EIROPAS
KOMISIJA

Strasbūrā, 18.4.2023.
COM(2023) 207 final

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

Kiberdrošības talantu deficīta pārvarēšana ES konkurētspējas, izaugsmes un noturības vairošanai
(“Kiberdrošības prasmju akadēmija”)

Kiberdrošības talantu deficīta pārvarēšana ES konkurētspējas, izaugsmes un noturības vairošanai
("Kiberdrošības prasmju akadēmija")

1. Neatliekama vajadzība mazināt risku, novēršot kiberdrošības prasmju deficītu un nepietiekamību

Kiberdrošība nav tikai pilsoņu, uzņēmumu un dalībvalstu drošības sastāvdaļa. Tai ir arī jānodrošina ES politiskā stabilitāte, valstu demokrātijas stabilitāte un sabiedrības un uzņēmumu uzplauksme. Kiberdrošības **apdraudējuma aina** pēdējos gados ir ievērojami mainījusies, ņemot vērā satraucošo tendenci arvien vairāk kiberuzbrukumu ES vērst pret kritisko militāro un civilo infrastruktūru. Apdraudētāji vairo savas spējas, un parādās jaunas, hibrīdiskas un novatoriskas briesmas, piemēram, mākslīgajā intelektā balstītu robotu un paņēmienu izmantošana[1]. Apdraudētāji struktūrām rada ievērojamu kaitējumu gan finansiālā, gan reputācijas ziņā, sevišķi ar izspiedējprogrammām[2].

Daudz kiberdrošības incidentu tiek vērsts arī uz dalībvalstu valsts pārvaldi un valdību, kā arī uz Eiropas iestādēm, struktūrām un aģentūrām (*EUIBA*)[3]. Uzbrukumi nemitīgi tiek virzīti[4] arī uz finansēm[5] un veselības aprūpi[6], kas ir sabiedrības un ekonomikas pamats. Ģeopolitiskā spriedze, ko izraisījis Krievijas iebrukums Ukrainā, ir palielinājusi kiberdrošības apdraudējumu[7] un var destabilizēt mūsu sabiedrību. ES **drošību** nevar garantēt bez **ES vislielākās vērtības – tās cilvēkiem.** ES steidzami vajadzīgi speciālisti ar prasmēm un iemaņām novērst, atklāt, apturēt kiberuzbrukumus un no tiem aizsargāt ES, ieskaitot tās kritiskāko infrastruktūru, un nodrošināt tai **noturību**.

Talantu deficīts kiberdrošībā vēl vairāk iegrožo Eiropas **konkurētspēju** un **izaugsmi**, kas lielā mērā atkarīgas no stratēģisko digitālo tehnoloģiju (mākslīgā intelekta, 5G, mākoņdatošanas u. c.) izstrādes un ieviešanas. Ir vajadzīgi prasmīgi kiberdrošības kadri, lai arī turpmāk ES spētu globālā vidē nodrošināt svarīgas progresīvas tehnoloģijas.

Lai sagatavotos un pretotos mainīgajam apdraudējumam un veicinātu ES konkurētspēju, ES kiberdrošības politika pēdējos gados ir gājusi uz priekšu un ir pieņemtas vairākas iniciatīvas,

---

[1] *ENISA Threat Landscape 2022 – ENISA* (europa.eu).

[2] *Europol Internet Organised Crime Threat Assessment (IOCTA) 2021*. Tādi darboņi balstās uz modeli "izspiedējprogrammatūra kā pakalpojums". 2022. gadā uzņēmumu gada izmaksas pārsniedza 18,4 miljardus euro (*Cybereason 2022 Report on the true cost or Ransomware*).

[3] Sk., piem., *Joint Publication by ENISA and CERT-EU, JP-23-01 – Sustained activity by specific threat actors, TLP:CLEAR, 15 February 2023*.

[4] *ENISA Threat Landscape 2022*.

[5] Sk., piem., Vācijā, kur 90 % krāpšanas pastā, par ko ziņots no 2021. gada 1. jūnija līdz 2022. gada 31. maijam, bijusi finansiāla pikšķerēšana jeb uzbrukums finanšu nozares uzņēmumiem, kurā bijis iesaistīts vairāk nekā 20 000 inficētu ierīču 125 valstīs, *The State of IT Security in Germany in 2022, Bundesamt für Sicherheit in der Informationstechnik (BSI), 1st of January 2023*.

[6] Sk., piem., Francijā, kur notikuši izspiedējprogrammas uzbrukumi valsts veselības aprūpes iestādēm, piem., "Centre Hospitalier Sud Francilien", kuros apdraudētājs aizskāris un publiskojis 11 GB persondatu un medicīnisko datu, kā arī ar personālu saistītus datus, *Panorama de la cybermenace 2022, Agence nationale de la sécurité des systèmes d'information (ANSSI), janvier 2023*.

[7] Sk. arī: *CERT-EU – Russia's war on Ukraine: one year of cyber operations* (europa.eu); Krievijas kiberdarbības pret Ukrainu. Eiropas Savienības vārdā sniegta Augstā pārstāvja deklarācija, 2022. gada 10. maijs; Eiropas Savienības vārdā sniegta Augstā pārstāvja deklarācija par launprātīgām kiberdarbībām, ko hakeri un hakeru grupas veic saistībā ar Krievijas agresiju pret Ukrainu, 2022. gada 19. jūlijs.

piemēram, ES kiberdrošības stratēģija digitālajai desmitgadei[8], pārskatītā Tīklu un informācijas drošības direktīva (TID2 direktīva)[9], ES nozaru kiberdrošības tiesību akti[10], ES kiberaizsardzības politika[11], Kibernoturības akts[12] un Kibersolidaritātes akts, ko Komisija ierosinājusi kopā ar šo paziņojumu. Taču mērķus šie tiesību akti nesasniegs bez kvalificētiem darbiniekiem, kas vajadzīgi to īstenošanai. Iedzīvotāju kopuma pamatzināšanas kiberdrošībā tiek risinātas iniciatīvās, kas atbalsta dzīvei sabiedrībā vajadzīgo vispārīgo prasmju attīstību[13], taču gan publiskajā, gan privātajā sektorā valstu un ES līmenī, arī standartizācijas organizācijās, būtisks kompetents ir kadri, **kas izpildītu minētās juridiskās un politiskās kiberdrošības prasības**.

Tāpēc ES drošība un konkurētspēja ir atkarīga no profesionāli kvalificētiem kiberdrošības kadriem. ES tomēr saskaras ar ļoti būtisku kvalificētu kiberdrošības speciālistu deficītu, kas ES, dalībvalstis, uzņēmumus un pilsoņus pakļauj kiberdrošības incidentu briesmām. 2022. gadā kiberdrošības speciālistu deficīts Eiropas Savienībā bija **260 000**[14] **un 500 000**[15] robežās, taču ir aprēķināts, ka vajadzīgs ap 883 000 ES kiberdrošības kadru[16], un tas liek domāt, ka pieejamās prasmes nav pieskaņotas darbaspēka tirgus vajadzībām. Kiberdrošības kadri turpina ciest no maldīga priekšstata par šās jomas "tehniskumu", tāpēc joprojām nespēj piesaistīt **sievietes**, kas ir 20 % kiberdrošības absolventu[17] un 19 % informācijas un komunikācijas tehnoloģiju (IKT) speciālistu[18]. Lai šo problēmu atrisinātu, **Eiropas Digitālās desmitgades politikas programmā 2030. gadam**[19] ir izvirzīts mērķis līdz 2030. gadam palielināt IKT speciālistu skaitu par 20 miljoniem, panākot arī dzimumu vienādāku pārstāvību. Bez tam jaunās ES politikas īstenošanai ir vajadzīgi pietiekami kvalificēti un skaitliski pietiekami kadri. Piemēram, vairāk nekā 42 % finansiālo pakalpojumu nozares vecāko IT vadītāju akcentē kiberdrošības prasmju un lietpratības trūkumu kā galveno problēmu, ar ko viņu saimnieciskā darbība saskarsies kiberdrošības aizsardzības un incidentu

[8] Kopīgs paziņojums Eiropas Parlamentam un Padomei " ES kiberdrošības stratēģija digitālajai desmitgadei" (JOIN/2020/18 final).

