs kibernetinio saugumo gynybos ir incidentų valdymo srityje[20] tuo metu, kai jie turės įgyvendinti sektorių kibernetinio saugumo srities teisės aktus, kaip antai Skaitmeninės veiklos atsparumo aktą (DORA).

Prie darbo rinkos suvaržymo taip pat prisideda darbdavių nenoras investuoti į žmogiškąjį kapitalą: jie ieško jau parengtų ir patyrusių darbuotojų[21]. Šis trūkumas turi įtakos visų rūšių įmonėms, įskaitant mažąsias ir vidutines įmones (**MVĮ**), sudarančias 99 proc. visų ES įmonių[22]. Didelių sunkumų kyla ir **viešojo administravimo įstaigoms**, kuriose kibernetinio saugumo incidentai pasitaiko dažniausiai ir turi didžiausią poveikį[23].

Todėl ES profesionalių kibernetinio saugumo srities talentų trūkumo problema turi būti sprendžiama skubos tvarka, nes kyla pavojus ES saugumui ir konkurencingumui.

2. Sinergijos ir suderintų veiksmų siekiant spręsti kibernetinio saugumo įgūdžių trūkumo problemą stoka

Europos ir nacionaliniu lygmeniu sėkmingai įgyvendinama nemažai viešųjų ir privačiųjų subjektų iniciatyvų, skirtų kibernetinio saugumo darbo rinkos trūkumų problemai spręsti. Tačiau jos yra pabiros ir iki šiol nepasiekė tokio lygio, kad padėtis tikrai pasikeistų.

Pirma, šiuo metu bendras supratimas apie ES kibernetinio saugumo darbo jėgos sudėtį ir susijusius įgūdžius yra ribotos, nors panašių kibernetinio saugumo srities pareigybių aprašymuose turėtų būti numatyti vienodi įgūdžiai. Kadangi susiję subjektai mažai naudojasi bendra **Europos kibernetinio saugumo specialistų orientacine sistema**, nėra priemonės, kuri padėtų bendrauti darbdaviams, pedagogams ir politikos formuotojams, ir nėra galimybių atlikti matavimus ir įvertinti kibernetinio saugumo darbo rinkos trūkumus. Tai taip pat trukdo rengti švietimo bei mokymo programas ir kurti karjeros galimybes, atitinkančias politiką ir su asmenimis, norinčiais užsiimti šia profesija, susijusius rinkos poreikius. Darbuotojų kvalifikacijos **kėlimas ir perkvalifikavimas** dažnai vykdomas pasitelkiant kibernetinio saugumo mokymus ir sertifikatus, kuriuos paprastai teikia privatūs teikėjai. Tačiau darbuotojams sunku susidaryti bendrą įspūdį apie kibernetinio saugumo mokymų ir išduodamų susijusių sertifikatų kokybę.

---

[17] Kibernetiniam saugumui skirto aukštojo išsilavinimo duomenų bazė (CyberHEAD).

[18] Tik 19 proc. IRT specialistų ES yra moterys Skaitmeninės ekonomikos ir visuomenės indeksas (DESI) 2022 m. | Europos skaitmeninės ateities formavimas (europa.eu). Duomenų apie tai, kiek moterų Sąjungoje dirba kibernetinio saugumo srityje, nėra.

[19] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos sprendimas (ES) 2022/2481, kuriuo nustatoma 2030 m. Skaitmeninio dešimtmečio politikos programa, kuria nustatomas stebėsenos ir bendradarbiavimo mechanizmas bendriems Europos skaitmeninės transformacijos tikslams ir uždaviniams (įskaitant įgūdžių sritį), nustatytiems 2030 m. Skaitmeninės politikos kelrodyje, įgyvendinti.

[20] S-RM 2022 m. kibernetinio saugumo įžvalgų ataskaita.

[21] Kibernetinio saugumo įgūdžių ugdymas ES, ENISA, 2019 m. gruodžio mėn.

[22] MVĮ apibrėžtis (europa.eu).

[23] Europos Sąjungos tinklų ir informacijos apsaugos agentūra (ENISA), 2022 m. grėsmių padėtis — ENISA (europa.eu).

Nors švietimas, mokymas ir karjeros galimybių formavimas yra būtini siekiant gerinti pasiūlą darbo rinkoje, šiuo metu nepakankamai įvertinamas **paklausos** vaidmuo rengiant savo darbo jėgą ir prisitaikant prie jos pokyčių. Privataus ir viešojo sektoriaus darbdaviams trūksta bendrų forumų ir vietų, kuriose jie galėtų telkti idėjas, kaip geriausiai parengti darbuotojus, ir spręsti, kaip **geriau įvertinti įgūdžius**, ypač darbuotojų atrankos proceso metu. Paklausiausi **dalykiniai įgūdžiai** yra susiję su kibernetiniu saugumu[24], kaip antai programinės įrangos kūrimo ar debesų kompiuterijos įgūdžiai[25], tačiau vis dar nepagrįstai neatsižvelgiama į **universaliuosius įgūdžius**. Darbdaviai dažniau reikalauja kritinio mąstymo ir analizės, problemų sprendimo ir savarankiško sprendimų priėmimo įgūdžių[26] ir artėjant 2025 m. šie įgūdžiai darosi vis svarbesni[27].

Jau yra daug viešų ir privačių investicijų į kibernetinio saugumo įgūdžių tobulinimą iniciatyvų, o ES plačiai **finansuoja** projektus pagal įvairias priemones[28]. Tačiau ES toliau susiduriant su kvalifikuotų darbuotojų trūkumo problema kyla klausimų dėl jų matomumo bei poveikio ir galima spręsti, kad šios iniciatyvos sistemingai nepatenkina rinkos poreikių – juos reikia nedelsiant išanalizuoti ES lygmeniu. Be to, kai finansavimo šaltiniai yra keli, tada dubliuojami veiksmai ir praleidžiama proga didinti veiklos mastą ir daryti realų poveikį. Be to, tie, kuriems reikalingos investicijos, ne visada gali nustatyti jų poreikius labiausiai atitinkančius šaltinius.

Suinteresuotieji subjektai bando spręsti sudėtingą ir įvairialypę kibernetinio saugumo įgūdžių trūkumo problemą. ES kibernetinio saugumo agentūra (ENISA) kuria priemones, susijusias su pareigybių aprašymais ar aukštuoju išsilavinimu[29], Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras (ECCC)[30] kibernetinio saugumo įgūdžius aptaria specialioje darbo grupėje, Europos saugumo ir gynybos koledžas (ESGK) dirba tobulindamas civilinės ir karinės srities darbuotojų kibernetinio saugumo įgūdžius bendros saugumo ir gynybos politikos kontekste[31], problemą bando spręsti privačios organizacijos[32], kibernetinio saugumo sertifikavimo sektorius kuria veiksmų gaires ir mokymus įgūdžių trūkumo problemai spręsti[33]. Valstybės narės taip pat bando keisti situaciją įgyvendindamos įvairias iniciatyvas, tokias kaip reglamentavimo iniciatyvos[34], kibernetinių įgūdžių akademijų[35] ar kibernetinio saugumo mokymo centrų[36],

[24] „LinkedIn 2023 Most In-Demand Skills: Learn the Skills Companies Need Most“

[25] ISACA 2022 m. kibernetinio saugumo padėties infografikas.

[26] Pavyzdžiui, Europos profesinio mokymo plėtros centro (CEDEFOP) priemonė „Skills-OVATE“ | CEDEFOP (europa.eu).

[27] Ataskaita „Darbo vietų ateitis“, 2020 m. spalio mėn., Pasaulio ekonomikos forumas.

