ЕВРОПЕЙСКА
КОМИСИЯ

Страсбург, 18.4.2023 г.
COM(2023) 207 final

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

Преодоляване на недостига на таланти в областта на киберсигурността за повишаване на конкурентоспособността, растежа и устойчивостта на ЕС

(„Академия на ЕС за киберумения“)

Преодоляване на недостига на таланти в областта на киберсигурността за повишаване на конкурентоспособността, растежа и устойчивостта на ЕС

(„Академия на ЕС за киберумения“)

1. Спешна необходимост от намаляване на рисковете чрез преодоляване на недостига на умения и пропуските в областта на киберсигурността

Киберсигурността не е само част от сигурността на гражданите, предприятията и държавите членки. Тя е и необходимост, за да се гарантират политическата стабилност на ЕС и стабилността на неговите демокрации, както и просперитетът на нашето общество и предприятия. **Картината на киберзаплахите** се промени значително през последните години, като тревожната тенденция е, че все по-голям брой кибератаки са насочени към военната и гражданската инфраструктура от критично значение в ЕС. Участниците в заплахите увеличават своите възможности и същевременно възникват съвършено нови, хибридни и непрекъснато развиващи се, като например използването на ботове и техники, базирани на изкуствен интелект[1]. По-специално заплахите, свързани със софтуер за изнудване, редовно нанасят значителни щети, както финансови, така и увреждащи репутацията, на юридически лица[2].

При голям брой киберинциденти цел на атаките бяха публичната администрация и правителствата в държавите членки, както и европейските институции, органи и агенции (EUIBA)[3]. Секторите на финансите[4] и здравеопазването[5], които са главната опора на обществото и икономиката, също постоянно са обект на посегателства[6]. Геополитическото напрежение, свързано с агресивната война на Русия срещу Украйна, увеличи киберзаплахите[7] и има потенциал да дестабилизира обществото ни. **Сигурността** на ЕС не може да бъде гарантирана без **най-ценния актив на Съюза: неговите граждани.** ЕС спешно се нуждае от специалисти с умения и познания за

[1] Доклад относно картината на заплахите на ENISA, 2022 г. — ENISA (europa.eu)

[2] Оценка на заплахата от организирана престъпност, ползваща се от интернет, Европол (IOCTA), 2021 г. Такива участници се основават на модела „софтуер за изнудване като услуга“. Годишните разходи за предприятията надхвърлят 18,4 милиарда евро през 2022 г., Cybereason 2022 Report on the true cost or Ransomware (Доклад за истинската цена на софтуера за изнудване, Cybereason, 2022 г.)

[3] Вж. например Съвместна публикация на Агенцията на Европейския съюз за киберсигурност (ENISA) и Екипа за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на ЕС (CERT-EU), JP-23-01 — Sustained activity by specific threat actors („Устойчива дейност на конкретни участници в заплахи“), TLP:CLEAR, 15 февруари 2023 г.

[4] Вж. например в Германия 90 % от измамите по пощата, докладвани от 1 юни 2021 г. до 31 май 2022 г., са били финансов фишинг или атака срещу дружество от финансовия сектор, включваща повече от 20 000 заразени устройства от 125 държави, The State of IT Security in Germany in 2022 („Състояние на ИТ сигурността в Германия през 2022 г.“), Bundesamt für Sicherheit in der Informationstechnik (BSI), 1 януари 2023 г.

[5] Вж. например във Франция атаките със софтуер за изнудване срещу обществени здравни заведения, като „Centre Hospitalier Sud Francilien“, по време на които 11 GB лични и медицински данни, както и данни, свързани с персонала, са били компрометирани и публикувани от автора на заплахата, Panorama de la cybermenace 2022, Agence nationale de la sécurité des systèmes d'information (ANSSI), janvier 2023 („Картина на киберзаплахите през 2022 г.“, Национална агенция но сигурност на информационните технологии (ANSSI), януари 2023 г.)

[6] Доклад относно картината на заплахите на ENISA, 2022 г.

[7] Вж. също CERT-EU — Russia’s war on Ukraine: one year of cyber operations („Войната на Русия срещу Украйна: една година кибероперации“ (europa.eu); Руски кибероперации срещу Украйна:Декларация на върховния представител от името на Европейския съюз, 10 май 2022 г.; Декларация на върховния представител от името на Европейския съюз относно злонамерени действия в киберпространството, извършвани от хакери и хакерски групи в контекста на агресията на Русия срещу Украйна, 19 юли 2022 г.

предотвратяване, откриване, възпиране на кибератаки и защита на Съюза, включително на неговите инфраструктури от най-критично значение, от такива кибератаки, както и осигуряване на неговата **устойчивост**.

Недостигът на таланти в областта на киберсигурността допълнително възпрепятства **конкурентоспособността** и **растежа** на Европа, които силно зависят от развитието и внедряването на стратегически цифрови технологии (напр. изкуствен интелект, 5G и облачни технологии). Необходима е квалифицирана работна сила в областта на киберсигурността, за да може ЕС да запази позицията си на доставчик на ключови авангардни технологии в световен мащаб.

За да се подготви и справи с тази променяща се картина на заплахите, както и за да насърчи конкурентоспособността на Съюза, политиката на ЕС в областта на киберсигурността претърпя значително развитие през последните години, което доведе до приемането на редица инициативи, като например Стратегията за киберсигурност за цифровото десетилетие[8], преразгледаната Директива за мрежова и информационна сигурност (Директива МИС 2)[9], секторното законодателство на ЕС в областта на киберсигурността[10], политиката на ЕС за киберотбрана[11], законодателния акт за киберустойчивост[12] и законодателния акт за киберсолидарност, предложен от Комисията заедно с настоящото съобщение. Без необходимите квалифицирани кадри обаче, които да ги прилагат, тези законодателни актове няма да постигнат целите си. Въпреки че основните познания на населението в областта на киберсигурността се разглеждат като част от инициативите в подкрепа на развитието на общите умения, необходими за участие в обществото[13], компетентната работна сила е от съществено значение както в публичния, така и в частния сектор, на национално равнище и на равнището на ЕС, включително в организациите за стандартизация, **за да бъдат изпълнени тези правни и политически изисквания в областта на киберсигурността.**

Следователно сигурността и конкурентоспособността на ЕС зависят от наличието на работна сила с професионална квалификация в областта на киберсигурността. Въпреки това Съюзът е изправен пред значителен недостиг на квалифицирани специалисти в

[8] Съвместно съобщение до Европейския парламент и Съвета „Стратегия на ЕС за киберсигурност за цифровото десетилетие“, JOIN(2020) 18 final

[9] Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2)

[10] Като например за финансовия сектор Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 (Регламент DORA).

[11] Съвместно съобщение до Европейския парламент и Съвета „Политика на ЕС за киберотбрана“, JOIN(2022) 49 final

[12] Предложение за Регламент на Европейския парламент и на Съвета относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на Регламент (ЕС) 2019/1020, COM/2022/454 final

[13] Сред съответните инициативи, насочени към общите цифрови умения на населението: 80 % от населението да постигне основни цифрови умения до 2030 г. като цел на Плана за действие на Европейския стълб на социалните права и Цифровия компас, плана за действие в областта на цифровото образование за периода 2021—2027 г., инструмента на Европейската рамка за цифрова компетентност или предложението за Препоръка на Съвета относно подобряването на предоставянето на цифрови умения в образованието и обучението.

