

Киберинциденти — откриване и реакция

Рамката на ЕС за сътрудничество се усъвършенства, но все още не функционира пълноценно поради закъснения в изпълнението и ограничен обмен на информация



ЕВРОПЕЙСКА
СМЕТНА
ПАЛАТА

Съдържание

Точки

01—23 | Основни послания

01—07 | Защо тази област е от значение

08—23 | Какво констатира и какво препоръчва ЕСП

24—01 | Подробни констатации и оценки

24—74 | Мрежите и механизмите на ЕС за киберсигурност подпомагат сътрудничеството и действията за реакция, но ограниченият обмен на информация и непълното им прилагане намаляват тяхната ефективност

24—51 | Мрежите на ЕС дават възможност за сътрудничество между държавите членки, но ограниченият обмен на информация намалява тяхната добавена стойност

52—61 | Резервът за киберсигурност на ЕС дава възможност за бързо активиране на услуги за реакция при инциденти

62—74 | Европейската система за предупреждение в областта на киберсигурността има за цел да подобри капацитета за откриване на заплахи, но все още не функционира

75—01 | Финансираните от ЕС проекти по програма „Цифрова Европа“ имат за цел да укрепят киберсигурността, но срещат трудности, свързани с изпълнението и докладването

75—81 | Забавянето при създаването на Експертната общност в сферата на киберсигурността са попречили нуждите ѝ да бъдат взети предвид при изготвянето на програма „Цифрова Европа“

82—96 | Финансираните от ЕС проекти имат подходящи цели, но много от тях са засегнати от оперативни проблеми

97—01 | Повечето финансирани от ЕС проекти не разполагат с подходящи рамки за изпълнение, а данните за изпълнението на програма „Цифрова Европа“, свързани с киберсигурността, са неточни

Приложения

Приложение I — Относно настоящия одит

Приложение II — Среда за киберсигурност на ЕС

Приложение III — Избрани действия в областта на киберсигурността

Приложение IV — Оценка на ЕСП на финансираните от ЕС проекти в областта на киберсигурността

Съкращения

Речник на термините

Отговори на Комисията

Отговори на Европейския център за експертни познания в областта на киберсигурността (ECCC)

Отговори на Агенцията на Европейския съюз за киберсигурност (ENISA)

Хронология

Одитен екип

01

Основни послания

Защо тази област е от значение

- 01** Рисковете от кибератаки се увеличават поради все по-голямата цифровизация на икономиката и ежедневието на гражданите. Киберсигурността се определя като „дейностите, необходими за защита от киберзаплахи на мрежите и информационните системи, на ползвателите на такива мрежи и системи и други лица, засегнати от киберзаплахи“¹. Киберсигурността изисква цялостен подход за предотвратяване, откриване, реакция и възстановяване след киберзаплахи.
- 02** Киберсигурността в ЕС е област, която обхваща множество публични и частни субекти на регионално, национално и европейско равнище в гражданската сфера. Тя е ключов елемент и на националната сигурност и отбрана.
- 03** Държавите членки носят основната отговорност за превенцията, готовността и реакцията при киберинциденти и кризи, които ги засягат. Тъй като тези инциденти могат да имат отражение върху гладкото функциониране на вътрешния пазар, ЕС също играе важна роля в случай на значителен инцидент или криза. През последните години ЕС е доразвил и усъвършенствал нормативната си рамка в областта на киберсигурността² и е създал различни мрежи и механизми, както е показано на [фигура 1](#) по-долу и в [приложение II](#).

¹ Регламент (ЕС) 2019/881 („Акт за киберсигурността“).

² Например Комисията е предложила [Сборен пакет от мерки в областта на цифровите технологии](#) през ноември 2025 г. и преразглеждане на [Акта на ЕС за киберсигурността](#) през януари 2026 г.

Фигура 1 | Мрежи и механизми на ЕС за киберсигурност през периода 2016—2025 г.