[28] Pavyzdžiui: Kibernetinio saugumo įgūdžių aljansas – Nauja Europos vizija – Projektas REWIRE (finansuojamas pagal programą „Erasmus+“); projektai, kuriais remiamas Kibernetinio saugumo kompetencijos centras (ECHO, CONCORDIA, CyberSec4Europe, SPARTA (finansuojami pagal programą „Horizontas 2020“), projektas „Cybersecpro“ (finansuojamas pagal Skaitmeninės Europos programą).

[29] Visų pirma: Europos kibernetinio saugumo įgūdžių sistema (ECSF); CYBERHEAD – Kibernetiniam saugumui skirto aukštojo išsilavinimo duomenų bazė; Kibernetinio saugumo pratybų platforma (angl. *Cyber Exercise Platform*); Europos kibernetinio saugumo iššūkiai (angl. *European Cyber Security Challenge*); Europos kibernetinio saugumo mėnuo (angl. *European Cyber Security Month*).

[30] 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/887, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas.

[31] Visų pirma Švietimo, mokymo, vertinimo ir pratybų kibernetinėje srityje platforma.

[32] Pavyzdžiui, Europos kibernetinio saugumo organizacijos penktoji darbo grupė „Švietimas, mokymas, sąmoningumas, kibernetiniai poligonai, žmogiškieji veiksniai“; organizacija DIGITALEUROPE.

[33] Pavyzdžiui, SANS institutas, (ISC)², ISACA

[34] Pavyzdžiui, nacionalinės švietimo ar kibernetinio saugumo strategijos.

[35] Pavyzdžiui, C-Academy Portugalijoje.

[36] Pavyzdžiui, Kibernetinio saugumo mokymo centrai Prancūzijoje.

kibernetinių nusikaltimų kompetencijos centrų[37] steigimas, viešojo ir privačiojo sektorių partnerystės[38]. Tačiau visų šių suinteresuotųjų subjektų darbas dažnai nepakankamai koordinuojamas ir stokoja sinergijos, be to, neišnaudojamas jo potencialas reikšmingai pakeisti darbo rinką, kaip matyti iš vis didėjančio kibernetinio saugumo specialistų trūkumo ES. Taip pat reikia stiprinti kibernetinių bendruomenių sąveiką, nes įgūdžiai, reikalingi kibernetiniam saugumui užtikrinti, kovai su **kibernetiniais nusikaltimais** ar **kibernetinei gynybai** stiprinti, dažnai yra panašūs.

Galiausiai, šiandien ES turi ribotas galimybes įvertinti **kibernetinio saugumo darbo rinkos padėtį bei pokyčius** ir jos darbuotojų įgūdžius. Valstybės narės ir Europos institucijos, įstaigos ir agentūros remiasi privačių subjektų surinktais duomenimis arba platesniu ES mastu, visų pirma Eurostato[39] ir Europos profesinio mokymo plėtros centro (CEDEFOP)[40], surinktu duomenų apie IRT specialistus rinkiniu. Kitaip tariant, ES turimas poreikių vaizdas yra dalinis ir fragmentiškas, o tai trukdo suformuoti bendrą vaizdą apie kibernetinio saugumo rinkos padėtį.

3. Koordinuotas ES atsakas: Kibernetinio saugumo įgūdžių akademija

3.1. Tikslas

Siekdama spręsti kibernetinio saugumo įgūdžių problemą ir pašalinti darbo rinkos trūkumus, taip pat atsižvelgdama į Europos įgūdžių metus, Komisija siūlo įsteigti **Kibernetinio saugumo įgūdžių akademiją**, kaip pranešimo apie Sąjungos padėtį 2022 m. ketinimų rašte yra skelbusi Europos Komisijos pirmininkė[41, 42].

Kibernetinio saugumo įgūdžių akademijos (toliau – Akademija) tikslas yra sukurti **bendrą prieigos ir sinergijos punktą**, kur būtų galima sužinoti švietimo ir mokymo kibernetinio saugumo srityje pasiūlymus, finansavimo galimybes ir konkrečius kibernetinio saugumo įgūdžių ugdymą remiančius veiksmus. Taip bus išplėstos suinteresuotųjų subjektų iniciatyvos, kad jos pasiektų tokį lygį, jog turėtų poveikį darbo rinkai, be kita ko, gynybos srityje. Siekiant didesnio poveikio ši veikla orientuojama į bendrus tikslus ir pagrindinius veiklos rezultatų rodiklius.

Akademijos prioritetas bus **kibernetinio saugumo specialistų** įgūdžių ugdymas. Akademijos veikla praturtins ne tik ES kibernetinio saugumo, bet ir švietimo ir mokymosi visą gyvenimą srityse politiką. Ji papildo dvi Tarybos rekomendacijas, susijusias su skaitmeniniu švietimu ir įgūdžiais; pasiūlymus dėl šių rekomendacijų Komisija teikia tuo pačiu metu, kaip ir šį komunikatą[43].

Akademija remsis keturiais veiklos ramsčiais: 1) skatins **kurti žinias švietimo ir mokymo būdais**, kuriant bendrą kibernetinio saugumo specialistų vaidmenų profilių ir susijusių įgūdžių sistemą, didinant Europos švietimo ir mokymo pasiūlą, kad ji atitiktų poreikius, kuriant karjeros galimybes ir užtikrinant kibernetinio saugumo mokymų ir sertifikatų

[37] Pavyzdžiui, Lietuvos kibernetinių nusikaltimų kompetencijų ir tyrimų centras Lietuvoje (L3CE).

[38] Pavyzdžiui, „Microsoft“ kibernetinio saugumo įgūdžių ugdymo iniciatyva (angl. *Cybersecurity Skilling Initiative*).

[39] IRT specialistai darbo rinkoje – Statistikos paaiškinimas (europa.eu).

[40] Pavyzdžiui, Europos profesinio mokymo plėtros centro (CEDEFOP) priemonė: „Skills-OVATE“ | CEDEFOP (europa.eu).

[41] Pranešimo apie Sąjungos padėtį 2022 m. ketinimų raštas Pirmininkei Robertai Metsolai ir Ministrui Pirmininkui Petrui Fialai.

[42] Bendras komunikatas Europos Parlamentui ir Tarybai, ES kibernetinės gynybos politika, JOIN(2022) 49 *final*.

[43] Pasiūlymai dėl Tarybos rekomendacijų dėl pagrindinių veiksnių, kurie leistų užtikrinti sėkmingą skaitmeninį švietimą ir mokymą ir dėl skaitmeninių įgūdžių ugdymo švietimo ir mokymo srityje gerinimo.

matomumą ir aiškumą, kad būtų augtų darbo jėgos pasiūla; 2) užtikrins geresnį turimų su įgūdžiais susijusios veiklos **finansavimo galimybių** orientavimą ir matomumą, siekiant kuo labiau padidinti jų poveikį; 3) ragins suinteresuotuosius subjektus **imtis veiksmų** ir 4) nustatys **rinkos raidos stebėsenos** ir gebėjimo įvertinti savo veiksmų efektyvumą rodiklius.

Akademijai įsteigti bus skirtas 10 mln. EUR finansavimas pagal Skaitmeninės Europos programą[44].