областта на киберсигурността, което излага на риск от киберинциденти ЕС и неговите държави членки, предприятия и граждани. През 2022 г. недостигът на специалисти по киберсигурност в Европейския съюз се оценяваше на стойност **между 260 000**[14] **и 500 000**[15], като нуждите на ЕС от работна сила в областта на киберсигурността се оценяваха на 883 000 специалисти[16], което предполага несъответствие между наличните умения и изискваните от пазара на труда. Работната сила в областта на киберсигурността страда от погрешно разбиране, свързано с техническия ѝ имидж, и продължава да не успява да привлече **жени**, които съставляват 20 % от висшистите по киберсигурност[17] и 19 % от специалистите по информационни и комуникационни технологии (ИКТ)[18]. За бъде решен този проблем, в европейската **политическа програма „Цифрово десетилетие до 2030 г.“**[19] е поставена целта да се увеличи броят на специалистите в областта на ИКТ с 20 милиона до 2030 г., като същевременно се постигне конвергенция между половете. Освен това прилагането на съвършено нови политики на ЕС изисква адекватно квалифицирана и достатъчна работна сила. Например над 42 % от висшите ИТ ръководители в сектора на финансовите услуги изтъкнаха липсата на умения и експертен опит в областта на киберсигурността като основно предизвикателство за своята стопанска дейност, когато става въпрос за киберотбраната и управлението на киберинциденти[20], за периода, в който ще трябва да прилагат секторното законодателство в областта на киберсигурността, като например акта за оперативната устойчивост на цифровите технологии (DORA).

Колебливите инвестиции на работодателите в човешки капитал, които търсят работна сила, притежаваща вече професионална квалификация и опит, допълнително допринасят за ограничаването на пазара на труда[21]. Този недостиг засяга всички видове дружества, включително малките и средните предприятия (**МСП**), които представляват 99 % от всички предприятия в ЕС[22]. Предизвикателството е голямо и за **публичните администрации**, голяма част от които са сред най-значително засегнатите от киберинцидентите[23].

Ето защо преодоляването на недостига на специалисти в областта на киберсигурността в ЕС е неотложен въпрос, тъй като сигурността и конкурентоспособността на ЕС са застрашени.

---

[14] (ISC)² в Оценка на киберуменията въз основа на Европейската рамка за умения в областта на киберсигурността (ECSF), уебинар на ENISA, 16 февруари 2023 г.

[15] Според Европейската организация за киберсигурност (ECSO), както е посочено в Съвместно съобщение до Европейския парламент и Съвета „Политика на ЕС за киберотбрана“, JOIN(2022) 49 final

[16] (ISC²) в Оценка на киберуменията въз основа на Европейската рамка за умения в областта на киберсигурността (ECSF), уебинар на ENISA, 16 февруари 2023 г.

[17] База данни за висшето образование в киберсигурността (CyberHEAD)

[18] Само 19 % от специалистите по ИКТ в ЕС са жени. Индекс за навлизането на цифровите технологии в икономиката и обществото (DESI) 2022 г. | Стратегия в областта на цифровите технологии (europa.eu). Няма данни за броя на жените, които работят в областта на киберсигурността в Съюза.

[19] Решение (ЕС) 2022/2481 на Европейския парламент и на Съвета от 14 декември 2022 г. за създаване на политическа програма „Цифрово десетилетие“ до 2030 г., с което се създава механизъм за наблюдение и сътрудничество за постигане на общите цели и задачи за цифровата трансформация на Европа, определени в Цифровия компас до 2030 г., включително в областта на уменията.

[20] S-RM Cyber Security Insights Report 2022 (Доклад за киберсигурността на S-RM, 2022 г.)

[21] Cybersecurity Skills Development in the EU („Развитие на уменията в областта на киберсигурността в ЕС“), ENISA, декември 2019 г.

[22] Определение за МСП (europa.eu)

[23] Доклад относно картината на заплахите на ENISA, 2022 г. — ENISA (europa.eu)

2. Липса на полезни взаимодействия и координирани действия за преодоляване на недостига на умения в областта на киберсигурността

Инициативите на европейско и национално равнище, провеждани от публични и частни субекти за преодоляване на недостига на работна сила в областта на киберсигурността, процъфтяват. Те обаче са разпокъсани и досега не са успели да достигнат критична маса, която да доведе до реална промяна.

На първо място, понастоящем има ограничено общо разбиране за състава на работната сила в областта на киберсигурността в ЕС и за свързаните с нея умения, като същевременно сходните професионални профили в областта на киберсигурността би следвало да включват един и същ набор от умения. Слабото използване на обща **европейска референтна рамка за специалисти по киберсигурност** от съответните участници води до липса на инструмент за комуникация между работодатели, преподаватели и създатели на политики, както и до невъзможност за извършване на измервания и оценка на пропуските на пазара на труда в областта на киберсигурността. Също така това възпрепятства изготвянето на програми за образование и обучение и създаването на пътеки за професионално развитие, отговарящи на нуждите на политиката и пазара на желаещите да навлязат в професията. За **повишаването на квалификацията и преквалификацията** на работната сила се разчита предимно на обучения и сертификати в областта на киберсигурността, които обикновено се предлагат от частни доставчици. Работната сила обаче среща трудности да получи представа за качеството на предлаганите обучения по киберсигурност и издаваните сертификати за тях.

Въпреки че образованието и обучението, както и изграждането на пътеки за професионално развитие са необходими за засилване на предлагането на пазара на труда, понастоящем се подценява ролята на **търсенето** в обучението на работната сила и адаптирането към нейното развитие. Работодателите от отрасъла и публичния сектор не разполагат с общи форуми и места, където да обменят идеи как най-добре да обучават работната сила и как да **оценяват по-добре уменията**, особено по време на процеса на набиране на персонал. Най-търсените **„твърди“ умения** може да са свързани с киберсигурността[24], като например разработване на софтуер или облачни изчисления[25], но **трансверсалните умения** продължават да се пренебрегват неоснователно. Критичното мислене и анализът, разрешаването на проблеми и способността за самоуправление са групи от умения, които са все по-търсени от работодателите[26] и стават все по-значими в периода до 2025 г.[27]

Вече съществуват много публични и частни инвестиционни инициативи в областта на уменията в областта на киберсигурността, като ЕС широко **финансира** проекти в рамките на различни инструменти[28]. Продължаващият недостиг на умения в ЕС обаче

---

[24] LinkedIn 2023 Most In-Demand Skills: Learn the Skills Companies Need Most („Най-търсените умения в LinkedIn за 2023 г.: усвояване на уменията, от които предприятията се нуждаят най-много“)

[25] Инфографика за състоянието на киберсигурността, ISACA, 2022 г.

[26] Като например инструментът CEDEFOP: Skills-OVATE | CEDEFOP (europa.eu)

[27] The Future of Jobs Report („Доклад за бъдещето на работните места“), октомври 2020 г., Световен икономически форум)

[28] Например: Cybersecurity Skills Alliance — New Vision for Europe — REWIRE project („Алианс за умения в областта на киберсигурността — Нова визия за Европа — проект REWIRE“) (финансиран от програма „Еразъм+“); проекти в подкрепа на Центъра за компетентност в областта на киберсигурността (ECHO, CONCORDIA, CyberSec4Europe, SPARTA (финансиран от инициатива „Хоризонт 2020“), Cybersecpro project (финансиран от програмата „Цифрова Европа“).