[9] Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris) par pasākumiem nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID2 direktīva).

[10] Kā Eiropas Parlamenta un Padomes Regula (ES) 2022/2554 (2022. gada 14. decembris) par finanšu nozares digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 (*DORA* regula) finanšu nozarē.

[11] Kopīgs paziņojums Eiropas Parlamentam un Padomei "ES kiberaizsardzības politika" (JOIN/2022/49 final).

[12] Priekšlikums – Eiropas Parlamenta un Padomes Regula par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulu (ES) 2019/1020 (COM(2022) 454 final).

[13] Starp attiecīgajām iniciatīvām, kas vērstas uz iedzīvotāju vispārīgajām digitālajām prasmēm: Eiropas sociālo tiesību pīlāra rīcības plāna un Digitālā kompasa, Digitālās izglītības rīcības plāna 2021.–2027. gadam, digitālās pratības satvara rīka un Padomes ieteikuma priekšlikuma par digitālo prasmju nodrošināšanas uzlabošanu izglītībā un apmācībā mērķrādītājs – 80 % iedzīvotāju līdz 2030. gadam ir apguvuši digitālās pamatprasmes.

[14] "(ISC)²" seminārā *Assessing Cyber Skills on the basis of the ECSF, ENISA webinar, 16 February 2023*.

[15] Pēc Eiropas Kiberdrošības organizācijas (*ECSO*) uzskatiem, kā nosaka Kopīgs paziņojums Eiropas Parlamentam un Padomei "ES kiberaizsardzības politika" (JOIN/2022/49 final).

[16] "(ISC)²" seminārā *Assessing Cyber Skills on the basis of the ECSF, ENISA webinar, 16 February 2023*.

[17] *Cybersecurity Higher Education Database (CyberHEAD)*.

[18] Tikai 19 % IKT speciālistu ES ir sievietes, Digitālās ekonomikas un sabiedrības indekss (DESI) 2022. gadā | Eiropas digitālās nākotnes veidošana (europa.eu). Nav pieejamu skaitļu par sievietēm Savienības kiberdrošības kadru vidū.

[19] Eiropas Parlamenta un Padomes Lēmums (ES) 2022/2481 (2022. gada 14. decembris), ar ko izveido Digitālās desmitgades politikas programmu 2030. gadam, kas izveido uzraudzības un sadarbības mehānismu, lai sasniegtu 2030. gada digitālajā kompasā noteiktos Eiropas digitālās pārveides kopīgos mērķus un mērķrādītājus, arī prasmju jomā.

pārvaldības jomā[20] laikā, kad būs jāīsteno nozaru kiberdrošības tiesību akti, piemēram, Digitālās darbības noturības akts (*DORA*).

Darbaspēka tirgu vēl vairāk ierobežo darba devēju vilcināšanās ieguldīt cilvēkkapitālā un jau apmācītu un pieredzes bagātu kadru meklēšana[21]. Šis trūkums ietekmē visu veidu uzņēmumus, ieskaitot mazos un vidējos (**MVU**), kādu ir 99 % no visiem ES uzņēmumiem[22]. Šī problēma ir liela arī **publiskās pārvaldes** iestādēs, ko kiberdrošības incidenti ir smagi skāruši un visvairāk ietekmējuši[23].

Līdz ar to ir steidzami jāpārvar ES kiberdrošības profesionālo talantu deficīts, jo uz spēles ir ES drošība un konkurētspēja.

2. Sinerģijas un koordinācijas trūkums kiberdrošības prasmju deficīta pārvarēšanā

Eiropas un valstu līmenī tiek īstenotas publisku un privātu struktūru iniciatīvas, kas domātas kiberdrošības darbaspēka tirgus nepilnību pārvarēšanai. Taču tās notiek izklaidus un pagaidām nav sasniegušas īstām pārmaiņām vajadzīgo kritisko masu.

Vispirms jāsaka, ka pašlaik nav pietiekami vienotas izpratnes par ES kiberdrošības kadru sastāvu un attiecīgajām prasmēm – bet līdzīgiem kiberdrošības speciālistu profiliem taču būtu vajadzīgs viens un tas pats prasmju kopums. Tā kā attiecīgie dalībnieki maz izmanto vienotu **Eiropas atsauces satvaru kiberdrošības speciālistiem**, trūkst rīka saziņai starp darba devējiem, izglītotājiem un politikas veidotājiem un spējas veikt mērījumus un novērtēt kiberdrošības darbaspēka tirgus nepilnības. Tas arī neļauj izstrādāt izglītības un apmācības programmas un radīt karjeras veidošanas iespējas, kas atbilstu politikas un tirgus vajadzībām tiem, kuri vēlas strādāt šajā profesijā. Kadru **prasmju pilnveide un pārkvalifikācija** lielā mērā atkarīga no kiberdrošības apmācības un apliecinājumiem, ko parasti piedāvā privāti pakalpojumu sniedzēji. Tomēr kadriem ir grūti iegūt izpratni par piedāvātās kiberdrošības apmācības un tās apliecinājumu kvalitāti.

Lai gan izglītība un apmācība un karjeras veidošanas iespējas ir nepieciešamas piedāvājuma uzlabošanai darbaspēka tirgū, pašlaik netiek diez ko augsti vērtēta **pieprasījuma** loma kadru apmācībā un pielāgošanās tā attīstībai. Nozares un publiskā sektora darba devējiem trūkst kopīgu forumu un vietu, kur sakopot domas par to, kā vislabāk apmācīt kadrus un kā **labāk novērtēt prasmes**, it īpaši – līgstot darbiniekus. Vispieprasītākās **pamatprasmes** var būt saistītas ar kiberdrošību[24], piemēram, programmatūras izstrādi vai mākoņdatošanu[25], taču joprojām nepamatoti tiek ignorētas **caurviju prasmes**. Kritiskā domāšana un analīze, problēmu risināšana un pašvadība ir prasmju grupas, kuras darba devēji pieprasa vairāk[26] un kuras kļūst arvien svarīgākas, nākot 2025. gadam[27].

Kiberdrošības prasmju jomā jau pastāv daudzas publisko un privāto ieguldījumu iniciatīvas, un projektus ES plaši **apmaksā** no dažādiem instrumentiem[28]. Tomēr pastāvīgais prasmju

---

[20] *S-RM Cyber Security Insights Report 2022*.

[21] *Cybersecurity Skills Development in the EU, ENISA, December 2019*.

[22] MVU definīcija (europa.eu).

[23] *ENISA Threat Landscape 2022 – ENISA* (europa.eu)

[24] *LinkedIn 2023 Most In-Demand Skills: Learn the Skills Companies Need Most*.

[25] *ISACA State of Cyber Security 2022 infographic*.

[26] Piem., *Cedefop* rīks: *Skills-OVATE | Cedefop* (europa.eu)

[27] *The Future of Jobs Report, October 2020, World Economic Forum*.

[28] Piemēram: *Cybersecurity Skills Alliance – New Vision for Europe – REWIRE project* (finansē programma "Erasmus+"); projekti, kas atbalsta Kiberdrošības kompetences centru (*ECHO*, *CONCORDIA*, *CyberSec4Europe*, *SPARTA* (finansē "Apvārsnis 2020"), *Cybersecpro project* (finansē Eiropas Digitalizācijas programma).

deficīts Eiropas Savienībā rada jautājumus par to pamanāmību un ietekmi un liek domāt, ka sistemātiski tās var neatbilst tirgus vajadzībām, kuras tad steidzami jākartē ES līmenī. Vairāki finansējuma avoti pie tam rada dublēšanos, un tiem trūkst iespējas paplašināties un panākt kārtīgu ietekmi. Turklāt tie, kuriem ir vajadzīgs ieguldījums, ne vienmēr spēj noteikt viņu vajadzībām piemērotākos avotus.