3.2.Akademijos valdymas

Galiausiai, siekiant sukurti infrastruktūrą, kuri būtų naudojama kaip **bendras prieigos punktas**, skirtas bendruomenės, mokymo paslaugų teikėjų ir pramonės atstovų bendradarbiavimui stiprinti, kuriame ES kibernetinio saugumo ekosistemos tiekėjai ir vartotojai galėtų susitikti ir mokytis, Akademija galėtų būtų įsteigta kaip **Europos skaitmeninės infrastruktūros konsorciumas (ESIK)**[45]. Ši priemonė leistų valstybėms narėms kartu siekti pašalinti kibernetinio saugumo įgūdžių trūkumą, taip pat glaudžiai bendradarbiauti su Komisija, ENISA ir ECCC, atsižvelgiant į jų įgaliojimus ir kompetenciją, bei sutelkti visus suinteresuotuosius subjektus, taip pat tiesiogines Europos, nacionalines ir privačias investicijas bendram tikslui. Šiuo tikslu suinteresuotos valstybės narės raginamos iki 2023 m. gegužės 30 d. pateikti Komisijai išankstinį pranešimą, ar ateityje jos teiks paraišką dėl tokio ESIK. Tokie savanoriški išankstiniai pranešimai leistų Komisijai anksti pateikti pastabas dėl ESIK paraiškos projekto, kad paspartėtų tolesnio projekto tobulinimo ir oficialaus pateikimo procesas. Viso proceso metu ir tiek, kiek prašys valstybės narės, Komisija padės rengti ESIK paraišką, veikdama kaip daugiašalio projekto spartintoja. Paraiškai gavus teigiamą Komisijos įvertinimą ir Skaitmeninio dešimtmečio programos komiteto patvirtinimą, Komisija priimtų sprendimą, kuriuo įsteigiamas ESIK, o tada padėtų koordinuoti ESIK įgyvendinimą[46].

Tuo metu, kol bus oficialiai įsteigtas ESIK, Komisija, sukurs virtualų bendrą prieigos punktą, patobulindama jai priklausančią **Skaitmeninių įgūdžių ir užimtumo platformą**[47], tam panaudodama Paramos Europos kibernetinio saugumo bendruomenei projektą[48].

ENISA prisidės prie Akademijos įgyvendinimo vadovaudamasi agentūros tikslais[49], visų pirma susijusiais su pagalba kibernetinio saugumo švietimo ir mokymo srityje, ir atsižvelgdama į savo ataskaitų teikimo įpareigojimus pagal TIS 2 direktyvą[50]. **ECCC** rems Kibernetinio saugumo įgūdžių akademijos įgyvendinimą veikdamas pagal savo strateginę darbotvarkę. Konkrečiai, ECCC įgyvendins Skaitmeninės Europos programos 3 strateginį tikslą (kibernetinis saugumas). Per **nacionalinius koordinavimo centrus (NKC)** jam padės

---

[44] 2021 m. balandžio 29 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/694, kuriuo nustatoma Skaitmeninės Europos programa ir panaikinamas Sprendimas (ES) 2015/2240

[45] ESIK buvo numatytas 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos sprendimo (ES) 2022/2481, kuriuo nustatoma 2030 m. Skaitmeninio dešimtmečio politikos programa, 13 ir paskesniuose straipsniuose.

[46] Ten pat, 12 straipsnis.

[47] Pradžios puslapis | Skaitmeninių įgūdžių ir užimtumo platforma (europa.eu).

[48] Žr. Europos kibernetinio saugumo kompetencijos centras ir tinklas. Naujas ES finansuojamas paramos kibernetinei bendruomenei projektas (europa.eu). 2022 m. gruodžio mėn. Europos Komisija pasirašė 3 mln. EUR vertės sutartį dėl paramos ES kibernetinei bendruomenei per Europos kibernetinio saugumo kompetencijos centrą. Šis projektas padės siekti ES tikslų dėl bendruomenės ir gebėjimų stiprinimo kibernetinio saugumo mokslinių tyrimų, inovacijų, diegimo ir pramoninės bazės klausimais.

[49] „ENISA Sąjungoje remia pajėgumų stiprinimą ir parengtį, padėdama Sąjungos institucijoms, įstaigoms, organams ir agentūroms, taip pat valstybėms narėms ir viešojo bei privačiojo sektorių suinteresuotiesiems subjektams <...> plėtoti įgūdžius ir kompetencijas kibernetinio saugumo srityje.“ (Kibernetinio saugumo akto 4 straipsnio 3 dalis).

[50] TIS 2 direktyvos 18 straipsnis.

Komisija ir valstybės narės. Prireikus bus pasitelkiama **Bendradarbiavimo grupė**, įsteigta pagal TIS 2 direktyvą[51]. Galiausiai, norint pasiekti Akademijos tikslą išspręsti kibernetinio saugumo įgūdžių trūkumo problemą, reikės suvienyti jėgas su **pramonės** ir **akademinės bendruomenės** atstovais.

4. Žinių kūrimas ir mokymas: bendro ES požiūrio į mokymą kibernetinio saugumo srityje nustatymas

Pagal Kibernetinio saugumo įgūdžių akademijos žinių kūrimo ir mokymo veiklos kryptį bus suformuotas struktūrinis požiūris, turintis aiškų tikslą padidinti Sąjungoje asmenų, turinčių kibernetinio saugumo įgūdžių, **skaičių**, geriau pritaikyti mokymą **rinkos poreikiams** ir užtikrinti **karjeros galimybių** matomumą.

4.1. Vienodai apibūdinti: bendras požiūris į kibernetinio saugumo specialistų vaidmenų profilius ir susijusius įgūdžius

ENISA jau atliko nemažai darbo apibrėždama kibernetinio saugumo specialistų vaidmenų profilius pagal Europos kibernetinio saugumo įgūdžių sistemą (**ECSF**)[52]. Tas darbas turėtų būti pagrindu Akademijai apibrėžiant ir vertinant atitinkamus įgūdžius, stebint įgūdžių trūkumo pokyčius ir teikiant informaciją apie naujus poreikius. Į kiekvieno ECSF kibernetinio saugumo specialisto vaidmens profilio aprašymą[53] yra įtraukti taikytini gebėjimai, nurodyti Europos e. kompetencijos sistemoje[54].

Todėl ENISA peržiūrės ECSF ir **nustatys kintančius** kibernetinio saugumo darbuotojų **įgūdžių poreikius ir spragas**, be kita ko, taikydama pažangias priemones (pvz., dirbtinį intelektą, didžiuosius duomenis[55], duomenų gavybą). Šiuo tikslu ENISA dirbs vadovaujant ESIK, kai jis bus įsteigtas, ir Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrui, kartu su nacionaliniais koordinavimo centrais, Komisija, ECCO projekto atstovais ir rinkos dalyviais[56]. Kibernetinės gynybos darbuotojų klausimu ENISA deramai atsižvelgs į ESGK atliktą darbą. Be to, kovos su kibernetiniais nusikaltimais srityje ENISA atsižvelgs į ES teisėsaugos mokymo agentūros (CEPOL) ir Europolo veiklą rengiant su kibernetiniais išpuoliais susijusią operacinio rengimo poreikių analizę[57].

---

[51] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva).

[52] Europos kibernetinio saugumo įgūdžių sistema (ECSF) – ENISA (europa.eu). ECSF padeda nustatyti ir suformuluoti užduotis, gebėjimus, įgūdžius ir žinias, susijusias su Europos kibernetinio saugumo specialistų vaidmenimis. Joje apibendrinami visi su kibernetiniu saugumu susiję vaidmenys nurodant profilius, kurie atskirai išsamiai analizuojami pagal jų atitinkamą atsakomybę, įgūdžius, sinergiją ir tarpusavio sąsajas.

[53] Šiuo klausimu žr. Naudotojo vadovą – Europos kibernetinio saugumo įgūdžių sistemą (ECSF), 2022 m. rugsėjo mėn.