ЕРИКС: екипи за реагиране при инциденти с компютърната сигурност

CONNECT: Генерална дирекция „Съобщителни мрежи, съдържание и технологии“ на Европейската комисия

EU-CyCLONe: Европейска мрежа за връзка на организациите при киберкризи

Директива за МИС: Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза

Директива за МИС 2: Директива (ЕС) 2022/2555 относно мерки за високо общо ниво на киберсигурност в Съюза

Източник: Европейска сметна палата (ЕСП).

- 04** Съгласно настоящата многогодишна финансова рамка за периода 2021—2027 г. основният източник на финансиране за областта на киберсигурността е [програмата „Цифрова Европа“](#) (DIGITAL). Тя разполага с общ бюджет от 8,1 млрд. евро, от които 1,4 млрд. евро са заделени за засилване на киберсигурността.
- 05** Целта на одита на ЕСП беше да провери дали действията на ЕС ефективно подпомагат откриването и реакцията при значителни и мащабни киберинциденти. ЕСП разгледа този аспект по отношение на:
- мрежите и механизмите на равнището на ЕС (т.е. мрежата на екипите за реагиране при инциденти с компютърната сигурност (мрежа на ЕРИКС), Европейската мрежа за връзка на организациите при киберкризи (EU-CyCLONe), Европейската система за предупреждение в областта на киберсигурността, Центъра за киберситуации и Резерва за киберсигурност на ЕС);
 - действията, финансирани по програма „Цифрова Европа“.
- 06** ЕСП очаква констатациите ѝ да допринесат за укрепване на киберустойчивостта на ЕС чрез повишаване на ефективността и ефикасността на мрежите и механизмите на ЕС, както и чрез извършването на по-добър подбор и наблюдение на финансираните от ЕС действия.
- 07** Одитът обхваща периода 2022—2025 г. Той се основава на документна проверка и анализ на относимите документи, одитни посещения в три държави членки — Ирландия, Гърция и Италия, както и писмени въпросници и интервюта със съответните заинтересовани страни. Повече информация за обхвата и подхода на одита е представена в [приложение I](#).

Какво констатира и какво препоръчва ЕСП

- 08** Общото заключение на ЕСП е, че действията на ЕС само частично подпомагат откриването и реакцията при значителни и мащабни киберинциденти. Въпреки че необходимата рамка за сътрудничество постепенно се изгражда, тя все още не е изцяло завършена. Ограниченият обмен на информация, слабостите в докладването и значителните закъснения в изпълнението ѝ не позволяват на мрежите и механизмите на ЕС до достигнат пълния си потенциал. В проектите, финансирани по програма „Цифрова Европа“, са заложили подходящи цели, но много от тях са засегнати от оперативни трудности и забавяния, а цялостната рамка за мониторинг на изпълнението показва слабости.
- 09** Настоящата рамка от мрежи и механизми на ЕС за подпомагане на откриването и реакцията при значителни киберинциденти е била изградена с течение на времето. През 2025 г. Съветът е приел [концепция за киберсигурността](#), в която се определя рамката на ЕС за управление на кризи в областта на киберсигурността. ЕСП установи, че този документ до голяма степен прецизира ролите и отговорностите по отношение на управлението на кризи в областта на киберсигурността. Независимо от това процедурните правила относно съвместното сътрудничество между мрежата на ЕРИКС (създадена през 2016 г.) и EU-CyCLONe (официализирана през 2023 г.) все още не са формализирани (точки [24—30](#)).
- 10** ЕСП установи, че обменът на информация чрез тези мрежи е ограничен. Това се дължи главно на забавяния при транспонирането на [Директивата относно мерки за високо общо ниво на киберсигурност в Съюза](#) (Директива МИС 2), трудности при определянето на това дали даден инцидент има трансгранично въздействие, както и на националното законодателство в областта на сигурността, което налага ограничения по отношение на обмена на информация. Нежеланието на държавите членки да споделят навременна и практическа информация значително ограничава добавената стойност на мрежите (точки [31—44](#)).