повдига въпроси относно тяхната видимост и въздействие и предполага, че те може да не съответстват систематично на нуждите на пазара, които трябва спешно да бъдат определени на равнището на ЕС. Освен това няколко източника на финансиране водят до дублиране на дейности и пропускане на възможността за увеличаване на мащаба и постигане на реално въздействие. В допълнение, тези, които се нуждаят от инвестиции, невинаги могат да определят най-подходящите източници за своите нужди.

Заинтересованите страни се опитват да се справят със сложния и многостранен проблем с недостига на умения в областта на киберсигурността. Агенцията на ЕС за киберсигурност (ENISA) разработва инструменти, свързани с ролевите профили или висшето образование[29], Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността (ECCC)[30] разглежда уменията в областта на киберсигурността в рамките на специална работна група, Европейският колеж по сигурност и отбрана (ЕКСО) работи по уменията в областта на киберсигурността на цивилната и военната работна сила в контекста на общата политика за сигурност и отбрана[31], частни организации се опитват да се справят с проблема[32], секторът за сертифициране в областта на киберсигурността разработва пътна карта и обучения, насочени към недостига на умения[33]. Държавите членки също се опитват да се справят с проблема чрез различни инициативи — от регулаторни[34] до създаване на академии за придобиване на умения в областта на киберсигурността[35] или киберкампуси[36], центрове за високи постижения в областта на киберпрестъпността[37] или чрез публично-частни партньорства[38]. В работата на всички тези заинтересовани страни обаче често липсва координираност и полезни взаимодействия и потенциалът за осъществяване на значима промяна на пазара на труда не е достигнат, както става ясно от растящия недостиг на работна сила в областта на киберсигурността в ЕС. Необходимо е също така да се увеличат полезните взаимодействия между кибернетичните общности, тъй като необходимите умения за поддържане на киберсигурността, борбата с **киберпрестъпността** или изграждането на **киберотбрана** често са от подобно естество.

И накрая, понастоящем ЕС разполага с ограничени средства за оценка на **състоянието и развитието на пазара на труда в областта на киберсигурността** и на уменията на работната му сила. Държавите членки и EUIBA разчитат на данни, събрани от частни субекти, или на по-широк набор от данни, събрани в ЕС, по-специално от Евростат[39] и

---

[29] По-специално: Европейската рамка за умения в областта на киберсигурността (ECSF); CYBERHEAD — Базата данни за висшето образование в киберсигурността; платформата за учение в областта на киберсигурността (CEP); Европейското състезание за киберсигурност; Европейският месец на киберсигурността.

[30] Регламент (ЕС) 2021/887 на Европейския парламент и на Съвета от 20 май 2021 г. за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове

[31] По-специално платформата за образование, обучение, учение и оценка в областта на киберсигурността (ETEE)

[32] Например работна група 5 „Образование, обучение, информираност, киберполигон, човешки фактори“ на Европейската организация за киберсигурност (ECSO); организацията DIGITALEUROPE

[33] Например Институтът SANS, (ISC)², ISACA

[34] Например в националните стратегии за образование или киберсигурност.

[35] Например C-Academy в Португалия.

[36] Например Cyber Campus във Франция.

[37] Например литовският център за високи постижения в областта на киберпрестъпността за обучение, изследвания и образование в Литва (L3CE)

[38] Например инициативата на Microsoft за придобиване на умения в областта на киберсигурността

[39] Заетост на специалисти по ИКТ — Статистиката в достъпна форма (Statistics Explained) (europa.eu)

Европейския център за развитие на професионалното обучение (CEDEFOP)[40] за специалистите в областта на ИКТ. С други думи, ЕС разполага с частична и фрагментирана представа за своите нужди, което му пречи да изгради обобщена визия за състоянието на пазара на труда в областта на киберсигурността.

3. Координиран отговор в целия ЕС: Академия на ЕС за киберумения

3.1.Цел

С цел справяне с предизвикателството, свързано с уменията в областта на киберсигурността, и преодоляване на недостига на пазара на труда, Комисията представя предложение за **Академия на ЕС за киберумения**, както бе съобщено от председателя на Европейската комисия в нейното писмо за намеренията относно състоянието на Съюза през 2022 г.[41, 42], и в контекста на Европейската година на уменията.

Целта на Академията на ЕС за киберумения (накратко „Академията“) е да се създаде **единна входна точка и полезни взаимодействия** по отношение на предложенията за образование и обучение в областта на киберсигурността, както и по отношение на възможностите за финансиране и конкретни действия в подкрепа на развиването на умения в областта на киберсигурността. С Академията ще се разширят инициативите на заинтересованите страни, за да се достигне критична маса, която да доведе до промяна на пазара на труда, включително в областта на отбраната. Тези дейности ще бъдат съгласувани с общи цели и ключови показатели за резултатите, за да се постигне по-голямо въздействие.

Акцентът на Академията ще бъде придобиването на умения от **специалисти в областта на киберсигурността**. Дейността на Академията ще допринесе за политиките на ЕС в областта на киберсигурността, както и за образованието и ученето през целия живот. С нея се допълват двете препоръки на Съвета, свързани с цифровото образование и умения, предложени от Комисията едновременно с настоящото съобщение[43].

Академията ще се основава на четири стълба: 1) насърчаване на **генерирането на знания чрез образование и обучение**, като се работи по обща рамка за ролевите профили в областта на киберсигурността и свързаните с тях умения, подобряване на европейското предлагане на образование и обучение, с цел да се отговори на нуждите, изграждане на пътеки за професионално развитие и осигуряване на видимост и яснота по отношение на обученията и сертификатите в областта на киберсигурността, за да се подобри предлагането на работна ръка; 2) осигуряване на по-добро насочване и видимост на наличните **възможности за финансиране** на дейности, свързани с уменията, за да се увеличи максимално тяхното въздействие; 3) приканване на заинтересованите страни **да предприемат действия**; и 4) определяне на показатели за **наблюдение на развитието на пазара** и възможност за оценка на ефективността на техните действия.

---

[40] Като например инструментът CEDEFOP: Skills-OVATE | CEDEFOP (europa.eu)

[41] Писмо за намерения относно състоянието на Европейския съюз през 2022 г. до председателя Roberta Metsola и до министър-председателя Petr Fiala

[42] Съвместно съобщение до Европейския парламент и Съвета „Политика на ЕС за киберотбрана“, JOIN(2022) 49 final

[43] Предложения за препоръки на Съвета относно факторите, от които зависи успехът на цифровото образование и обучение, и относно подобряването на предоставянето на цифрови умения в образованието и обучението.

Създаването на Академията ще бъде подкрепено с финансиране в размер на 10 милиона евро от програмата „Цифрова Европа“[44].