[54] Europos e. kompetencijos sistema (e-CF) | „Esco“ (europa.eu). „e-CF“ pateikiamos nuoseklios sąsajos su IRT kvalifikacijomis ir kitomis sektoriui reikšmingomis sistemomis, įskaitant „DigComp“.

[55] Žr., pavyzdžiui, CEDEFOP parengtą „Skills-OVATE“.

[56] Agentūra toliau naudosis kitų ES finansuojamų projektų (pvz., REWIRE, „Data Space For Skills“ (DS4S), „CyberSecPro, Concordia“) rezultatais ir panašių iniciatyvų (pvz., „Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom and United States“ (Kvalifikuotų kibernetinio saugumo srities specialistų rengimas penkiose šalyse. Australijos, Kanados, Naujosios Zelandijos, Jungtinės Karalystės ir Jungtinių Amerikos Valstijų įžvalgos), EBPO ataskaita, paskelbta 2023 m. kovo 21 d.), kad galėtų ateityje pateikti naujausią poreikių aplinkoje, kurioje nuolat keičiasi paklausa, viziją.

[57] CEPOL operacinio rengimo poreikių vertinimas (OTNA).

ECSF bus reguliariai papildoma ir peržiūrima Akademijoje kas dvejus metus. Be to, Komisija ir Europos išorės veiksmų tarnyba, remiamos ES agentūrų ir įstaigų, tokių kaip ESGK[58], Europolo ir CEPOL[59], pagal poreikį padės apibrėžti sektoriams skirtus konkrečius profilius ir susijusius įgūdžius.

Taip pat bus nustatyti ryšiai tarp ECSF ir atitinkamų ES užimtumo politikos priemonių[60]. Konkrečiai, ECSF pareigybių aprašymai ir susiję įgūdžiai bus įtraukti į **ESCO klasifikaciją**. Taip bus patikslinta kibernetinio saugumo srities profesijų ir įgūdžių klasifikacija ir sąsajos tarp jų, todėl asmenims bus paprasčiau kelti kvalifikaciją ir persikvalifikuoti, taip pat bus remiamas darbo jėgos pasiūlos ir paklausos derinimas atsižvelgiant į įgūdžius ir tarpvalstybinis judumas.

4.2. Bendradarbiavimo kuriant kibernetinio saugumo švietimo ir mokymo programas skatinimas

Įsteigus ESIK, Akademija turėtų gauti valstybių narių paramą, kad ji taptų į paklausiausius įgūdžius orientuota **pavyzdine kibernetinio saugumo mokymo kūrimo ir teikimo vieta Europoje**, startuoliams, MVĮ ir viešojo administravimo įstaigoms teikiančia mokymo darbo vietoje ir mokomosios praktikos galimybes novatoriškose kibernetinio saugumo įmonėse ir kibernetinio saugumo kompetencijos centruose. ESIK, rengdamas tokį mokymą, turėtų bendradarbiauti su visais suinteresuotaisiais subjektais, įskaitant pramonės atstovus, ir remtis projektais, kaip antai Skaitmeninės Europos programos lėšomis finansuojamu **„CyberSecPro“**[61], į kurį įsitraukusios 17 aukštojo mokslo institucijų ir 13 saugumo bendrovių iš 16 valstybių narių siekia kartu formuoti visų kibernetinio saugumo mokymo programų geriausią patirtį.

Akademija bendradarbiaus su visais susijusiais suinteresuotaisiais subjektais siekdama **paskatinti jaunimą** pradėti karjerą kibernetinio saugumo srityje. Atsižvelgdamos į pasiūlymą dėl Tarybos rekomendacijos dėl skaitmeninių įgūdžių ugdymo švietimo ir mokymo srityje gerinimo, valstybės narės turėtų priimti ir sustiprinti mokytojams ir dėstytojams specialistams įdarbinti ir mokyti skirtas priemones, taip pat palengvinti kibernetinio saugumo įgūdžių įgijimą, be kita ko, per pameistrystę. Turėtų būti skatinama įtraukti kibernetinį saugumą į švietimo ir mokymo programas, kartu užtikrinant jų prieinamumą, kurti **pameistrystės** ir stažuočių pasiūlą, skatinti novatoriškus metodus, įskaitant, pavyzdžiui, rimtuosius žaidimus ir bendras imitavimo platformas, organizuoti kibernetinio saugumo specialistų darbo išbandymo savaites, paaiškinti netechninių vaidmenų profilius. Taip pat turėtų būti remiamas sunkiai pasiekiamų grupių, pavyzdžiui, neįgalių jaunuolių, gyvenančių atokiose ar kaimo vietovėse, ir kitų mažumų grupių, naudojimasis šiomis kibernetinio saugumo mokymosi galimybėmis.

---

[58] Šiuo klausimu žr. Bendrą komunikatą Europos Parlamentui ir Tarybai, ES kibernetinės gynybos politika, JOIN(2022) 49 *final*.

[59] Šiuo klausimu bus atsižvelgta į darbą, susijusį su šiuo metu kuriama Kovos su kibernetiniais nusikaltimais mokymo gebėjimų sistema (angl. *Cybercrime Training Competency Framework*, TCF).

[60] Pavyzdžiui, Europos įgūdžių (gebėjimų), kvalifikacijų ir profesijų klasifikatorius (ESCO), „Europass“, Europos užimtumo tarnybų bendradarbiavimo tinklas (EURES).

[61] Pagal „CyberSecPro“ , pavyzdžiui, bus atlikta universitetuose siūlomų kibernetinio saugumo programų, kursų ir vasaros mokyklų bei naudojamų Europos kreditų perkėlimo sistemos (ECTS) vertinimo skalių analizė, užtikrinamas tikslinio skaičiaus – daugiau kaip 530 stažuotojų – dalyvavimas 3 metų laikotarpiu, mokomi išorės asmenys iš įvairių pramonės šakų ir sektorių.

Komisija toliau teiks paramą mikrokredencialų, profesinio mokymo ir mokymo programų rengimui. Konkrečiai, pagal programą „Erasmus+“ toliau bus finansuojamos **jungtinės bakalauro ir magistrantūros programos, jungtiniai kursai ar moduliai, kurie leistų gauti mikrokredencialų**, ir **mišrios intensyvios programos**[62] visomis temomis, įskaitant **kibernetinį saugumą**. Taip pat bus remiamas tolesnis **Europos universitetų iniciatyvos**[63] ir **profesinės kompetencijos centrų**[64] įgyvendinimas siekiant skatinti glaudesnį aukštojo mokslo, atitinkamo profesinio rengimo ir mokymo institucijų bendradarbiavimą Europoje. Šis glaudesnio bendradarbiavimo tikslas bus remiamas pagal ES finansavimo programas, įskaitant „Erasmus+“ ir Skaitmeninės Europos programą, taip pat ES lėšomis, skirtomis **individualiųjų mokymosi sąskaitų**[65] kūrimui.

Siekiant palengvinti akademinės bendruomenės ir kibernetinio saugumo įgūdžių mokymo paslaugų teikėjų ir privačiojo ir viešojo sektorių darbdavių bendradarbiavimą nacionaliniu lygmeniu ir skatinti viešojo ir privačiojo sektorių sinergiją, nacionaliniai koordinavimo centrai raginami įvertinti galimybę valstybėse narėse steigti **kibernetinio saugumo mokymo centrus** . Kibernetinio saugumo mokymo centrų tikslas būtų nacionaliniu lygmeniu rodyti pavyzdį kibernetinio saugumo bendruomenei, o Akademija padėtų jiems plėsti tinklaveiką ir toliau koordinuoti veiklą.