Ieinteresētās personas ir centušās risināt sarežģīto un daudzšķautņaino jautājumu par kiberdrošības prasmju deficītu. ES Kiberdrošības aģentūra (*ENISA*) ir izstrādājusi instrumentus, kas attiecas uz funkciju profiliem vai augstāko izglītību[29], Eiropas Kiberdrošības kompetences centrs (*ECCC*)[30] īpašā darba grupā risina kiberdrošības prasmju jautājumus, Eiropas Drošības un aizsardzības koledža (EDAK) nodarbojas ar civilo un militāro kadru kiberdrošības prasmēm kopīgās drošības un aizsardzības politikas[31] kontekstā, šo jautājumu cenšas risināt privātas organizācijas [32], kiberdrošības sertifikācijas nozare izstrādā ceļvedi un apmācību, kam jāaizpilda robi prasmēs[33]. Dalībvalstis arī cenšas šo jautājumu risināt ar dažādām iniciatīvām, sākot ar regulējumu[34] un beidzot ar kiberdrošības prasmju akadēmiju[35] vai kibermītņu[36] izveidi, kibernoziedzības profilakses izcilības centriem[37] vai publiskā un privātā sektora partnerībām[38]. Tomēr visu ieinteresēto personu darbam palaikam trūkst koordinācijas un sinerģijas un tas neīsteno potenciālu darbaspēka tirgū ienest būtiskas pārmaiņas – par to liecina ES augošais kiberdrošības kadru deficīts. Ir jāpalielina arī kiberkopienu sinerģija, jo kiberdrošības uzturēšanai, **kibernoziedzības** apkarošanai un **kiberaizsardzības** reaģētspējai vajadzīgās prasmes mēdz būt līdzīgas.

Visbeidzot, patlaban ES rīcībā esošie līdzekļi ir par trūcīgiem **kiberdrošības darbaspēka tirgus stāvokļa un attīstības** un kadru prasmju novērtēšanai. Dalībvalstis un *EUIBA* balstās uz privātu struktūru savāktiem datiem vai plašāku ES savāktu datu kopumu, sevišķi *Eurostat*[39] un Eiropas Profesionālās izglītības attīstības centra (*Cedefop*)[40] datiem par IKT speciālistiem. Citiem vārdiem sakot, ES ir nepilnīgs un neviengabalains priekšstats par vajadzībām, un tas tai neļauj vispusīgi aptvert stāvokli kiberdrošības darbaspēka tirgū.

3. Visā ES koordinēta reaģēšana – Kiberdrošības prasmju akadēmija

3.1. Mērķis

Lai risinātu kiberdrošības prasmju problēmas un pārvarētu deficītu darbaspēka tirgū, Komisija mudina veidot **Kiberdrošības prasmju akadēmiju**, par ko Eiropas Komisijas

---

[29] Galvenie: Eiropas kiberdrošības prasmju satvars (*ECSF*); *CYBERHEAD – Cybersecurity Higher Education Database*; *Cyber Exercise Platform (CEP)*; *European Cyber Security Challenge*; *European Cyber Security Month*.

[30] Eiropas Parlamenta un Padomes Regula (ES) 2021/887 (2021. gada 20. maijs), ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu.

[31] Sevišķi kiberjomas izglītības, apmācības, izvērtēšanas un mācību platforma (*ETEE*).

[32] Piemēram, Eiropas Kiberdrošības organizācijas (*ECSO*) 5. darba grupa "Izglītība, apmācība, informētība, kibertelpas, cilvēkfaktori"; organizācija *Digitaleurope*.

[33] Piemēram, *SANS Institute*, "(ISC)²", *ISACA*.

[34] Piemēram, valstu izglītības vai kiberdrošības stratēģijās.

[35] Piemēram, *C-Academy* Portugālē.

[36] Piemēram, *Cyber Campus* Francijā.

[37] Piemēram, Lietuvas Kibernoziedzības apkarošanas prasmju un izpētes izcilības centrs ("L3CE").

[38] Piemēram, *Microsoft's Cybersecurity Skilling Initiative*.

[39] *ICT specialists in employment – Statistics Explained* (europa.eu).

[40] Piem., *Cedefop* rīks *Skills-OVATE | CEDEFOP* (europa.eu).

priekšsēdētāja Eiropas Prasmju gada sakarā paziņojusi 2022. gada nodomu vēstulē[41, 42] par stāvokli Savienībā.

Kiberdrošības prasmju akadēmijas (saīsināti – "Akadēmija") mērķis ir izveidot **vienotu piekļuves punktu un sinerģiju** kiberdrošības izglītības un apmācības piedāvājumiem, kā arī finansēšanas iespējām un specifiskiem kiberdrošības prasmju izkopšanas atbalsta pasākumiem. Tā paplašinās ieinteresēto personu iniciatīvas, lai sasniegtu kritisko masu, kas radīs pārmaiņas darbaspēka tirgū, arī militārajā jomā. Lai panāktu plašāku ietekmi, pasākumi būs pieskaņoti kopīgajiem mērķiem un galvenajiem snieguma rādītājiem.

Akadēmija koncentrēsies uz **kiberdrošības speciālistu** prasmju veidošanu. Akadēmijas darbība tiks izmantota ES kiberdrošības politikā, kā arī izglītībā un mūžizglītībā. Tas papildina divus Padomes ieteikumus par digitālo izglītību un prasmēm, kurus Komisija ierosināja reizē ar šo paziņojumu[43].

Akadēmija balstīsies uz četriem pīlāriem: 1) **izglītojot un apmācot veicināt zināšanu radīšanu** ar izstrādātu vienotu satvaru kiberdrošības funkciju profiliem un ar tiem saistītajām prasmēm, uzlabot Eiropas izglītības un apmācības piedāvājumu, lai apmierinātu vajadzības, uzlabot karjeras veidošanas iespējas un nodrošināt kiberdrošības apmācības un to apliecinājumu pamanāmību un skaidrību, lai uzlabotu darbaspēka piedāvājumu; 2) nodrošināt pieejamo **finansēšanas iespēju** labāku pamanāmību un novirzīšanu ar prasmēm saistītai darbībai, lai maksimalizētu to ietekmi; 3) aicināt ieinteresētās personas **uz rīcību**; 4) noteikt rādītājus **tirgus attīstības uzraudzīšanai** un savu pasākumu efektivitātes novērtēšanai.

Akadēmijas īstenošanu atbalstīs 10 miljonu euro finansējums no programmas "Digitālā Eiropa" (*DEP*)[44].

3.2. Akadēmijas pārvalde

Lai nodrošinātu infrastruktūru, kas kalpo par **vienotu piekļuves punktu** sadarbības veicināšanai starp augstskolu mācībspēkiem, apmācības rīkotājiem un nozari, kur ES kiberdrošības ekosistēmas piedāvājuma un pieprasījuma puses varētu tikties un saņemt apmācību, beigu beigās Akadēmija varētu pārveidoties par **Eiropas digitālās infrastruktūras konsorciju (*EDIC*)**[45]. Tāds instruments ļautu dalībvalstīm kopīgi strādāt kiberdrošības prasmju deficīta pārvarēšanā, kā arī cieši sadarboties ar Komisiju, *ENISA* un Eiropas Kiberdrošības kompetences centru (*ECCC*) saskaņā ar to pilnvarām un kompetenci, kā arī iesaistīt visas attiecīgās ieinteresētās personas un virzīt Eiropas, valstu un privātos ieguldījumus uz kopīgu mērķi. Šim nolūkam ieinteresētās dalībvalstis tiek mudinātas līdz 2023. gada 30. maijam iesniegt Komisijai priekšpaziņojumu par gaidāmiem dalības pieteikumiem tādā *EDIC*. Brīvprātīgais priekšpaziņojums ļautu Komisijai laikus izteikt piezīmes par *EDIC* pieteikuma projektu, nodrošinot tā tālāku izstrādi un oficiālu iesniegšanu straujākā tempā. Visa procesa laikā un tādā mērā, kādā pieprasa dalībvalstis, Komisija, darbojoties par daudzvalstu projekta paātrinātāju, atvieglos *EDIC* pieteikuma sagatavošanu. Kad Komisija būs pieteikumu pozitīvi novērtējusi un Digitālās desmitgades programmas

[41] Nodomu vēstule priekšsēdētājai Robertai Metsolai un premjerministram Petram Fialam "Stāvoklis Savienībā 2022. gadā".