3.2. Управление на Академията

В крайна сметка, за да се осигури инфраструктура, която да служи като **единна входна точка** за насърчаване на сътрудничеството между академичните среди, доставчиците на обучение и сектора, където да се срещат и обучават предлагащите и търсещите страни на екосистемата на ЕС за киберсигурност, Академията би могла да бъде под формата на **консорциум за европейска цифрова инфраструктура (КЕЦИ)**[45]. Този инструмент ще позволи на държавите членки да работят съвместно за преодоляване на недостига на умения в областта на киберсигурността, както и да си сътрудничат тясно с Комисията, ENISA и Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността (ECCC), в съответствие с техните мандати и компетенции, и да привлекат всички заинтересовани страни, но и да насочат европейските, националните и частните инвестиции към общата цел. За тази цел заинтересованите държави членки се насърчават да представят на Комисията до 30 май 2023 г. предварително уведомление, че ще подадат заявление за КЕЦИ. Това доброволно предварително уведомяване ще позволи на Комисията да направи ранни коментари по проекта на заявлението за КЕЦИ, като по този начин ще даде възможност за неговото по-нататъшно разработване и официално представяне по по-бърз начин. По време на целия процес и доколкото е поискано от държавите членки, Комисията, в ролята си на ускорител на многонационални проекти, ще улесни изготвянето на заявлението за КЕЦИ. След положителна оценка на заявлението от Комисията и одобрение от комитета по програмата „Цифрово десетилетие“, Комисията ще издаде решение за създаване на КЕЦИ и впоследствие ще подпомогне координирането на изпълнението на КЕЦИ[46].

Междувременно, докато тече официалното създаване на КЕЦИ, Комисията ще създаде виртуална единна входна точка чрез подобряване на **платформата на Комисията за цифрови умения и работни места**[47] с помощта на проекта „Подкрепа на Европейската общност за киберсигурност“ (ECCO) [48].

ENISA ще допринася за изпълнението на Академията в съответствие с целите на агенцията[49], по-специално по отношение на подпомагането на образованието и обучението в областта на киберсигурността, и като взема предвид задълженията си за

---

[44] Регламент (ЕС) 2021/694 на Европейския парламент и на Съвета от 29 април 2021 г. за създаване на програмата „Цифрова Европа“ и за отмяна на Решение (ЕС) 2015/2240

[45] КЕЦИ са създадени с член 13 и следващи от Решение (ЕС) 2022/2481 на Европейския парламент и на Съвета от 14 декември 2022 г. за създаване на политическа програма „Цифрово десетилетие“ до 2030 г.

[46] Пак там, член 12.

[47] Начало | Платформа за цифрови умения и работни места (europa.eu)

[48] Вж. Европейски център и мрежа за промишлени, технологични и изследователски експертни познания в областта на киберсигурността: нов проект, финансиран от ЕС, в подкрепа на кибернетичната общност (europa.eu). През декември 2022 г. Европейската комисия подписа договор на стойност 3 милиона евро за подкрепа на кибернетичната общност на ЕС в рамките на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността. Този проект ще допринесе за постигане на целите на ЕС за изграждане на общност и капацитет във връзка с научните изследвания, иновациите, използването и промишлената база в областта на киберсигурността.

[49] „ENISA подпомага изграждането на капацитет и подготвеността в целия Съюз, като съдейства на институциите, органите, службите и агенциите на Съюза, както и на държавите членки и заинтересованите страни от публичния и частния сектор, с цел […] развиване на уменията и знанията в областта на киберсигурността.“ (член 4, параграф 3 от Акта за киберсигурността).

докладване съгласно Директивата МИС 2[50]. **ECCC** ще работи в съответствие със своята стратегическа програма, за да подкрепи изпълнението на Академията на ЕС за киберумения. Особено важно е, че ECCC ще изпълни стратегическа цел 3 (киберсигурност) на програмата „Цифрова Европа“. Той ще се ползва от подкрепата на Комисията и държавите членки чрез **Националните координационни центрове (НКЦ)**. В случаите, когато е уместно, ще бъде привлечена **групата за сътрудничество**, създадена в съответствие с Директивата МИС 2[51]. И накрая, за постигането на целта на Академията за преодоляване на недостига на умения в областта на киберсигурността ще е необходимо да се обединят усилията на **отрасъла** и **Академията**.

4. Генериране на знания и обучение: създаване на общ подход на ЕС към обучението по киберсигурност

В рамките на стълба за генериране на знания и обучение на Академията на ЕС за киберумения ще бъде разработен структуриран подход с ясната цел да се увеличи **броят** на лицата с умения в областта на киберсигурността в ЕС, да се насочи по-добре обучението към **нуждите на пазара** и да се осигури видимост на **пътеките за професионално развитие**.

4.1.Да говорим на един и същи език: общ подход по отношение на ролевите профили и свързаните с тях умения в областта на киберсигурността

ENISA вече работи за определяне на ролевите профили на специалистите в областта на киберсигурността в рамките на Европейската рамка за умения в областта на киберсигурността (**ECSF**)[52]. Това следва да се превърне в основа за Академията за определяне и оценяване на съответните умения, за проследяване на промените по отношение на недостига на умения и предоставянето на насоки за новите нужди. За всяка роля в областта на киберсигурността от ECSF като елемент от описанието[53] на профила е включен набор от умения от приложимата европейска рамка за електронните компетентности[54].

Ето защо ENISA ще преразгледа ECSF и ще **определи променящите се нужди от умения и недостига** по отношение на работната сила в областта на киберсигурността, включително чрез авангардни инструменти (напр. изкуствен интелект, големи данни[55], извличане на данни). За тази цел ENISA ще работи под ръководството на КЕЦИ, когато бъде създаден, ECCC, заедно с НКЦ, Комисията, проекта ECCO, и участниците на

---

[50] Член 18 от Директивата МИС 2.

[51] Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2)

[52] Европейска рамка за умения в областта на киберсигурността (ECSF) — ENISA (europa.eu) — ECSF подпомага идентифицирането и формулирането на задачи, компетенции, умения и знания, свързани с ролите на европейските специалисти в областта на киберсигурността. В нея са обобщени всички роли, свързани с киберсигурността, в профили, които се анализират поотделно в детайли по отношение на съответните отговорности, умения, полезни взаимодействия и взаимозависимости.

[53] В тази връзка вж. Ръководство за потребителя — Европейска рамка за умения в областта на киберсигурността (ECSF) — септември 2022 г.

[54] Европейска рамка за електронните компетентности (e-CF) | Esco (europa.eu) — e-CF осигурява последователни връзки в контекста на квалификациите в областта на ИКТ и други рамки от значение за сектора, сред които DigComp

[55] Вж. например Skills-OVATE, разработен от Cedefop.

пазара[56]. Що се отнася до работната сила в областта на киберотбраната, ENISA ще вземе надлежно под внимание работата, извършена от ЕКСО. По същия начин в областта на борбата с киберпрестъпността ENISA ще вземе предвид дейностите, извършвани от Агенцията на Европейския съюз за обучение в областта на правоприлагането (CEPOL) и Европол при изготвянето на анализ на нуждите от оперативно обучение[57] във връзка с кибератаките.

ECSF ще бъде редовно допълвана и преразглеждана в рамките на Академията през двугодишен цикъл. В допълнение Комисията и Европейската служба за външна дейност ще допринесат за определянето на специфични профили и свързаните с тях умения за секторите, ако е необходимо, с подкрепата на агенции и органи на ЕС, като например ЕКСО[58], Европол и CEPOL[59].

Връзки ще бъдат създадени също между ECSF и съответните инструменти на политиката на ЕС по заетостта[60]. По-специално профилите на длъжностите на ECSF, както и свързаните с тях умения, ще бъдат интегрирани в **Европейската класификация на уменията, компетентностите, квалификациите и професиите (ESCO)**. Това ще подобри класификацията и връзките между професиите и уменията в областта на киберсигурността, като се улесни повишаването на квалификацията и преквалификацията на специалистите и се подпомогне намирането на работа въз основа на уменията, както и трансграничната мобилност.