ENISA taip pat gerins savo kibernetinio saugumo mokymo pasiūlą, suderindama **savo kursų katalogą**[66] su ECSF profiliais ir rengdama kiekvienam profiliui skirtus mokymo modulius, o tai gali pagerinti valstybių narių mokymo pasiūlą. ENISA taip pat išplės savo **mokytojų mokymo programą**[67], atsižvelgdama į ES institucijų, įstaigų, organų ir agentūrų, valstybių narių valdžios institucijų ir **viešųjų ir privačių ypatingos svarbos operatorių**, kuriems taikoma TIS 2 direktyva, profesinius poreikius.

Be to, savo kibernetinio saugumo mokymo pasiūlą plės kitos ES agentūros ir įstaigos. Pavyzdžiui, įgyvendinant ES kibernetinės gynybos politiką, **ESGK** parengs naują kibernetinio saugumo kursų grupę, o kai kuriuos dabartinius kursus suderins su ECSF. Išklausius šiuos kursus bus galima sertifikuoti mokymosi rezultatus[68]. ESGK, bendradarbiaudamas su Komisija, įvertins galimybę įtraukti sertifikatus į ES e. ID dėklę. ESGK taip pat įvertins galimybę vertinti įgūdžių mechanizmus, pagal kuriuos bus išduodami sertifikatai. Kovos su kibernetiniais nusikaltimais srityje taip pat bus siekiama glaudžiai bendradarbiauti su **CEPOL Kovos su kibernetiniais nusikaltimais akademija**[69], kad būtų mokymo programas rengiantys ir įgyvendinantys subjektai pasiektų sinergiją ir vieni kitus papildytų.

4.3.Kibernetinio saugumo mokymo ir sertifikavimo sinergijos kūrimas ir matomumo užtikrinimas valstybėse narėse

[62] Pagal mišrias intensyvias programas derinamas mokymas internetu ir trumpas fizinio mobilumo laikotarpis.

[63] Europos universitetų iniciatyva | Europos švietimo erdvė (europa.eu).

[64] Profesinės kompetencijos centrai | „Erasmus+“ (europa.eu).

[65] Pagal 2022 m. birželio 16 d. Tarybos rekomendaciją dėl individualiųjų mokymosi sąskaitų.

[66] Mokymo kursai — ENISA (europa.eu).

[67] Mokytojų mokymo programa — ENISA (europa.eu).

[68] Pagal 2020 m. spalio 19 d. Tarybos sprendimo (BUSP) 2020/1515, kuriuo įsteigiamas Europos saugumo ir gynybos koledžas ir panaikinamas Sprendimas (BUSP) 2016/2382, 20 straipsnio 4 dalį.

[69] CEPOL Kovos su kibernetiniais nusikaltimais akademija įsteigta 2019 m., kad egzistuotų naujausius standartus atitinkanti platforma, padedanti gerinti žinias apie kibernetinius nusikaltimus ir kibernetinius pajėgumus Europoje.

Akademija turėtų spręsti mokymo ir sertifikavimo matomumo ir sinergijos klausimą. Tai būtų naudinga civilinėms, gynybos, teisėsaugos ir diplomatinėms kibernetinėms bendruomenėms, nes daugeliu atvejų visuose sektoriuose reikalinga vienoda kvalifikacija, įgyta pagal panašias mokymo programas ir mokymosi rezultatus.

Akademija suteiktų **bendrą prieigos punktą** asmenims, kuriuos domina karjera kibernetinio saugumo srityje. Artimiausiu metu tai bus daroma tobulinant Komisijos **Skaitmeninių įgūdžių ir užimtumo platformą**, tam pasinaudojant ECCO projektu. Specialiame kibernetinio saugumo karjeros skyriuje bus pateiktos nuorodos į esamas priemones – aukštojo mokslo programas, mokymo galimybes, įskaitant kursus, kurių metu galima gauti mikrokredencialų, ir profesinio rengimo ir mokymo programas, taip pat darbo pasiūlymus. Tai bus pasiekta platformoje nurodant arba į ją integruojant vykstantį darbą ir iniciatyvas, kaip antai tuos, kuriuos vykdo ENISA, kuri, bendradarbiaudama su akademine bendruomene, sudarė **švietimo institucijų**, kuriose teikiamos kibernetinio saugumo programos, **sąvadą**. Ji bus toliau tobulinama padedant nacionaliniams koordinavimo centrams. Be to, ENISA, padedama nacionalinių koordinavimo centrų, Komisijos ir ECCO projekto, ir bendradarbiaudama su sertifikatus išduodančiais subjektais, taip pat remdamasi kitomis susijusiomis iniciatyvomis[70], sukurs ir konsoliduos dvi **esamų viešojo ir privačiojo sektorių mokymų ir kibernetinio saugumo sertifikatų duomenų saugyklas**. Jos taip pat bus įtrauktos į Skaitmeninių įgūdžių ir užimtumo platformos bendrą prieigos punktą. Šis darbas taip pat bus naudingas nacionaliniams koordinavimo centrams, kurių užduotis visų pirma yra propaguoti ir skleisti kibernetinio saugumo švietimo programas[71].

Specialistai taip pat turi būti užtikrinti, kad mokymai, kuriuose jie dalyvauja, yra reikiamos kokybės. Šiuo klausimu ENISA parengs **bandomąjį projektą**, pagal kurį bus apsvarstyta galimybė nustatyti Europos kibernetinių įgūdžių atestavimo sistemą.

Be to, nors būtina nustatyti įgūdžius ir mokymus ir susieti juos su pareigybių aprašymais, tačiau taip pat svarbu užtikrinti, kad kibernetinio saugumo paslaugos būtų teikiamos turint reikiamą kompetenciją, kvalifikaciją ir patirtį. Tai ypač taikoma valdomiems saugumo paslaugų teikėjams, kurie teikia paslaugas tokiose srityse kaip reagavimas į incidentus, skverbimosi testavimas, saugumo auditai ir konsultacijos. TIS 2 direktyvoje ir pasiūlyme dėl Kibernetinio solidarumo akto nustatytos konkrečios tokių valdomų saugumo paslaugų teikėjų užduotys. Todėl Komisija taip pat siūlo tikslinį **Kibernetinio saugumo akto pakeitimą**[72], kad būtų galima ES lygmeniu taikyti valdomų saugumo paslaugų sertifikavimo schemas. Tokiomis sertifikavimo schemomis turėtų būti siekiama, be kita ko, užtikrinti, kad šias paslaugas teiktų darbuotojai, turintys itin aukšto lygio techninių žinių ir kompetencijos atitinkamose srityse.

Mikrokredencialų kokybės užtikrinimo ir pripažinimo mechanizmai[73] padeda užtikrinti mokymosi rezultatų skaidrumą, palyginamumą ir perkeliamumą. Pagal Tarybos

[70] Pavyzdžiui, „W4C Academy“ - „Women4Cyber“ arba Visuotinio kibernetinių nusikaltimų tyrėjų ir prokurorų sertifikavimo projektas, skirtas teisėsaugos ir teisminėms institucijoms.

[71] „1. Nacionaliniai koordinavimo centrai vykdo šias užduotis: <...> g) nedarant poveikio valstybių narių nacionalinei kompetencijai švietimo srityje ir atsižvelgdami į atitinkamas ENISA užduotis, bendradarbiauja su nacionalinėmis institucijomis galimo indėlio kibernetinio saugumo švietimo programų propagavimo ir sklaidos srityje“, Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro (ECCC) reglamento 7 straipsnio 1 dalies g punktas. Taip pat žr. susijusią 28 konstatuojamąją dalį.