[42] Kopīgs paziņojums Eiropas Parlamentam un Padomei "ES kiberdrošības stratēģija digitālajai desmitgadei", JOIN/2022/49 final.

[43] Priekšlikumi – Padomes ieteikumi par galvenajiem faktoriem, kas veicina sekmīgu digitālo izglītību un apmācību un par digitālo prasmju nodrošināšanas uzlabošanu izglītībā un apmācībā.

[44] Eiropas Parlamenta un Padomes Regula (ES) 2021/694 (2021. gada 29. aprīlis), ar ko izveido programmu "Digitālā Eiropa" un atceļ Lēmumu (ES) 2015/2240.

[45] *EDIC* ieviesti ar Eiropas Parlamenta un Padomes Lēmuma (ES) 2022/2481 (2022. gada 14. decembris), ar ko izveido politikas programmu "Digitālās desmitgades ceļš" 2030. gadam, 13. un nāk. pantiem.

komiteja to būs apstiprinājusi, Komisija pieņems lēmumu par *EDIC* izveidi un pēc tam palīdzēs koordinēt *EDIC* īstenošanu[46].

Pa to laiku un kamēr *EDIC* tiks oficiāli veidots, Komisija ar Eiropas Kiberdrošības kopienas atbalsta (*ECCO*) projekta[47] atbalstu veidos virtuālu vienotu piekļuves punktu, uzlabojot Komisijas **Digitālo prasmju un darba vietu platformu**[48].

ENISA palīdzēs īstenot Akadēmiju saskaņā ar aģentūras mērķiem[49], sevišķi attiecībā uz palīdzību izglītībā un apmācībā kiberdrošības jomā, un ņemot vērā ziņošanas pienākumus, ko tai uzliek TID2 direktīva[50]. ***ECCC*** strādās saskaņā ar savu stratēģisko programmu, lai atbalstītu Kiberdrošības prasmju akadēmijas īstenošanu. Galvenais, *ECCC* īstenos programmas "Digitālā Eiropa" 3. stratēģisko mērķi (kiberdrošība). Tā saņems Komisijas un dalībvalstu atbalstu caur **nacionālajiem koordinācijas centriem (NKC)**. Attiecīgos gadījumos tiks iesaistīta ar TID2 direktīvu[51] izveidotā **sadarbības grupa**. Visbeidzot, lai sasniegtu Akadēmijas mērķi pārvarēt kiberdrošības prasmju deficītu, būs jāapvieno spēki ar **nozari** un **augstskolu mācībspēkiem**.

4. Zināšanu radīšana un apmācība – vienotas ES pieejas izveide apmācībai kiberdrošībā

Kiberdrošības prasmju akadēmijas zināšanu veidošanas un apmācības pīlārā tiks izstrādāta strukturēta pieeja ar skaidru mērķi ES palielināt to personu **skaitu**, kurām ir kiberdrošības prasmes, lai apmācības labāk piekārtotu **tirgus vajadzībām** un nodrošinātu **karjeras veidošanas iespēju** pamanāmību.

4.1. Runāt vienu valodu – ar vienotu pieeja kiberdrošības funkciju profiliem un ar tiem saistītajām prasmēm

ENISA jau ir strādājusi, lai noteiktu kiberdrošības speciālistu funkciju profilus saskaņā ar Eiropas kiberprasmju kompetences satvaru (***ECSF***)[52]. Tam jākļūst par pamatu, uz kura Akadēmija nosaka un novērtē attiecīgās prasmes, novēro prasmju deficīta mainību un norāda uz jaunām vajadzībām. Katrai *ECSF* kiberdrošības funkcijai kā profila apraksta elements[53] ir iekļauts piemērojamā Eiropas e-kompetences satvara kopums[54].

---

[46] Turpat, 12. pants.

[47] Sk. Eiropas Kiberdrošības kompetences centrs un tīkls – jauns ES apmaksāts projekts kiberkopienas atbalstīšanai (europa.eu). 2022. gada decembrī Eiropas Komisija parakstīja 3 miljonu euro līgumu par atbalstu ES Kiberkopienai Eiropas Kiberdrošības kompetences centrā. Šis projekts palīdzēs sasniegt ES mērķus, kas attiecas uz kopienu un spēju veidošanu kiberdrošības pētniecībā, inovācijā, ieviešanā un rūpnieciskajā bāzē.

[48] Mājas lapa | Digitālo prasmju un darba vietu platforma (europa.eu).

[49] "*ENISA* visā Savienībā atbalsta spēju veidošanu un uzlabo gatavību, palīdzot Savienības iestādēm, struktūrām, birojiem un aģentūrām, kā arī dalībvalstīm un publiskajām un privātajām ieinteresētajām personām .. attīstīt prasmes un kompetenci kiberdrošības jomā." Kiberdrošības akta 4. panta 3. punkts.

[50] TID2 direktīvas 18. pants.

[51] Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris) par pasākumiem nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID2 direktīva).

[52] Eiropas kiberdrošības prasmju satvars (*ECSF*) – *ENISA* (europa.eu). *ECSF* palīdz apzināt un formulēt uzdevumus, iemaņas, prasmes un zināšanas, kas saistās ar Eiropas kiberdrošības speciālistu funkcijām. Tajā visas ar kiberdrošību saistītās funkcijas ir apkopotas profilos, kas tiek individuāli analizēti, detalizēti skatot to attiecīgos pienākumus, prasmes, sinerģiju un savstarpējo atkarību.

[53] Par to sk. *User Manual – European Cybersecurity Skills Framework (ECSF) – September 2022*.

[54] Eiropas kiberprasmju kompetences satvars (*e-CF*) | *Esco* (europa.eu). Šis *e-CF* sniedz konsekventas saites nozares IKT kvalifikācijas un citu attiecīgu satvaru kontekstā, to vidū – *DigComp*.

Tāpēc *ENISA* pārskatīs *ECSF* un **noteiks kiberdrošības kadru mainīgās vajadzības un deficītu**, izmantojot arī progresīvus rīkus (piemēram, mākslīgo intelektu, lielos datus[55], datizraci). Šajā nolūkā *ENISA* strādās *EDIC* vadībā, kad tas būs izveidots – *ECCC* vadībā, kopā ar NKC, Komisiju, *ECCO* projektu un tirgus dalībniekiem[56]. Kiberaizsardzības kadru lietās *ENISA* pienācīgi ņems vērā EDAK paveikto darbu. Līdzīgā kārtā kibernoziedzības apkarošanas jomā *ENISA*, veidojot operatīvo apmācības vajadzību analīzi[57] par kiberuzbrukumiem, ņems vērā ES Tiesībaizsardzības apmācības aģentūras (*CEPOL*) un Eiropola veikumu.

Reizi divos gados Akadēmija *ECSF* regulāri papildinās un pārskatīs. Turklāt Komisija un Eiropas Ārējās darbības dienests ar ES aģentūru un struktūru, kā EDAK[58], Eiropola un *CEPOL*[59], atbalstu vajadzības gadījumā palīdzēs noteikt specifiskus nozaru profilus un ar tiem saistītas prasmes.

Tiks arī veidoti sakari starp *ECSF* un attiecīgajiem ES nodarbinātības politikas instrumentiem[60]. Tā, ***ESCO* klasifikācijā** tiks integrēti *ECSF* amatu profili, kā arī ar tiem saistītās prasmes. Tas uzlabos profesiju un prasmju klasifikāciju un saikni kiberdrošības jomā, atvieglojot cilvēkiem prasmju pilnveidi un pārkvalifikāciju un atbalstot prasmēm atbilstoša darba piemeklēšanu un pārrobežu mobilitāti.