4.2.Насърчаване на сътрудничеството за разработване на програми за образование и обучение в областта на киберсигурността

След създаването на КЕЦИ Академията следва да получава подкрепа от държавите членки, за да се превърне в **референтно място в Европа за разработване и провеждане на обучения по киберсигурност**, насочени към най-търсените умения, и да предоставя възможности за обучения и стажове в работна среда за стартиращи предприятия и МСП, както и за публичните администрации, в иновативни дружества и центрове за компетентност в областта на киберсигурността. КЕЦИ следва да работи с всички заинтересовани страни, включително отрасъла, при разработването на такива обучения, както и да се основава на проекти като **CyberSecPro**[61], който е финансиран от програмата „Цифрова Европа“ и обединява 17 висши училища и 13 дружества за

[56] Агенцията ще продължи да използва резултатите от други проекти, финансирани от ЕС (например REWIRE, Data Space For Skills (DS4S), CyberSecPro, Concordia) и методологии, произтичащи от подобни инициативи (например „Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom and United States“ — „Изграждане на квалифицирана работна сила в областта на киберсигурността в пет държави: данни от Австралия, Канада, Нова Зеландия, Обединеното кралство и Съединените щати“, доклад на ОИСР, представен на 21 март 2023 г.), за да се осигури в бъдеще актуална представа за нуждите в среда, в която търсенето непрекъснато се развива.

[57] CEPOL Operational Training Needs Assessment (OTNA) („Оценка на нуждите от оперативно обучение“)

[58] Вж. в тази връзка Съвместно съобщение до Европейския парламент и Съвета „Политика на ЕС за киберотбрана“, JOIN(2022) 49 final

[59] В тази връзка ще бъде обърнато внимание на работата по Рамката за компетентност за обучение по киберпрестъпност (TCF), която се разработва в момента.

[60] Като например Европейската класификация на уменията, компетентностите, квалификациите и професиите (ESCO), Europass, европейската мрежа за сътрудничество на службите по заетостта (EURES).

[61] CyberSecPro — В рамките на този проект например ще се извърши анализ на програмите, курсовете и летните училища по киберсигурност, предлагани в университетите, и на използваните таблици за оценка по Европейската система за трансфер и натрупване на кредити (ECTS), ще се осигури ангажирането на целевия брой от над 530 стажанти за тригодишния период, ще се обучат външни лица от различни отрасли и сектори.

сигурност от 16 държави членки, за да се превърне в най-добрата практика за всички програми за обучение по киберсигурност.

Академията ще работи с всички заинтересовани страни за **привличане на младите поколения** към кариера в областта на киберсигурността. В съответствие с предложението за препоръка на Съвета относно по-доброто предоставяне на цифрови умения в образованието и обучението държавите членки следва да създадат и засилят мерки за наемане и обучение на специализирани учители и обучители, както и да улеснят придобиването на умения в областта на киберсигурността, включително чрез възможности за чиракуване. Следва да се насърчава включването на киберсигурността в програмите за образование и обучение, като същевременно се гарантира тяхната достъпност, разработват се предложения за **чиракуване** и стажове, насърчават се новаторски подходи, включително например сериозни игри и споделени платформи за симулации, организират се седмици за интегриране в длъжности, свързани с киберсигурността, изясняват се нетехническите ролеви профили на длъжностите. Участието в тези възможности за обучение по киберсигурност на труднодостъпни групи, като например младежи с увреждания, живеещи в отдалечени или селски райони и от други малцинствени групи, също следва да бъде подкрепено.

Комисията ще продължи да оказва подкрепа за разработването на програми за микроквалификации, професионално образование и обучение. По-специално **съвместни бакалавърски и магистърски програми, съвместни курсове или модули, които могат да донесат микроквалификации** и **смесени интензивни програми**[62] по всички теми, включително **киберсигурността,** ще продължат да се финансират в рамките на програма „Еразъм+“. По-нататъшното разгръщане на **инициативата „Европейски университети“**[63] и на **центровете за високи постижения в областта на професионалното образование**[64] също ще бъде подкрепено, за да се насърчи засилването на сътрудничеството между висшите училища и съответните институции за професионално образование и обучение в цяла Европа. Програмите за финансиране от Съюза, включително „Еразъм+“ и програмата „Цифрова Европа“, ще подкрепят тази цел за задълбочаване на сътрудничеството, както и средствата на ЕС за разработване на **индивидуални сметки за обучение**[65].

За да се улесни сътрудничеството на национално равнище между академичните среди и доставчиците на обучение за придобиване на умения в областта на киберсигурността с работодателите от частния и публичния сектор, както и да се насърчат полезните взаимодействия между публичния и частния сектор, НКЦ се приканват да проучат възможността за създаване на **киберкампуси** в държавите членки. Целта на киберкампусите ще бъде да осигурят центрове за високи постижения на национално равнище за кибернетичната общност, а Академията ще подпомогне създаването на мрежи и по-нататъшната координация на техните дейности.

ENISA също ще подобри предлаганото от нея обучение по киберсигурност, като приведе **своя каталог с курсове**[66] в съответствие с профилите на ECSF и разработи

[62] Смесените интензивни програми съчетават онлайн преподаване с кратък период на физическа мобилност.

[63] Инициатива „Европейски университети“ | Европейско пространство за образование (europa.eu)

[64] Центрове за високи постижения в областта на професионалното образование и обучение | „Еразъм+“ (europa.eu)

[65] В съответствие с Препоръка на Съвета от 16 юни 2022 г. относно индивидуални сметки за обучение

[66] Курсове за обучение — ENISA (europa.eu)

модули за обучение по всеки профил, което може да подобри предлаганото от държавите членки обучение. ENISA също така ще разшири своята **програма за обучение на обучители**[67], насочена към професионалните нужди на EUIBA, публичните органи на държавите членки и **публичните и частните оператори от критично значение** в обхвата на Директивата МИС 2.

Освен това други агенции и органи на ЕС ще засилят предлаганото от тях обучение по киберсигурност. Например в изпълнение на политиката на ЕС в областта на киберотбраната **ЕКСО** ще разработи нов набор от курсове по киберсигурност и ще приведе някои от настоящите си курсове в съответствие с ECSF. Тези курсове ще завършват със сертифициране на резултатите от обучението[68]. ЕКСО, в сътрудничество с Комисията, ще проучи възможността за интегриране на сертификатите в портфейла за европейска цифрова самоличност (EUeID). ЕКСО ще проучи допълнително възможните механизми за оценка на уменията, въз основа на които ще се издават сертификатите. По същия начин в областта на борбата с киберпрестъпността ще се търсят тесни връзки с **Академията на CEPOL за киберпрестъпността**[69], за да се насърчат полезните взаимодействия и взаимното допълване при разработването и изпълнението на програмите за обучение.

4.3. Създаване на полезни взаимодействия и осигуряване на видимост на обученията и сертифицирането в областта на киберсигурността в държавите членки

Академията следва да разгледа въпроса за видимостта и полезните взаимодействия на обучението и сертифицирането. Това би било от полза за гражданските, отбранителните, правоприлагащите и дипломатическите кибернетични общности, тъй като в много случаи всички сектори се нуждаят от едни и същи експертни познания, основани на сходни учебни програми и резултати от обучението.