[72] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas).

[73] Pavyzdžiui, mokymosi rezultatų, kuriuos asmenys įgyja po trumpų mokymų, įrašai arba sertifikatai.

rekomendaciją dėl europinio požiūrio į mikrokredencialus[74] valstybės narės raginamos įtraukti kibernetinio saugumo mikrokredencialus į savo nacionalines kvalifikacijų sandaras. Tai leistų joms susieti kibernetinio saugumo mikrokredencialus su Europos kvalifikacijų sandara[75]. Naudojantis Europos skaitmeninių mokymosi kredencialų infrastruktūra gali būti išduodamos skaitmeniniu būdu pasirašytos asmenų kibernetinio saugumo kvalifikacijos ir mikrokredencialai. Juose pateikiama daug duomenų, įskaitant duomenis apie mokymosi rezultatus kibernetinio saugumo srityje, ir jie gali būti saugomi būsimoje **ES e. ID skaitmeninėje dėklėje**[76].

Veiksmai įgyvendinant Akademiją

Valstybės narės ir pramonės atstovai

- Užtikrins paramą kibernetinio saugumo srities mokymosi **mikrokredencialų** kūrimui ir pripažinimui pagal Tarybos rekomendaciją dėl europinio požiūrio į mikrokredencialus.
- Į **nacionalines kvalifikacijų sandaras** įtrauks kibernetinio saugumo kvalifikacijas, įskaitant mikrokredencialus.
- Teiks **mokymosi darbo vietoje galimybes** pameistrystės praktikos forma asmenims, dalyvaujantiems kibernetinio saugumo įgūdžių ugdymo iniciatyvose.

Komisija

- Trumpuoju laikotarpiu, iki 2023 m. pabaigos, sukurs **bendrą prieigos punktą**, skirtą kibernetinio saugumo programoms, esamiems mokymams ir kibernetinio saugumo sertifikatams, prieinamą per **Skaitmeninių įgūdžių ir užimtumo platformą**.
- 2023 m. balandžio 18 d. pateiks pasiūlymą dėl **Kibernetinio saugumo akto** pakeitimo, kad būtų sudarytos sąlygos sertifikuoti valdomus saugumo paslaugų teikėjus.

ES įstaigos ir agentūros

- Iki 2023 m. pabaigos sukurs **ECSF** kaip bendrą požiūrį į kibernetinio saugumo specialistų vaidmenų profilius ir susijusius įgūdžius.
- ENISA – 2023 m. antrą ketvirtį pradės kurti bandomąjį projektą, pagal kurį būtų sukurta **Europos kibernetinių įgūdžių atestavimo sistema**.
- ENISA – iki 2023 m. pabaigos peržiūrės savo **kursų katalogą** ir atvers savo **mokytojų mokymo programą** viešiesiems ir privatiesiems ypatingos svarbos operatoriams.
- Iki 2023 m. vidurio baigs **derinti ESGK mokymo programas su ECSF**.

5. Suinteresuotųjų subjektų dalyvavimas: įsipareigojimas šalinti kibernetinio saugumo įgūdžių trūkumą

Akademijoje bus formuojamas koordinuotas požiūris į suinteresuotųjų subjektų dalyvavimą siekiant spręsti kibernetinio saugumo įgūdžių trūkumo problemą. Bus siekiama kuo labiau

[74] Tarybos rekomendacija dėl europinio požiūrio į mikrokredencialus mokymuisi visą gyvenimą ir įsidarbinamumui skatinti.

[75] 2017 m. gegužės 22 d. Tarybos rekomendacija dėl Europos mokymosi visą gyvenimą kvalifikacijų sandaros, kuria panaikinama 2008 m. balandžio 23 d. Europos Parlamento ir Tarybos rekomendacija dėl Europos mokymosi visą gyvenimą kvalifikacijų sąrangos kūrimo.

[76] Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo dėl Europos skaitmeninės tapatybės sistemos nustatymo iš dalies keičiamas Reglamentas (ES) Nr. 910/2014.

padidinti įvairių suinteresuotųjų subjektų įsipareigojimų, kuriais siekiama sumažinti kibernetinio saugumo įgūdžių trūkumą, matomumą ir poveikį.

Komisija ragina suinteresuotuosius subjektus prisiimti konkrečius įsipareigojimus specialiais veiksmais kelti ir keisti darbuotojų kvalifikaciją, kuo labiau atsižvelgiant į nustatytą kibernetinio saugumo įgūdžių trūkumą. Apie tokius **suinteresuotųjų subjektų įsipareigojimus dėl kibernetinio saugumo** turėtų būti pranešta **Skaitmeninių įgūdžių ir užimtumo platformoje**, panašiai kaip ir kitų platformoje jau rodomų skaitmeninių įsipareigojimų atveju. Komisija taip pat ragina suinteresuotuosius subjektus, Platformoje prisiimančius įsipareigojimus dėl kibernetinio saugumo, prisijungti prie **Plataus masto skaitmeninės partnerystės pagal Įgūdžių paktą**[77]. Įsipareigojimus dėl kibernetinio saugumo, prisiimtus pagal Plataus masto skaitmeninę partnerystę, skatinama pateikti Skaitmeninių įgūdžių ir užimtumo platformoje. Be to, apie Skaitmeninių įgūdžių ir užimtumo platformoje prisiimtus įsipareigojimus skatinama pranešti pagal Plataus masto skaitmeninę partnerystę pagal Įgūdžių paktą.

Komisija taip pat ragina valstybes nares **toliau dėti pastangas įgyvendinant deklaraciją „Moterys skaitmeninėje ekonomikoje“**[78] siekiant paskatinti moteris imtis aktyvaus ir ryškaus vaidmens skaitmeninių technologijų sektoriuje ir užtikrinti lyčių konvergenciją darbo vietose kibernetinio saugumo srityje. Komisija taip pat ragina valstybes nares plėtoti sąveiką su savo **„Europos socialinio fondo +“** (ESF+) programomis siekiant toliau remti lyčių lygybės darbo rinkoje tikslo įgyvendinimą[79], pavyzdžiui, parengiant **mergaitėms ir moterims skirtas mentorystės programas.** Jos gali padėti formuoti sektinus pavyzdžius siekiant paskatinti mergaites rinktis kibernetinio saugumo specialybes, kartu kovojant su lyčių stereotipais. Jos taip pat drąsina moteris kelti kvalifikaciją bei persikvalifikuoti ir skatina kurti bendruomenę, kuri galėtų padėti moterims patekti į kibernetinio saugumo darbo rinką arba kilti pareigose.

Valstybės narės, įgyvendindamos savo nacionalines kibernetinio saugumo strategijas, turėtų priimti konkrečias priemones, kuriomis būtų siekiama sumažinti **kibernetinio saugumo įgūdžių trūkumą**[80], nustatyti, kaip šalinti įgūdžių spragas, ir geriau nukreipti šias pastangas, ir galiausiai užtikrinti tinkamą savo įsipareigojimų pagal TIS 2 direktyvą įgyvendinimą.