4.2. Sadarbības veicināšana kiberdrošības izglītības un apmācības programmu izstrādē

Kad būs izveidots *EDIC*, Akadēmijai būs vajadzīgs atbalsts no dalībvalstīm, lai kļūtu par **Eiropas uzziņas centru kiberdrošības apmācības plānošanai un sniegšanai**, kas pievēršas vispieprasītākajām prasmēm un kiberdrošības ziņā inovatīvos uzņēmumos un kiberdrošības kompetences centros nodrošina apmācības un stažēšanās iespējas jaunuzņēmumiem un MVU, kā arī publiskās pārvaldes iestādēm. *EDIC* būs jāsadarbojas ar visām attiecīgajām ieinteresētajām personām, ieskaitot nozari, lai izstrādātu apmācību un balstītos uz tādiem projektiem kā programmas "Digitālā Eiropa" finansētais ***CyberSecPro***[61], kas apvieno 17 augstskolas un 13 drošības uzņēmumus no 16 dalībvalstīm, lai kļūtu par paraugpraksi visās kiberdrošības apmācības programmās.

Akadēmija sadarbosies ar visām attiecīgajām ieinteresētajām personām, lai darbam kiberdrošībā **piesaistītu jaunākās paaudzes**. Saskaņā ar Padomes ieteikuma priekšlikumu par to, kā uzlabot digitālo prasmju nodrošināšanu izglītībā un apmācībā, dalībvalstīm būtu jāizveido un jāpastiprina pasākumi, kas ļauj pieņemt darbā un apmācīt specializējušos

---

[55] Sk., piem., *Cedefop* izveidoto *Skills-OVATE*.

[56] Aģentūra turpinās izmantot citu ES finansētu projektu (piemēram, *REWIRE*, Prasmju datu telpa (*DS4S*), *CyberSecPro*, *Concordia*) rezultātus un metodiku, kas izriet no līdzīgām iniciatīvām (piemēram, *"Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom and United States"*, ESAO ziņojums, kas publicēts 2023. gada 21. martā), lai nākotnē nodrošinātu pašu jaunāko skatījumu uz vajadzībām vidē, kurā nemitīgi mainās pieprasījums.

[57] *CEPOL Operational Training Needs Assessment (OTNA)*.

[58] Par to sk. Kopīgo paziņojumu Eiropas Parlamentam un Padomei "ES kiberaizsardzības politika" (JOIN/2022/49 final).

[59] Šajā sakarā uzmanība tiks pievērsta noritošajam kibernoziedzības apmācības kompetences sistēmas (*TCF*) izstrādes darbam.

[60] Piem., Eiropas prasmju, kompetences, kvalifikācijas un profesiju klasifikācija (*ESCO*), *Europass*, Eiropas Nodarbinātības dienestu sadarbības tīkls (*EURES*).

[61] *CyberSecPro*. Piemēram, tas analizēs augstskolās piedāvātās kiberdrošības programmas, kursus un vasaras kursus un izmantotās Eiropas kredītpunktu pārneses un uzkrāšanas sistēmas (*ECTS*) vērtēšanas tabulas, nodrošinās mērķi vairāk nekā 530 praktikantu iesaistīt trīs gadu laikposmā, apmācīs ārpusniekus no dažādām nozarēm un sektoriem.

izglītotājus un apmācītājus un atvieglo kiberdrošības prasmju apguvi, cita starpā izmantojot māceklību. Būtu jāveicina kiberdrošības integrēšana izglītības un apmācības programmās, vienlaikus nodrošinot to pieejamību, **māceklības** un stažēšanās piedāvājuma attīstīšana, inovatīvu pieeju veicināšana, to vidū, piemēram, nopietnas spēles un kopīgas simulācijas platformas, intensīvas apmācības nedēļu organizēšana kiberdrošības amatos un netehnisko funkciju profilu izskaidrošana. Būtu jāatbalsta arī dalība šajās kiberdrošības mācībās grūti sasniedzamām grupām, piemēram, jauniešiem invalīdiem, kuri dzīvo nomaļos rajonos vai laukos, un citām mazākuma grupām.

Komisija turpinās sniegt atbalstu mikrodiplomu, profesionālās izglītības un apmācības programmu izstrādei. Tā, "Erasmus+" turpinās finansēt **kopīgas bakalaura un maģistra studiju programmas, kopīgus kursus vai moduļus, kuros var iegūt mikrodiplomus**, un **jauktas intensīvas programmas**[62] visos tematos, ieskaitot **kiberdrošību**. Tiks atbalstīta arī **iniciatīvas "Eiropas universitātes"**[63] un **profesionālās izcilības centru**[64] tālāka izvēršana, lai visā Eiropā veicinātu ciešāku sadarbību starp augstāko izglītību un attiecīgajām profesionālās izglītības un apmācības iestādēm. Šo ciešākas sadarbības mērķi atbalstīs ES finansēšanas programmas, to vidū "Erasmus+" un "Digitālā Eiropa", kā arī ES fondi **individuālo mācību kontu**[65] izstrādei.

Lai atvieglotu augstskolu mācībspēku un kiberdrošības prasmju apmācības rīkotāju valsts līmeņa sadarbību ar privātā un publiskā sektora darba devējiem un veicinātu publiskā un privātā sektora sinerģiju, NKC tiek aicināti izpētīt iespējas dalībvalstīs izveidot **kibermītnes**. Kibermītņu mērķis būtu valsts līmenī kiberdrošības kopienai nodrošināt izcilības centrus, un Akadēmija tām palīdzētu tīkloties un vēl labāk koordinēt darbību.

ENISA arī uzlabos savu kiberdrošības apmācību piedāvājumu, **kursu sarakstu**[66] pieskaņojot *ECSF* profiliem un katram profilam izstrādājot mācību moduļus, tā varbūt uzlabojot dalībvalstu apmācības piedāvājumu. *ENISA* arī paplašinās savu **"apmācītāju apmācīšanas" programmu**[67], pievēršoties *EUIBA* un dalībvalstu publisko iestāžu un **publisko un privāto kritisko operatoru** profesionālajām vajadzībām TID2 direktīvas piemērošanas jomā.

Arī citas ES aģentūras un struktūras stiprinās savu kiberdrošības apmācības piedāvājumu. Piemēram, **EDAK**, īstenojot ES kiberaizsardzības politiku, izstrādās jaunu kiberdrošības kursu kopumu un dažus no pašreizējiem kursiem pieskaņos *ECSF*. Šie kursi ļaus izdot mācību sasniegumu apliecinājumus[68]. Sadarbībā ar Komisiju EDAK pētīs iespēju apliecinājumus iekļaut *EUeID* makā. EDAK turpinās pētīt iespējas izvērtēt prasmju apguves mehānismus, uz kuru pamata tiks izdoti apliecinājumi. Tāpat kibernoziedzības apkarošanas jomā tiks meklēti cieši sakari ar ***CEPOL* Kibernoziedzības apkarošanas akadēmiju**[69], lai

[62] Jauktas intensīvās programmas apvieno tiešsaistes mācīšanu ar īsu fiziskas mobilitātes periodu.

[63] *European Universities initiative | European Education Area (europa.eu)*.

[64] *Centres of Vocational Excellence | Erasmus+* (europa.eu).

[65] Saskaņā ar Padomes Ieteikumu (2022. gada 16. jūnijs) par individuālajiem mācību kontiem.

[66] *Training Courses – ENISA* (europa.eu).

[67] *Train the trainer programme – ENISA* (europa.eu)

[68] Saskaņā ar Padomes Lēmuma (KĀDP) 2020/1515 (2020. gada 19. oktobris), ar ko izveido Eiropas Drošības un aizsardzības koledžu un atceļ Lēmumu (KĀDP) 2016/2382, 20. panta 4. punktu.

[69] *CEPOL* Kibernoziedzības apkarošanas akadēmija tika izveidota 2019. gadā, lai nodrošinātu mūsdienīgu platformu kibernoziedzības apkarošanas zinību un kiberspēju uzlabošanai Eiropā.

veicinātu sinerģiju un savstarpēju papildināmību apmācību programmu izstrādē un īstenošanā.

4.3. Sinerģijas radīšana un kiberdrošības apmācības un tās apliecinājumu pamanāmības nodrošināšana visās dalībvalstīs

Akadēmijai jārisina jautājums par apmācības un tās apliecinājumu pamanāmību un sinerģiju. Tas nāktu par labu civilajām, aizsardzības, tiesībaizsardzības un diplomātiskajām kiberkopienām, jo daudzos gadījumos visās nozarēs ir vajadzīga vienāda lietpratība uz līdzīgu mācību programmu un mācību sasniegumu pamata.