Академията ще осигури **единна входна точка** за лицата, които се интересуват от кариера в областта на киберсигурността. В краткосрочен план това ще се осъществи чрез подобряване на **платформата за цифрови умения и работни места** на Комисията с подкрепата на проекта ECCO. Специален раздел, посветен на кариерите в областта на киберсигурността, ще бъде свързан със съществуващите инструменти — от програмите за висше образование, през възможностите за обучение, включително курсове, водещи до придобиване на микроквалификации, и програмите за професионално образование и обучение, до предложенията за работа. Това ще бъде постигнато чрез препратки или интегриране в платформата на текущата работа и инициативи, като например тези на ENISA, която в сътрудничество с академичните среди създаде **карта на образователните институции**, предлагащи програми в областта на киберсигурността. Това ще бъде допълнително засилено с подкрепата на НКЦ. Освен това ще бъдат разработени и консолидирани две **хранилища на съществуващи обучения от публичния и частния сектор и на сертификати за киберсигурност** от ENISA с подкрепата на НКЦ, Комисията и проекта ECCO, както и

[67] Програма за обучение на обучители — ENISA (europa.eu)

[68] В съответствие с член 20, параграф 4 от Решение (ОВППС) 2020/1515 на Съвета от 19 октомври 2020 г. за създаване на Европейски колеж по сигурност и отбрана и за отмяна на Решение (ОВППС) 2016/2382

[69] Академията на CEPOL за киберпрестъпност беше създадена през 2019 г., за да се осигури модерна платформа за подобряване на знанията за киберпрестъпността и кибернетичният капацитет в Европа.

в сътрудничество със структури, предоставящи сертификати и участващи в други съответни инициативи[70]. Те също ще бъдат интегрирани в единната входна точка на платформата за цифрови умения и работни места. Тази работа ще бъде от полза и за НКЦ, чиято задача е по-специално да се насърчават и разпространяват образователни програми в областта на киберсигурността[71].

Необходимо е също така да се предоставят гаранции на специалистите, че обученията, в които участват, са с необходимото качество. В тази връзка ENISA ще разработи **пилотен проект** за проучване на създаването на европейска схема за атестиране на уменията в областта на киберсигурността.

Освен това определянето на уменията и обученията и свързването им с профила на длъжността е от съществено значение, но също така е важно да се гарантира, че услугите в областта на киберсигурността се предоставят с необходимата компетентност, експертни познания и опит. Това важи с особена сила за доставчиците на управлявани услуги за сигурност в области като реакция на инциденти, тестване за пробив, одити на сигурността и консултации. В Директивата МИС 2 и в предложението за законодателен акт за киберсолидарност се определят конкретни задачи за такива доставчици на управлявани услуги за сигурност. Поради това Комисията предлага и **целенасочено изменение на Акта за киберсигурността**[72], за да се даде възможност за определяне на схеми за сертифициране на управлявани услуги за сигурност на равнището на ЕС. Такива схеми за сертифициране следва да имат за цел, наред с другото, да гарантират, че тези услуги се предоставят от персонал с много високо ниво на технически познания и компетентност в съответните области.

Механизмите за осигуряване на качество и признаване на микроквалификации[73] улесняват постигането на прозрачност, сравнимост и преносимост на резултатите от обучението. В съответствие с Препоръката на Съвета относно европейския подход към микроквалификациите[74] държавите членки се насърчават да включат микроквалификациите за киберсигурност в своите национални квалификационни рамки. Това ще им позволи да свържат микроквалификациите за киберсигурност с Европейската квалификационна рамка[75]. Инфраструктурата за европейски цифрови удостоверения за учене е на разположение за издаване на цифрово подписани

[70] Например W4C Academy — Women4Cyber или Global Cybercrime Certification project за правоприлагащи и съдебни органи.

[71] „1. Националните координационни центрове имат следните задачи: [...] ж) без да се засягат националните компетентности на държавите членки в областта на образованието и като се вземат предвид съответните задачи на ENISA, да взаимодействат с националните органи по отношение на възможния принос за насърчаване и разпространение на образователни програми в областта на киберсигурността“, член 7, параграф 1, буква ж) от Регламента за Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове. Вж. също свързаното съображение 28.

[72] Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността)

[73] Например документи или сертификати за резултатите от обучението, които лицата придобиват след кратки обучения.

[74] Препоръка на Съвета относно европейски подход към микрокредитите с цел стимулиране на ученето през целия живот и пригодността за заетост

[75] Препоръка на Съвета от 22 май 2017 г. относно Европейската квалификационна рамка за учене през целия живот и за отмяна на препоръката на Европейския парламент и на Съвета от 23 април 2008 г. за създаване на Европейска квалификационна рамка за обучение през целия живот

удостоверения за квалификации и микроквалификации за киберсигурност на физически лица. Те съдържат богати данни, включително за резултатите от обучението по киберсигурност, и могат да се съхраняват в бъдещия цифров портфейл **EUeID**[76].

Действия в рамките на Академията

Държавите членки и отрасълът

- Осигуряване на подкрепа за разработването и признаването на **микроквалификации за обучение по киберсигурност** в съответствие с Препоръката на Съвета относно европейски подход към микрокредитите.
- Включване на квалификациите по киберсигурност, включително микроквалификациите, в **националните квалификационни рамки**.
- Осигуряване на **възможности за обучение в работна среда** чрез чиракуване за лицата, които участват в инициативи за развитие на уменията в областта на киберсигурността.

Комисията

- В краткосрочен план — създаване на **единна входна точка за** програми за киберсигурност, съществуващи обучения и за сертификати за киберсигурност чрез **платформата за цифрови умения и работни места** до края на 2023 г.
- Предлагане (на 18 април 2023 г.) на изменение на **Акта за киберсигурността**, което да позволи сертифицирането на доставчици на управлявани услуги за сигурност.

Органите и агенциите на ЕС

- Утвърждаване на **ECSF** като общ подход по отношение на ролевите профили и свързаните с тях умения в областта на киберсигурността до края на 2023 г.
- поставя през второто тримесечие на 2023 г. началото на разработването на пилотен проект за създаване на **европейска схема за атестиране** на умения в областта на киберсигурността.
- ENISA преразглежда своя **каталог с курсове** и открива своята програма за **обучение на обучители** за публични и частни оператори от критично значение до края на 2023 г.
- Завършване на **привеждането на учебните програми на ЕКСО в съответствие с ECSF** до средата на 2023 г.

5. Участие на заинтересованите страни: поемане на ангажимент за преодоляване на недостига на умения в областта на киберсигурността

В рамките на Академията ще бъде разработен координиран подход за участие на заинтересованите страни, за да се преодолее недостигът на умения в областта на киберсигурността. Целта ще бъде да се увеличи максимално видимостта и въздействието на ангажиментите на различните заинтересовани страни за намаляване на недостига на умения в областта на киберсигурността.

[76] Предложение за Регламент на Европейския парламент и на Съвета за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на рамка за европейска цифрова самоличност

Комисията приканва заинтересованите страни да поемат конкретни ангажименти чрез мерки за повишаване на квалификацията и за преквалификация на работниците чрез специални действия, които да се основават в максимална степен на установения недостиг на умения в областта на киберсигурността. Такива ангажименти на **заинтересованите страни в областта на киберсигурността** следва да бъдат отразени в **платформата за цифрови умения и работни места**, подобно на други ангажименти в областта на цифровите технологии, които вече са видими в платформата. Освен това Комисията насърчава заинтересованите страни, които поемат ангажимент в областта на киберсигурността в рамките на платформата, да се присъединят към **цифровото широкомащабно партньорство в рамките на Пакта за умения**[77]. Насърчава се представянето на ангажиментите в областта на киберсигурността, поети в рамките на цифровото широкомащабно партньорство, на платформата за цифрови умения и работни места. По подобен начин се насърчава отразяването на ангажиментите, поети в рамките на платформата за цифрови умения и работни места, в рамките на цифровото широкомащабно партньорство на Пакта за умения.