Kai kurios valstybės narės naudojasi **civilinių, gynybos ir teisėsaugos iniciatyvų sinergija**. Pavyzdžiui, darbuotojų ugdymas pasitelkiant savo nacionalinę privalomąją karo tarnybą arba kibernetinio saugumo specialistus rezervininkus – karinį parengimą turinčius piliečius, užimančius kibernetinio saugumo pareigas ginkluotosiose pajėgose[81], sudaro sąlygas visuomenei, o ypač jaunimui ugdyti savo kibernetinio saugumo ir kibernetinės gynybos įgūdžius. Tas pats tinka ir **kovos su kibernetiniais nusikaltimais** srityje, nes tarp bendrų kibernetinio saugumo veiksmų ir teisėsaugos veiksmų reaguojant į kibernetinio saugumo incidentus yra daug panašumų. Komisija skatina valstybes nares diskutuoti apie tokias

[77] Inicijuotos naujos Europos partnerystės, skirtos ES skaitmeninio dešimtmečio užmojams įgyvendinti | Europos skaitmeninės ateities formavimas (europa.eu), kurios sukurtos pagal Įgūdžių paktą siekiant spręsti informacinių ir ryšių technologijų (IRT) specialistų trūkumo problemą.

[78] ES šalys įsipareigoja skatinti moterų dalyvavimą skaitmeninėje ekonomikoje | Europos skaitmeninės ateities formavimas (europa.eu).

[79] 2021 m. birželio 24 d. Europos Parlamento ir Tarybos reglamento (ES) 2021/1057, kuriuo nustatomas „Europos socialinis fondas +“ (ESF+) ir panaikinamas Reglamentas (ES) Nr. 1296/2013, 4 straipsnio 1 dalies c punktas.

[80] TIS 2 direktyvos 7 straipsnio 2 dalies f punktas.

[81] Ataskaita - „Cyber Conscription: Experience and Best Practice from Selected Countries“, Martin Hurt ir Tiia Sõmer, Tarptautinis gynybos ir saugumo studijų centras, 2021 m. vasario mėn.

iniciatyvas ir įvertinti, kaip kvalifikuoti darbuotojai galėtų geriausiai pasitarnauti gynybos ir civilinėms kibernetinio saugumo bendruomenėms.

Komisija apsvarstys pasiūlymus, kaip pašalinti esamas ir numatomas spragas, nustatytas jai atliekant ES institucijų, įstaigų, organų ir agentūrų poreikių peržiūrą. Ji visų pirma skatins darbuotojus dalyvauti būsimoje **ES ir Jungtinių Amerikos Valstijų (JAV) kibernetinio saugumo stažuotėje**, įkurtoje ES ir JAV dialogo metu.

Veiksmai įgyvendinant Akademiją

Pramonės atstovai

- Nuo 2023 m. balandžio 18 d. pasiūlys konkrečius **įsipareigojimus dėl kibernetinio saugumo** Skaitmeninių įgūdžių ir užimtumo platformoje.

Valstybės narės

- **Nacionalinėse kibernetinio saugumo strategijose** numatys konkrečias priemones kibernetinio saugumo srities įgūdžių trūkumui mažinti.

Valstybės narės ir pramonės atstovai

- Iki 2030 m. įgyvendins deklaraciją „Moterys skaitmeninėje ekonomikoje“ ir pasieks **lyčių konvergenciją kibernetinio saugumo darbo vietose**.

6. Finansavimas. Sinergijos kūrimas siekiant kuo labiau padidinti kibernetinio saugumo įgūdžių ugdymo išlaidų poveikį

Įgyvendinant Akademiją investicijų į kibernetinio saugumo įgūdžius poveikis bus padidintas sukuriant bendrą prieigą, sudarant sąlygas geriau nukreipti lėšas pagal rinkos poreikius ir racionalizuojant finansavimo naudojimą, skatinant skirtingų priemonių sinergiją ir vengiant pastangų pasikartojimo[82].

6.1. Lėšų ir poreikių derinimas

Įgyvendinant Akademiją ECCC, remiamas Komisijos, ECCO projekto ir nacionalinių koordinavimo centrų, rinks **informaciją apie tai, kaip ES lėšos naudojamos kibernetinio saugumo įgūdžių ugdymui finansuoti**, ir vertins, kaip ES lėšomis remiamas kibernetinio saugumo įgūdžių trūkumo mažinimas. Atsižvelgdamas į šią apibendrintą informaciją, ECCC sieks užtikrinti, kad ES lėšos būtų geriau panaudojamos nustatytiems poreikiams patenkinti. Jis finansuos veiksmus, kuriais būtų šalinamos aktualiausios kibernetinio saugumo darbo jėgos spragos, įskaitant tas, kurios susijusios su kibernetinio saugumo politikos poreikių įgyvendinimu.

6.2. Turimų lėšų ir partnerystės iniciatyvų, skirtų kibernetinio saugumo įgūdžiams ugdyti, matomumo užtikrinimas

Trumpuoju laikotarpiu **Skaitmeninių įgūdžių ir užimtumo platforma** taps bendru prieigos punktu visiems suinteresuotiesiems subjektams, ir jame bus prieinama visa informacija apie kibernetinio saugumo įgūdžių ugdymo finansavimo galimybes.

[82] Finansavimo galimybės (europa.eu). Paramos įgūdžių paktui tarnyba teikia bendrą prieigą prie informacijos apie įgūdžių ugdymo finansavimą, įskaitant skaitmeninės ekosistemos finansavimą. Paramos paktui tarnyba teikia bendrą informaciją apie finansavimo priemones, kurios nėra skirtos tik kibernetinio saugumo įgūdžiams ugdyti, tačiau Akademija vis tiek turėtų atsižvelgti į jos darbą, kad būtų išvengta pasikartojimo.

ES investuoja į žmones ir jų įgūdžius ir pasitelkia partnerystes, ypač su pramonės atstovais, kad organizuotų kvalifikacijos kėlimo ir perkvalifikavimo veiksmus, naudodamasi keliomis priemonėmis, nustatytomis pagal **Europos įgūdžių darbotvarkę**[83], visų pirma pagal **Įgūdžių paktą**[84] ir **Skaitmeninio švietimo veiksmų planą**[85]. Pagal **Skaitmeninės Europos programą** finansuojamos kibernetinio saugumo įgūdžių galimybės, konkrečiai, įgyvendinant daugiašalių projektų iniciatyvas, aiškiai papildančias programos „Europos horizontas“ paramą moksliniams tyrimams ir novatoriškiems technologiniams sprendimams kibernetinio saugumo srityje. **Europos gynybos fondas**[86] finansuoja mokslinius tyrimus ir technologijų plėtrą siekiant vykdyti veiksmingas kibernetines operacijas, įskaitant mokymus ir pratybas[87]. Tokios iniciatyvos toliau bus remiamos pagal programą **„Erasmus +“**, be kita ko, vykdant mišriąsias intensyvias programas ir bendradarbiavimo projektus.

Valstybės narės raginamos sutelkti tiesiogiai valdomas ES lėšas kibernetinio saugumo įgūdžiams ir darbo vietoms remti. Sanglaudos politikos fondai, pavyzdžiui, **Europos regioninės plėtros fondas (ERDF)** ir **ESF+**, turi didelį potencialą užtikrinti sinergiją šiuo klausimu[88]. Veiksmai pagal **Ekonomikos gaivinimo ir atsparumo didinimo priemonę** (RRF)[89] ir programą **„InvestEU“**[90] svariai papildo pastangas įgyvendinti Akademijos tikslus.

Veiksmai įgyvendinant Akademiją

Europos kibernetinio saugumo kompetencijos centras ir ENISA

- Iki 2024 m. pabaigos **susies** esamą finansavimą, skirtą kibernetinio saugumo įgūdžiams, su rinkos poreikiais, įvertins **veiksmingumą** ir nustatys finansavimo **prioritetus**.

Komisija

- Iki 2023 m. pabaigos sukurs kibernetinio saugumo įgūdžių finansavimo galimybėms skirtą **bendrą prieigos punktą** Skaitmeninių įgūdžių ir užimtumo platformoje.