Akadēmija nodrošinātu **vienotu piekļuves punktu** tiem, kuri ieinteresēti kiberdrošībnieka karjerā. Tuvākajā laikā tas tiks darīts, ar *ECCO* projekta atbalstu uzlabojot Komisijas **Digitālo prasmju un darba vietu platformu**. Īpaša sadaļa par karjeru kiberdrošības jomā būs saistīta ar pastāvošajiem rīkiem, sākot ar augstākās izglītības programmām un apmācības iespējām, ieskaitot kursus, kuru rezultātā tiek izsniegti mikrodiplomi un apgūtas profesionālās izglītības un apmācības programmas, un beidzot ar darba piedāvājumiem. Tas tiks panākts, atsaucoties uz notiekošo darbu un iniciatīvām, vai tos integrējot platformā: piemēram, *ENISA*, kas sadarbībā ar augstskolu mācībspēkiem **kartē izglītības iestādes**, kuras nodrošina kiberdrošības programmas. Tas tiks vēl vairāk uzlabots ar valstu koordinācijas centru atbalstu. Turklāt *ENISA* ar NKC, Komisijas un *ECCO* projekta atbalstu un sadarbībā ar struktūrām, kas nodrošina apliecinājumu izdošanu, un izmantojot arī citas attiecīgas iniciatīvas, izstrādās un konsolidēs divus **publiskā un privātā sektora pastāvošu apmācību un kiberdrošības apliecinājumu repozitorijus**[70]. Tie tiks integrēti arī Digitālo prasmju un darba vietu platformas vienotajā piekļuves punktā. Šis darbs nāks par labu arī NKC, kuru galvenais uzdevums ir veicināt un izplatīt kiberdrošības izglītības programmas[71].

Ir arī jānodrošina speciālistiem apstiprinājums, ka viņiem sniegtā apmācība ir pietiekami kvalitatīva. Šajā sakarā *ENISA* izstrādās **izmēģinājuma projektu**, izpētot Eiropas kiberdrošības prasmju apliecināšanas shēmas izveidi.

Būtiski ir arī apzināt prasmes un apmācību un tās iesaistīt amata profilā, taču ir svarīgi arī nodrošināt, ka kiberdrošības pakalpojumiem tiek vajadzīgā kompetence, lietpratība un pieredze. Tas īpaši attiecas uz pārvaldītu drošības pakalpojumu sniedzējiem tādās jomās kā reaģēšana uz incidentiem, ielaušanās testēšana, drošības revīzija un konsultācijas. TID2 direktīvā un Kiberdrošības akta priekšlikumā tādiem pārvaldītu drošības pakalpojumu sniedzējiem ir noteikti konkrēti uzdevumi. Tāpēc Komisija ierosina arī **mērķētus grozījumus Kiberdrošības aktā**[72], lai ES līmenī būtu iespējamas pārvaldītu drošības pakalpojumu apliecināšanas shēmas. Starp tādu shēmu mērķiem jābūt nodrošināt, ka pakalpojumus sniedz darbinieki ar ļoti augstām tehniskām zināšanām un kompetenci attiecīgajās jomās.

---

[70] Piemēram, *W4C Academy – Women4Cyber* vai *Global Cybercrime Certification project* tiesībaizsardzības un tiesu iestādēm.

[71] "1. Nacionālajiem koordinācijas centriem ir šādi uzdevumi: .. g) neskarot dalībvalstu kompetenci izglītības jomā un ņemot vērā attiecīgos *ENISA* uzdevumus, sadarboties ar valstu iestādēm attiecībā uz iespējamu ieguldījumu kiberdrošības izglītības programmu veicināšanā un izplatīšanā", *ECCC* regulas 7. panta 1. punkta g) apakšpunkts. Sk. arī attiecīgo 28. apsvērumu.

[72] Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts).

Mikrodiplomu kvalitātes nodrošināšanas un atzīšanas mehānismi[73] veicina mācību sasniegumu pārredzamību, salīdzināmību un pārnesamību. Saskaņā ar Padomes ieteikumu par Eiropas pieeju mikrodiplomiem[74] dalībvalstis tiek mudinātas savā kvalifikācijas ietvarstruktūrā iekļaut kiberdrošības mikrodiplomus. Tas tām ļautu kiberdrošības mikrodiplomus sasaistīt ar Eiropas kvalifikācijas ietvarstruktūru[75]. Eiropas mācību digitālo apliecinājumu infrastruktūra ir gatava indivīdiem izdot digitāli parakstītas kiberdrošības kvalifikācijas atestātus un mikrodiplomus. Tie ietver bagātīgus datus, arī par kiberdrošības mācību sasniegumiem, un tos varēs glabāt topošajā ***EUeID* digitālajā makā**[76].

Akadēmijas pasākumi

Dalībvalstis un nozare

- Nodrošināt atbalstu kiberdrošības mācību **mikrodiplomu** izstrādei un atzīšanai saskaņā ar Padomes ieteikumu par Eiropas pieeju mikrodiplomiem.
- Iekļaut kiberdrošības kvalifikācijas atestātus, ieskaitot mikrodiplomus, **valsts kvalifikācijas ietvarstruktūrā**.
- Ar māceklību nodrošināt **mācību iespējas darbā** cilvēkiem, kuri izmanto kiberdrošības prasmju pilnveides iniciatīvas.

Komisija

- Tuvākajā laikā – līdz 2023. gada beigām – izveidot **vienotu piekļuves punktu** kiberdrošības programmām, pastāvošajai apmācībai un kiberdrošības sertifikācijai **Digitālo prasmju un darba vietu platformā**.
- Ierosināt **Kiberdrošības akta grozījumu**, lai 2023. gada 18. aprīlī varētu apstiprināt pārvaldītus drošības nodrošinātājus.

ES struktūras un aģentūras

- Līdz 2023. gada beigām izveidot ***ECSF*** kā vienotu pieeju kiberdrošības funkciju profiliem un ar tiem saistītajām prasmēm.
- 2023. gada 2. ceturksnī *ENISA* sāks izstrādāt izmēģinājuma projektu, kas veido **Eiropas kiberdrošības prasmju apliecināšanas shēmu**.
- *ENISA* pārskatīs savu **kursu sarakstu** un līdz 2023. gada beigām atvērs **"apmācītāju apmācīšanas" programmu** kritiskiem publiskā un privātā sektora operatoriem.
- Līdz 2023. gada vidum pabeigt **EDAK mācību programmu pieskaņošanu *ECSF***.

5. Ieinteresēto personu iesaiste – apņemšanās pārvarēt kiberdrošības prasmju deficītu

Akadēmijā tiks izstrādāta koordinēta pieeja ieinteresēto personu iesaistei, lai pārvarētu kiberdrošības prasmju deficītu. Mērķis būs maksimalizēt dažādu ieinteresēto personu saistību pamanāmību un ietekmi, lai mazinātu kiberdrošības prasmju deficītu.

[73] Piemēram, ieraksti vai atestāti par mācību sasniegumiem, ko iegūst pēc nelielas apmācības.

[74] Padomes Ieteikums par Eiropas pieeju mikroapliecinājumiem mūžizglītībā un nodarbināmībā.

[75] Padomes Ieteikums (2017. gada 22. maijs) par Eiropas kvalifikāciju ietvarstruktūru mūžizglītībai un ar ko atceļ Eiropas Parlamenta un Padomes 2008. gada 23. aprīļa Ieteikumu par Eiropas kvalifikāciju ietvarstruktūras izveidošanu mūžizglītībai.

[76] Priekšlikums – Eiropas Parlamenta un Padomes Regula, ar ko Regulu (ES) Nr. 910/2014 groza attiecībā uz Eiropas digitālās identitātes regulējuma izveidi.