Комисията освен това призовава държавите членки да **положат усилия за прилагане на Декларацията за жените в областта на цифровите технологии**[78], за да насърчат жените да играят активна и значима роля в сектора на цифровите технологии и за постигане на конвергенция между половете на длъжностите в областта на киберсигурността. Комисията също така насърчава държавите членки да развиват полезни взаимодействия с програмите си по **Европейския социален фонд+** (ЕСФ+), за да подкрепят допълнително целта за равенство между половете на пазара на труда[79], например чрез създаване на програми за **наставничество за момичета и жени.** Чрез тях може да се улесни изграждането на ролеви модели за привличане на момичета към професии в областта на киберсигурността, като същевременно ще се подпомогне преодоляването стереотипите, свързани с пола. Освен това ще се насърчи повишаването на квалификацията и преквалификацията на жените, както и изграждането на общност, която може да подпомогне навлизането или кариерата на жените на пазара на труда в сектора на киберсигурността.

Държавите членки следва да приемат, като част от **националните си стратегии за киберсигурност, конкретни мерки за намаляване на недостига на умения в областта на киберсигурността**[80], които набелязват и насочват по-добре усилията за преодоляване на недостига на умения и в крайна сметка гарантират правилното изпълнение на техните задължения съгласно Директивата МИС 2.

Някои държави членки се възползват от **полезни взаимодействия между инициативи в гражданската и отбранителната област и в областта на правоприлагането**. Например увеличаването на работната сила с помощта на задължителната военна служба или използването на специалисти по киберотбрана от запаса, които са военно обучени граждани, заемащи длъжности в областта на киберсигурността във

[77] Нови европейски партньорства, стартирани с цел постигане на амбициите за цифровото десетилетие на Европа | Стратегия в областта на цифровите технологии (europa.eu), създадена в рамките на Пакта за умения за преодоляване на недостига на кадри в областта на информационните и комуникационните технологии (ИКТ)

[78] EU countries commit to boost participation of women in digital („Държавите от ЕС се ангажират да увеличат участието на жените в цифровите технологии“) | Стратегия в областта на цифровите технологии (europa.eu)

[79] Регламент (ЕС) 2021/1057 на Европейския парламент и на Съвета от 24 юни 2021 г. за създаване на Европейския социален фонд плюс (ЕСФ+) и за отмяна на Регламент (ЕС) № 1296/2013, член 4, параграф 1, буква в)

[80] Директива МИС 2, член 7, параграф 2, буква е).

въоръжените сили[81], позволява на населението, и особено на младите хора, да повишат уменията си в областта на киберсигурността и киберотбраната. Това важи и за **борбата с киберпрестъпността**, тъй като съществуват много сходства между общите усилия в областта на киберсигурността и дейностите на правоприлагащите органи в отговор на киберинциденти. Комисията насърчава дискусиите между държавите членки по такива инициативи и ги приканва да преценят как квалифицираната работна сила може да служи най-добре както на отбранителната, така и на гражданската общност в областта на киберсигурността.

Комисията ще обмисли предложения за това как да преодолее настоящия и очаквания недостиг, установен при прегледа на нуждите на EUIBA. Тя по-специално ще насърчи служителите да се възползват от откриващата се възможност за **стипендия за киберсигурност между ЕС и Съединените щати (САЩ)**, създадена в рамките на диалога между ЕС и САЩ.

Действия в рамките на Академията

Отрасълът

- Предлагане на конкретни **ангажименти в областта на киберсигурността** в рамките на платформата за цифрови умения и работни места, считано от 18 април 2023 г.

Държавите членки

- Включване в **националните стратегии за киберсигурност** на конкретни мерки за преодоляване на недостига на умения в областта на киберсигурността.

Държавите членки и отрасълът

- Прилагане на Декларацията за жените в областта на цифровите технологии и постигане на **конвергенция между половете на длъжностите в областта на киберсигурността** до 2030 г.

6. Финансиране: изграждане на полезни взаимодействия с цел максимално увеличаване на въздействието на инвестициите за развитие на умения в областта на киберсигурността

В рамките на Академията въздействието на инвестициите в умения в областта на киберсигурността ще бъде увеличено в максимална степен чрез осигуряване на обща входна точка, улесняване на по-доброто насочване на средствата към нуждите на пазара и интегриране на използването на финансирането, улесняване на полезните взаимодействия между различните инструменти, като същевременно се избягва дублиране на усилията[82].

6.1. Съобразяване на финансовите средства с нуждите

[81] Доклад — Cyber Conscription: Experience and Best Practice from Selected Countries, Martin Hurt and Tiia Sõmer, International Centre for Defence and Security („Опит и най-добри практики от избрани държави“, Мартин Хърт и Тия Симер, Международен център за отбрана и сигурност“) февруари 2021 г.

[82] Възможности за финансиране (europa.eu) — Чрез службите за подкрепа на Пакта за умения се осигурява единна входна точка за информация за финансиране на уменията, включително за цифровата екосистема. Службите за подкрепа на Пакта за умения предоставят обща информация за инструментите за финансиране, които не са конкретно насочени към уменията в областта на киберсигурността, въпреки че тяхната работа следва да бъде взета предвид от Академията, за да се избегне дублиране.

В рамките на Академията ЕССС, с подкрепата на Комисията, проекта ЕССО и НКЦ, ще събере **информация за това как средствата на ЕС се използват за финансиране на уменията в областта на киберсигурността** и ще оцени как средствата на ЕС подпомагат намаляването на недостига на умения в областта на киберсигурността. Въз основа на тази обобщена информация, ЕССС ще се опита да осигури по-добро насочване на средствата на ЕС към установените нужди. По този начин ще се финансират действия за преодоляване на недостига на работна сила в областта на киберсигурността, където е най-неотложно, включително там, където е свързано с изпълнението на нуждите на политиката за киберсигурност.

6.2. Осигуряване на видимост на наличните средства и партньорски инициативи за умения в областта на киберсигурността

В краткосрочен план **платформата за цифрови умения и работни места** ще се превърне в единна входна точка за заинтересованите страни, където ще бъде налична цялата информация за възможностите за финансиране на умения в областта на киберсигурността.

ЕС инвестира в хората и техните умения и използва партньорства, особено с отрасъла, за да мобилизира действия за повишаване на квалификацията и преквалификация чрез няколко инструмента, определени в рамките на **Европейската програма за умения**[83], по-специално **Пакта за умения**[84] и **плана за действие в областта на цифровото образование**[85]. Програмата „**Цифрова Европа**“ финансира възможности за придобиване на умения в областта на киберсигурността, по-специално чрез инициативи за многонационални проекти, като ясно допълва подкрепата, предлагана от „Хоризонт Европа“ за научни изследвания и иновативни технологични решения в областта на киберсигурността. **Европейският фонд за отбрана**[86] финансира научноизследователската дейност и разработването на технологии за провеждане на ефективни кибернетични операции, включително обучения и учения[87]. „**Еразъм+**“ ще продължи да подкрепя такива инициативи, включително чрез смесени интензивни програми и проекти за сътрудничество.