7. Pažangos vertinimas. Integruota atskaitomybė

Įgyvendinant Akademiją bus parengta **metodika, pagal kurią bus galima įvertinti pažangą, padarytą siekiant panaikinti kibernetinio saugumo įgūdžių trūkumą**.

[83] Europos įgūdžių darbotvarkė. Užimtumas, socialiniai reikalai ir įtrauktis. Europos Komisija (europa.eu).

[84] ES finansavimo priemonės, skirtos kvalifikacijos kėlimui ir perkvalifikavimui. Užimtumas, socialiniai reikalai ir įtrauktis. Europos Komisija (europa.eu).

[85] 2021–2027 m. skaitmeninio švietimo veiksmų planas.

[86] 2021 m. balandžio 29 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/697, kuriuo įsteigiamas Europos gynybos fondas ir panaikinamas Reglamentas (ES) 2018/1092.

[87] Valstybės narės yra įsipareigojusios rengti bendrus mokymus ir pratybas, pavyzdžiui, rengdamos ir dalyvaudamos nuolatinio struktūrizuoto bendradarbiavimo (PESCO) kibernetinių mokymų ir pratybų projektuose, kaip antai ES kibernetinis mokslinės kompetencijos ir inovacijų centras (ES CAIH) ir Kibernetinių poligonų federacija.

[88] Reglamento (ES) 2021/1058 3 straipsnio 1 dalis ir Reglamento (ES) 2021/1057 4 straipsnio 1 dalies g punktas.

[89] Pavyzdžiui, pagal Estijos ekonomikos gaivinimo ir atsparumo didinimo planą numatoma, kad investicijos (10 mln. EUR) į skaitmeninius įgūdžius bus skirtos IRT specialistams skirtiems mokymams tobulinti, IRT specialistų kvalifikacijos kėlimui ir perkvalifikavimui kibernetinio saugumo srityje finansuoti ir padės rengti bandomąją programą, skirtą IRT specialistų kvalifikacijos sistemai pertvarkyti.

[90] Suinteresuotieji subjektai (pvz., mokymo paslaugų teikėjai ir įmonės, norinčios kurti arba patobulinti savo kibernetinio saugumo mokymus) gali kreiptis į „InvestEU“ konsultacijų centrą, kuris projektų rengėjams ir subjektams teikia techninę paramą ir pagalbą, be kita ko, dėl gebėjimų stiprinimo, ir ieškoti informacijos „InvestEU“ portale.

7.1.Kibernetinio saugumo rodiklių nustatymas siekiant stebėti kibernetinio saugumo darbo rinkos raidą

Naudojant **skaitmeninės ekonomikos ir visuomenės indeksą (DESI)**, apibendrinami Europos skaitmeninimo veiklos rodikliai ir stebima ES valstybių narių pažanga. Įgyvendinant Kibernetinio saugumo įgūdžių akademiją, ENISA, bendradarbiaudama su Komisija ir TIS bendradarbiavimo grupe[91] ir konsultuodamasi su susijusiais rinkos dalyviais ir nacionaliniais koordinavimo centrais, parengs **rodiklius,** be kita ko, susijusius su lytimi, kad būtų galima sekti ES valstybėse narėse padarytą pažangą siekiant padidinti kibernetinio saugumo specialistų skaičių. ENISA remsis DESI metodika[92] ir užtikrins, kad rodikliai atitiktų Europos skaitmeninius tikslus dėl IRT specialistų ir dėl lyčių konvergencijos užtikrinimo IRT srityje. Tada Komisija sieks įtraukti tokius rodiklius į DESI**,** kad būtų galima kasmet sekti kibernetinio saugumo įgūdžių ir darbo rinkos padėtį.

7.2.Duomenų rinkimas ir ataskaitų teikimas

ENISA, naudodamasi parama pagal ECCO projektą ir padedama nacionalinių koordinavimo centrų, rinks duomenis apie rodiklius. Remdamasi surinktais duomenimis ENISA parengs **metinę ataskaitą**, į kurią bus atsižvelgta rengiant Skaitmeninio dešimtmečio pažangos ataskaitą[93], o pastaraja kartu su DESI bus toliau remiamasi rengiant **Europos semestro** konkrečioms šalims skirtą analizę ir rekomendacijas[94]. Be to, kibernetinio saugumo įgūdžių rodikliais ENISA naudosis, **kas dvejus metus** rengdama TIS 2 direktyvoje numatytą kibernetinio saugumo būklės Sąjungoje ataskaitą, kurioje bus aptariami kibernetinio saugumo pajėgumai, informuotumas apie jį ir su juo susiję įpročiai ES.

7.3.Kibernetinio saugumo pagrindinių veiklos rezultatų rodiklių (PVRR) rengimas

Siekdama pašalinti Europos kibernetinio saugumo srities talentų trūkumą, ENISA, glaudžiai bendradarbiaudama su Komisija ir nacionaliniais koordinavimo centrais, pasiūlys Komisijai PVRR, parengtus naudojant 2030 m. Skaitmeninio dešimtmečio politikos programos metodiką ir verslo patirtį. ENISA deramai atsižvelgs į PVRR, kuriuos valstybės narės naudoja savo nacionalinėms kibernetinio saugumo strategijoms įvertinti[95].

<u>Veiksmai įgyvendinant Akademiją</u>

ENISA

- Iki 2023 m. pabaigos parengs kibernetinio saugumo įgūdžių **rodiklius ir PVRR**.
- **Surinks duomenis** apie rodiklius ir apie juos praneš (pirmą kartą duomenys bus surinkti iki 2025 m.).

Komisija

- Dirbs siekdama įtraukti **kibernetinio saugumo rodiklius į DESI** ir **Skaitmeninio dešimtmečio pažangos ataskaitą**.

[91] Remiantis metodika, kurią turi sukurti ENISA kas dvejus metus teikiamos kibernetinio saugumo padėties Sąjungoje ataskaitos reikmėms pagal TIS 2 direktyvos 18 straipsnio 3 dalį, ir ją papildant.

[92] Žr. metodologinę pastabą dėl 2022 m. skaitmeninės ekonomikos ir visuomenės indekso (DESI), pasiekiamą adresu Skaitmeninės ekonomikos ir visuomenės indeksas (DESI) | Europos skaitmeninės ateities formavimas (europa.eu).

[93] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos sprendimas (ES) 2022/2481, kuriuo nustatoma 2030 m. skaitmeninio dešimtmečio politikos programa.

[94] Ten pat, 25 konstatuojamoji dalis.

[95] TIS 2 direktyvos 7 straipsnio 4 dalis.

8. Išvada

Šiuo komunikatu numatytos pamatinės priemonės, padėsiančios pertvarkyti ES požiūrį į ES specialistų kibernetinio saugumo įgūdžių ugdymą. Siekiama sumažinti kibernetinio saugumo įgūdžių trūkumą ir aprūpinti ES reikiamais darbuotojais, kad ji galėtų reaguoti į nuolat kintančią grėsmių padėtį, įgyvendinti ES politiką, kuria siekiama apsaugoti ES nuo kibernetinių išpuolių, taip pat didinti verslo galimybes ir konkurencingumą. Kvalifikuota kibernetinio saugumo darbo jėga gali būti naudinga **civilinėms, gynybos, diplomatinėms ir teisėsaugos** bendruomenėms, ir palengvinti jų sinergiją.

Komisija ragina valstybes nares ir visus suinteresuotuosius subjektus įgyvendinti Kibernetinio saugumo įgūdžių akademijos užmojus.