Komisija aicina ieinteresētās personas uzņemties konkrētas saistības, apņemoties ar īpašām darbībām uzlabot darbinieku prasmes un pārkvalificēšanos, pēc iespējas vairāk koncentrējoties uz konstatēto kiberdrošības prasmju deficītu. Par tādiem **ieinteresēto personu solījumiem kiberdrošības jomā** būtu jāpaziņo **Digitālo prasmju un darba vietu platformā**, tāpat kā par citām digitālām saistībām, kas jau ir redzamas platformā. Komisija arī mudina ieinteresētās personas, kuras platformā apņemas iesaistīties kiberdrošībā, pievienoties **plašajai digitālajai partnerībai saskaņā ar Prasmju pilnveides paktu**[77]. Plašās digitālās partnerības ietvaros uzņemtās kiberdrošības saistības būtu iesniedzamas Digitālo prasmju un darba vietu platformā. Tāpat tiek mudināts ziņot par saistībām, kas uzņemtas saskaņā ar Digitālo prasmju un darba vietu platformu, saskaņā ar Prasmju pilnveides pakta liela mēroga digitālo partnerību.

Komisija arī aicina dalībvalstis **turpināt centienus īstenot deklarāciju "Sievietes digitālajā jomā"**[78], lai mudinātu sievietes uzņemties aktīvu un nozīmīgu lomu digitālo tehnoloģiju nozarē un panākt dzimumu vienādāku pārstāvību kiberdrošības amatos. Komisija arī mudina dalībvalstis veidot sinerģiju ar savām **Eiropas Sociālā fonda+** (ESF+) programmām, lai vēl vairāk atbalstītu dzimumu līdztiesības mērķi attiecībā uz dalību darbaspēka tirgū[79], piemēram, izveidojot **mentorēšanas programmas jaunietēm un sievietēm**. Tās var atvieglot paraugu veidošanu, lai piesaistītu jaunietes kiberdrošības profesijām, vienlaikus cīnoties ar stereotipiem dzimumu jautājumos. Komisija arī mudina uzlabot sieviešu prasmes un viņas pārkvalificēt un veicina tādas kopienas attīstību, kas spēj atbalstīt sieviešu ienākšanu vai pozīciju uzlabošanu kiberdrošības darba tirgū.

Dalībvalstīm būtu **savā kiberdrošības stratēģijā jānosaka īpaši pasākumi, kas mazina kiberdrošības prasmju deficītu**[80], jāapzina un labāk jāvirza centieni pārvarēt prasmju deficītu un galu galā jānodrošina savu pienākumu pienācīga īstenošana saskaņā ar TID2 direktīvu.

Dažas dalībvalstis izmanto **sinerģiju starp civilajām, aizsardzības un tiesībaizsardzības** iniciatīvām. Piemēram, paplašina kadru rezerves, izmantojot valsts obligāto karadienestu vai pieaicinot kiberrezervistus, kas ir militāri izglītoti pilsoņi, kuri bruņotajos spēkos ieņem kiberdrošības amatus[81], ļauj iedzīvotājiem, sevišķi jauniešiem, uzlabot kiberdrošības un kiberaizsardzības prasmes. Tas pats attiecas uz **kibernoziedzības apkarošanu**, jo pastāv daudz līdzības starp vispārējiem kiberdrošības centieniem un tiesībaizsardzības darbībām reaģēšanā uz kiberdrošības incidentiem. Komisija mudina dalībvalstis iniciatīvas apspriest un izvērtēt, kā kvalificēti kadri var vislabāk kalpot gan militārās, gan civilās kiberdrošības kopienām.

Komisija apdomās priekšlikumus par to, kā novērst pašreizējās un paredzamās nepilnības, kas konstatētas pārskatā par *EUIBA* vajadzībām. Tā īpaši mudinās darbiniekus izmantot gaidāmo **ES un ASV kiberdrošības stipendiju**, kas izveidota ES un ASV dialogā.

---

[77] *New European Partnerships launched to deliver on the EU's ambitions for the Digital Decade | Shaping Europe's digital future* (europa.eu) – atbilstoši Prasmju pilnveides paktam izveidotas jaunas partnerības informācijas un komunikācijas tehnoloģiju (IKT) deficīta novēršanai.

[78] *EU countries commit to boost participation of women in digital | Shaping Europe's digital future* (europa.eu).

[79] Eiropas Parlamenta un Padomes Regulas (ES) 2021/1057 (2021. gada 24. jūnijs), ar ko izveido Eiropas Sociālo fondu Plus (ESF+) un atceļ Regulu (ES) Nr. 1296/2013, 4. panta 1. punkta c) apakšpunkts.

[80] TID2 direktīvas 7. panta 2. punkta f) apakšpunkts.

[81] Ziņojums – *Cyber Conscription: Experience and Best Practice from Selected Countries, Martin Hurt and Tiia Sõmer, International Centre for Defence and Security, February 2021*.

Akadēmijas pasākumi

Nozare

- Ierosināt konkrētus **kiberdrošības solījumus** Digitālo prasmju un darba vietu platformā no 2023. gada 18. aprīļa.

Dalībvalstis

- **Valsts kiberdrošības stratēģijā** iekļaut īpašus pasākumus, ar kuriem pārvarēt kiberdrošības prasmju deficītu.

Dalībvalstis un nozare

- Īstenot deklarāciju "Sievietes digitālajā jomā" un līdz 2030. gadam panākt **dzimumu vienādāku pārstāvību kiberdrošības amatos**.

6. Finansēšana – veidot sinerģiju, lai maksimalizētu kiberdrošības prasmju attīstīšanas izdevumu ietekmi

Akadēmijā ieguldījumu ietekme kiberdrošības prasmēs tiks maksimalizēta, nodrošinot vienotu piekļuves punktu, veicinot līdzekļu labāku novirzīšanu tirgus vajadzībām un integrējot finansējuma izmantošanu, veicinot sinerģiju starp dažādiem instrumentiem, vienlaikus izvairoties no centienu dublēšanās[82].

6.1. Līdzekļu un vajadzību salāgošana

Akadēmijā *ECCC* ar Komisijas, *ECCO* projekta un NKC atbalstu ievāks **informāciju par to, kā ES līdzekļi tiek izmantoti kiberdrošības prasmju finansēšanai**, un vērtēs, kā ES fondi atbalsta kiberdrošības prasmju deficīta mazināšanu. Ņemot vērā apkopoto informāciju, *ECCC* centīsies nodrošināt ES līdzekļu labāku novirzīšanu konstatētajām vajadzībām. Tas finansēs darbības, kas pārvarētu spiedīgākās kiberdrošības kadru nepilnības, ieskaitot tās, kas saistītas ar kiberdrošības politikas vajadzību īstenošanu.

6.2. Kiberdrošības prasmju jomā pieejamo līdzekļu un partnerības iniciatīvu pamanāmības nodrošināšana

Tuvākajā laikā **digitālo prasmju un darba vietu platforma** kļūs par vienīgo piekļuves punktu ieinteresētajām personām, kur būs pieejama visa informācija par kiberdrošības prasmju finansēšanas iespējām.

ES iegulda cilvēkos un viņu prasmēs un izmanto partnerības, sevišķi ar nozari, lai mobilizētu rīcību prasmju pilnveides un pārkvalifikācijas jomā, izmantojot vairākus instrumentus, kas noteikti **Eiropas Prasmju programmā**[83], it īpaši **Prasmju pilnveides paktu**[84] un **Digitālās izglītības rīcības plānu**[85]. **Programma "Digitālā Eiropa"** finansē kiberdrošības prasmju iespējas, galvenokārt ar daudzvalstu projektu iniciatīvām, skaidri papildinot atbalstu, ko

[82] Finansēšanas iespējas (europa.eu). Prasmju atbalsta pakalpojumu pakts nodrošina vienotu piekļuves punktu informācijai par prasmju finansēšanu, arī digitālajai ekosistēmai. Pakta atbalsta pakalpojumi sniedz vispārīgu informāciju par finansēšanas instrumentiem, kas nav īpaši vērsti uz kiberdrošības prasmēm, kaut gan Akadēmijai būtu jāņem vērā to darbs, lai izvairītos no dublēšanās.

[83] *European Skills Agenda – Employment, Social Affairs & Inclusion – European Commission* (europa.eu).

[84] *EU funding instruments for upskilling and reskilling – Employment, Social Affairs & Inclusion – European Commission* (europa.eu).

[85] Digitālās izglītības rīcības plāns 2021.–2027. gadam.