Държавите членки се насърчават да мобилизират средствата на ЕС, които пряко управляват, в подкрепа на уменията и работните места в областта на киберсигурността. Фондовете на политиката на сближаване, като **Европейския фонд за регионално развитие (ЕФРР)** и **ЕСФ+**, имат значителен потенциал за полезни взаимодействия в това отношение[88]. Обхватът на действията по **Механизма за възстановяване и устойчивост** (МВУ)[89] и **InvestEU**[90] включва допълнителни ключови фактори за постигане на целите на Академията.

---

[83] Европейска програма за умения — Заетост, социални въпроси и приобщаване — Европейска комисия (europa.eu)

[84] Инструменти на ЕС за финансиране за повишаване на квалификацията и преквалификация — Европейска комисия (europa.eu)

[85] План за действие в областта на цифровото образование за периода 2021—2027 г.

[86] Регламент (ЕС) 2021/697 на Европейския парламент и на Съвета от 29 април 2021 г. за създаване на Европейски фонд за отбрана и за отмяна на Регламент (ЕС) 2018/1092

[87] Държавите членки са поели ангажимент за съвместни обучения и учения, например чрез създаване и участие в проекти за кибернетично обучение и учения в рамките на постоянното структурирано сътрудничество (PESCO), като например Европейски център за кибернетични академични изследвания и иновации (EU CAIH) и Федеративни киберполигони

[88] Член 3, параграф 1 от Регламент (ЕС) 2021/1058 и член 4, параграф 1, буква ж) от Регламент (ЕС) 2021/1057.

[89] Например, в естонския план за възстановяване и устойчивост се предвиждат инвестиции (10 милиона евро) в цифрови умения, които ще включват преразглеждане на обученията, достъпни за експертите в областта на ИКТ,

Действия в рамките на Академията

Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и ENISA

- **Изготвяне на карта на** съществуващото финансиране от Съюза за умения в областта на киберсигурността спрямо нуждите на пазара, оценка на **ефективността** и определяне на **приоритетите за финансиране** до края на 2024 г.

Комисията

- Създаване на **единна входна точка** за възможностите за финансиране на умения в областта на киберсигурността в платформата за цифрови умения и работни места до края на 2023 г.

7. Измерване на напредъка: вградена отчетност

В рамките на Академията ще бъде разработена **методология**, която ще позволи **измерване на напредъка по отношение на преодоляването на недостига на умения в областта на киберсигурността**.

7.1. Определяне на показатели за киберсигурност за наблюдение на развитието на пазара на труда в областта на киберсигурността

Индексът за навлизането на цифровите технологии в икономиката и обществото (DESI) обобщава съответните показатели за постиженията на Европа в областта на цифровите технологии и проследява развитието на държавите — членки на ЕС. В рамките на Академията за умения в областта на киберсигурността ENISA, в сътрудничество с Комисията и групата за сътрудничество за МИС[91], ще разработи **показатели**, включително свързани с пола, за проследяване на напредъка на държавите — членки на ЕС, по отношение на увеличаването на броя на специалистите в областта на киберсигурността, като се консултира и със съответните участници на пазара и НКЦ. ENISA ще използва методологията на DESI[92] и ще гарантира, че показателите са в съответствие с цифровите цели на Европа по отношение на специалистите в областта на ИКТ и постигането на конвергенция между половете в областта на ИКТ. След това Комисията ще работи за интегрирането на тези показатели

ще се финансира повишаване на квалификацията и преквалификация на специалистите в областта на ИКТ по киберсигурност и ще се допринесе за изготвянето на пилотна програма за преработване на квалификационната рамка за специалисти в областта на ИКТ.

[90] Заинтересованите страни (напр. доставчици на обучение и дружества, които искат да разработят или подобрят своите дейности за обучение в областта на киберсигурността) могат да се обърнат към консултантския център InvestEU, който предоставя техническа подкрепа и помощ, включително изграждане на капацитет, на разработчици на проекти и структури, и да се консултират с портала InvestEU.

[91] Изготвяне и допълване на методологията, която ще бъде разработена от ENISA за целите на двугодишния доклад на агенцията за състоянието на киберсигурността в Съюза в съответствие с член 18, параграф 3 от Директивата МИС 2.

[92] Вж. методологическата бележка към индекса за навлизането на цифровите технологии в икономиката и обществото (DESI) за 2022 г., достъпна на адрес Индексът за навлизането на цифровите технологии в икономиката и обществото (DESI) | Стратегия в областта на цифровите технологии (europa.eu)

в DESI**,** като по този начин ще се даде възможност за проследяване на годишна база на състоянието на уменията и пазара на труда в областта на киберсигурността.

7.2.Събиране на данни и докладване

ENISA ще събира данни за показателите с подкрепата на проекта ECCO и НКЦ. Въз основа на събраните данни ENISA ще изготвя **годишен доклад**, който ще се използва за Доклада за състоянието на Цифровото десетилетие[93], който на свой ред, заедно с DESI, ще бъде включен в специфичните за всяка държава анализ и препоръки[94] на **европейския семестър**. Освен това показателите за уменията в областта на киберсигурността ще бъдат взети предвид в **двугодишния доклад на ENISA** за състоянието на киберсигурността в ЕС, предвиден в Директивата МИС 2, обхващащ способностите, осведомеността и хигиената в областта на киберсигурността в целия ЕС.

7.3.Изготвяне на ключови показатели за резултатите (КПР) в областта на киберсигурността

С цел преодоляване на недостига на таланти в областта на киберсигурността, ENISA, в тясно сътрудничество с Комисията и НКЦ, ще предложи на Комисията ключови показатели за резултатите, като се основава на методологията от политическата програма „Цифрово десетилетие“ до 2030 г., както и на опита на отрасъла. ENISA ще вземе надлежно под внимание ключовите показатели за резултатите, използвани от държавите членки за оценка на техните национални стратегии за киберсигурност[95].

Действия в рамките на Академията

Агенция на Европейския съюз за киберсигурност (ENISA)

- Изготвяне на **показатели и КПР** за уменията в областта на киберсигурността до края на 2023 г.
- **Събиране на данни** за показателите и изготвяне на доклади за тях, като първото събиране ще се извърши до 2025 г.

Комисията

- Работа за интегрирането на **показателите за киберсигурността в DESI** и в **Доклада за състоянието на цифровото десетилетие на Европа**.

8. Заключение

С настоящото съобщение се поставят основите на нов подход на ЕС за повишаване на уменията в областта на киберсигурността на специалистите в ЕС. Целта е да се намали недостигът на умения в областта на киберсигурността и да се осигури на ЕС необходимата работна сила, за да може той да реагира на постоянно променящата се картина на заплахите, да прилага политиките на ЕС, целящи да предпазят ЕС от кибератаки, но също така и за да се увеличат възможностите за стопанска дейност и да се засили конкурентоспособността. Квалифицираната работна сила в областта на киберсигурността може да бъде от полза за **гражданските, отбранителните,**

[93] Решение (ЕС) 2022/2481 на Европейския парламент и на Съвета от 14 декември 2022 г. за създаване на политическа програма „Цифрово десетилетие“ до 2030 г.

[94] Пак там, съображение 25.

[95] Член 7, параграф 4 от Директива МИС 2.

дипломатическите и правоприлагащите общности и да улесни полезните взаимодействия между тях.

Комисията призовава държавите членки и всички заинтересовани страни да дадат своя принос за постигане на амбициозните цели на Академията на ЕС за киберумения.