"Apvārsnis Eiropa" kiberdrošības jomā piedāvā pētniecībai un inovatīviem tehnoloģiskiem risinājumiem. **Eiropas Aizsardzības fonds**[86] finansē pētniecību un tehnoloģiju izstrādi, lai veiktu efektīvas kiberoperācijas, ieskaitot apmācību un vingrināšanos[87]. **"Erasmus+"** turpinās atbalstīt tādas iniciatīvas, cita starpā izmantojot jauktas intensīvas programmas un sadarbības projektus.

Dalībvalstis tiek mudinātas mobilizēt ES līdzekļus, ko tās tieši pārvalda, lai atbalstītu kiberdrošības prasmes un darba vietas. Kohēzijas politikas fondiem, kā **Eiropas Reģionālās attīstības fondam (ERAF)** un **ESF+**, šajā sakarā ir būtisks sinerģijas potenciāls[88]. **Atveseļošanas un noturības mehānisma** (ANM)[89] un ***InvestEU***[90] darbību tvērumā ir turpmāka būtiska savstarpēja papildināmība Akadēmijas mērķu sasniegšanā.

<u>Akadēmijas pasākumi</u>

Eiropas Kiberdrošības kompetences centrs un *ENISA*

- Līdz 2024. gada beigām izveidot esošo ES finansējumu kiberdrošības prasmju **kartējumu** atkarībā no tirgus vajadzībām, novērtēt **efektivitāti** un noteikt finansēšanas **prioritātes**.

Komisija

- Līdz 2023. gada beigām izveidot **vienotu piekļuves punktu** kiberdrošības prasmju finansēšanas iespējām Digitālo prasmju un darba vietu platformā.

7. Veikuma novērtēšana – integrēta pārskatatbildība

Akadēmijā tiks izstrādāta **metodika**, kas ļaus **novērtēt veikumu kiberdrošības prasmju deficīta pārvarēšanā**.

7.1. Kiberdrošības rādītāju noteikšana kiberdrošības darbaspēka tirgus attīstības uzraudzībai

Digitālās ekonomikas un sabiedrības indekss (*DESI*) apkopo Eiropas digitālā snieguma rādītājus un seko ES dalībvalstu attīstībai šajā jomā. Kiberdrošības prasmju akadēmijas ietvaros *ENISA* sadarbībā ar Komisiju un TID sadarbības grupu[91] izstrādās **rādītājus**, arī dzimumu līdztiesībai, lai sekotu progresam, kas ES dalībvalstīs panākts kiberdrošības speciālistu skaita palielināšanā, apspriežoties arī ar attiecīgajiem tirgus dalībniekiem un NKC.

---

[86] Eiropas Parlamenta un Padomes Regula (ES) 2021/697 (2021. gada 29. aprīlis), ar ko izveido Eiropas Sociālo fondu Plus (ESF+) un atceļ Regulu (ES) Nr. 2018/1092.

[87] Dalībvalstis ir apņēmušās rīkot kopīgas mācības un vingrinājumus, izveidojot pastāvīgās strukturētās sadarbības (*PESCO*) kiberapmācības un mācību projektus un tajos piedaloties: ES Kiberlietu akadēmija un inovācijas centrs *(EU CAIH)*, federatīvie kiberpoligoni u. c.

[88] Regulas (ES) 2021/1058 3. panta 1. punkts un Regulas (ES) 2021/1057 4. panta 1. punkta g) apakšpunkts.

[89] Piemēram, Igaunijas atveseļošanas un noturības plānā ir paredzēti ieguldījumi (10 miljoni euro) digitālajās prasmēs, kas ietvers IKT ekspertiem pieejamās apmācības pārskatīšanu, finansēs IKT speciālistu prasmju pilnveidi un pārkvalifikāciju kiberdrošības jomā un palīdzēs izstrādāt izmēģinājuma programmu IKT speciālistu kvalifikācijas sistēmas pārveidei.

[90] Ieinteresētās personas (piemēram, apmācības nodrošinātāji un uzņēmumi, kuri vēlas izstrādāt vai uzlabot savas kiberdrošības apmācības darbības) var vērsties *InvestEU* konsultāciju centrā, kas sniedz tehnisko atbalstu un palīdzību, ieskaitot spēju veidošanu projektu izstrādātājiem un vienībām, un ielūkoties *InvestEU* portālā.

[91] Izmantojot un papildinot metodiku, kas *ENISA* jāizstrādā aģentūras divgadu ziņojuma par kiberdrošības stāvokli Savienībā vajadzībām saskaņā ar TID2 direktīvas 18. panta 3. punktu.

ENISA izmantos *DESI* metodiku[92] un nodrošinās, ka rādītāji atbilst Eiropas digitālajiem mērķrādītājiem, kas attiecas uz IKT speciālistiem un dzimumu vienādāku pārstāvību IKT jomā. Tad Komisija strādās ar tādu rādītāju integrēšanu *DESI*, ar to ļaujot katru gadu sekot stāvoklim kiberdrošības prasmju un darba tirgus jomā.

7.2. Datu vākšana un ziņošana

Ar *ECCO* projekta un NKC atbalstu *ENISA* apkopos datus par rādītājiem. Uz savākto datu pamata *ENISA* sagatavos **gada ziņojumu**, kas palīdzēs sagatavot ziņojumu par digitālo desmitgadi[93], kuru kopā ar *DESI* tālāk izmantos **Eiropas pusgada** konkrētām valstīm adresētajā analīzē un ieteikumos[94]. Turklāt kiberdrošības prasmju rādītāji palīdzēs sagatavot TID2 direktīvā paredzēto *ENISA* **divgadu ziņojumu** par kiberdrošības stāvokli ES, aptverot kiberdrošības spējas, informētību un higiēnu visā ES.

*7.3. Kiberdrošības galveno snieguma rādītāju (***KPI***) sagatavošana*

Lai pārvarētu Eiropas kiberdrošības talantu deficītu, *ENISA* ciešā sadarbībā ar Komisiju un valstu koordinācijas centriem ierosinās Komisijai galvenos snieguma rādītājus, izmantojot 2030. gada politikas programmas "Digitālās desmitgades ceļš" metodiku, kā arī nozares pieredzi. *ENISA* pienācīgi ņems vērā galvenos snieguma rādītājus, ko dalībvalstis izmanto savu kiberdrošības stratēģiju novērtēšanā[95].

Akadēmijas pasākumi

ENISA

- Līdz 2023. gada beigām sagatavot **rādītājus un *KPI*** kiberdrošības prasmju jomā.
- **Ievākt datus** par rādītājiem un ziņot par tiem, pirmoreiz – līdz 2025. gadam.

Komisija

- Strādāt ar **kiberdrošības rādītāju integrēšanu *DESI*** un **digitālās desmitgades ziņojumā**.

8. Nobeigums

Šajā paziņojumā ir noteikti pamati ES pieejas pārstrādāšanai, lai uzlabotu speciālistu kiberdrošības prasmes ES. Mērķis ir mazināt kiberdrošības prasmju deficītu un nodrošināt ES ar kadriem, kas vajadzīgi reaģēšanai pastāvīgi mainīga apdraudējuma vidē, īstenot ES politiku, kuras mērķis ir pasargāt ES no kiberuzbrukumiem, kā arī uzlabot uzņēmējdarbības iespējas un konkurētspēju. Prasmīgi kiberdrošības kadri var pozitīvi ietekmēt **civilās, militārās, diplomātiskās un tiesībaizsardzības** kopienas, veicinot to sinerģiju.

Komisija aicina dalībvalstis un visas ieinteresētās personas tiekties uz augstajiem Kiberdrošības prasmju akadēmijas mērķiem.

[92] Sk. Digitālās ekonomikas un sabiedrības indeksa (*DESI*) 2022. gada piezīmi par metodiku, *The Digital Economy and Society Index (DESI) | Shaping Europe's digital future* (europa.eu).

[93] Eiropas Parlamenta un Padomes Lēmums (ES) 2022/2481 (2022. gada 14. decembris), ar ko izveido politikas programmu "Digitālās desmitgades ceļš" 2030. gadam.

[94] Turpat, 25. apsvērums.

[95] TID2 direktīvas 7. panta 4. punkts.