Препоръка 1

Да се засили обменът на информация между държавите членки

За да се подобри капацитетът за откриване и реакция при киберинциденти, Комисията, с подкрепата на Агенцията на Европейския съюз за киберсигурност (ENISA), следва:

- а) да предложи на групата за сътрудничество в областта на мрежовата и информационната сигурност да извърши подробен анализ на ограниченията, свързани със защитата на националната сигурност, които затрудняват обмена на информация и засягат киберустойчивостта на ЕС, и да набележи правни и технически решения за засилване на обмена на информация при зачитане на границите на националната сигурност;
- б) да направи необходимото (без да се засягат решенията на съзаконодателите), единната входяща точка за уведомления за инциденти, предложена в Сборния пакет от мерки в областта на цифровите технологии, да дава възможност за откриване на потенциални трансгранични инциденти;
- в) да разработи решения, които да позволяват докладване на ENISA на инциденти в реално време.

Целеви срок за изпълнение — букви а) и б) — 2027 г., буква в) — 2028 г.

11 През 2022 г. Комисията е обособила в структурите си сектор „Център за киберситуации“, с цел да подобри ситуационната си осведоменост, което от своя страна следва да ѝ помогне при изпълнението на институционалните ѝ задължения за управление на кризи. Функционирането на Центъра се осъществява до голяма степен чрез договор с външни доставчици на услуги. ЕСП установи, че задачите, изпълнявани от външните доставчици, частично се припокриват със съществуващия капацитет на Агенцията на Европейския съюз за киберсигурност (ENISA) по отношение на ситуационната осведоменост и наблюдението на заплахите. Одиторите считат, че при създаването на Центъра за киберситуации не е оползотворен в достатъчна степен потенциалът за рационализация, тъй като не е взета предвид информацията, с която Комисията и ENISA вече разполагат. Освен това липсата на всеобхватен и подробен план за бъдещето на Центъра след изтичането на горепосочения договор излага на риск дейността му в периода след 2026 г. (точки [45](#)—[51](#)).



Препоръка 2

Да се рационализират способностите на ЕС за ситуационна осведоменост в областта на киберсигурността и да се оптимизира разпространението на информация

За да се повиши ефективността, Комисията следва, в сътрудничество с ENISA, да разгледа възможността за съвместно събиране и анализ на информация за ситуационна осведоменост. Тя следва също така да предостави тази информация и свързаните с нея доклади за киберзаплахите на съответните генерални дирекции и агенции на ЕС.

Целеви срок за изпълнение — 2027 г.

- 12** Със [Законодателния акт в областта на киберсолидарността](#) от 2024 г. се създава Резерв за киберсигурност на ЕС, който има за цел да помага на държавите членки да реагират при големи киберинциденти и възстановяването от тях. Резервът се състои от избрани доставчици на услуги за всяка държава членка, които са в постоянна готовност да реагират при възникване на инциденти. Въпреки че този подход помага да се отговори на специфичните изисквания на държавите членки и да се изгради доверие, наличният бюджет е разделен поравно между държавите и не отчита специфичните им нужди (точки [52—57](#)).
- 13** ЕСП счита, че използването на предварително договорени доставчици дава възможност за своевременно активиране на услуги за реакция при инциденти. Въпреки че Резервът за киберсигурност на ЕС има за цел преди всичко да подпомага действията при реакция и възстановяване от инциденти, той може да се използва за подобряване на готовността, когато не се използва за реакция. Този гъвкав подход може да предотврати неизползването на предплатените услуги. Съществува обаче риск Резервът да се използва предимно за повишаване на готовността, а не за реакция, което би било в противоречие с основното му предназначение (точки [58—61](#)).
- 14** Европейската система за предупреждение в областта на киберсигурността е мрежа от национални и трансгранични киберхъбове, които имат за цел да подобрят откриването, анализа и реакцията при киберзаплахи. ЕСП установи, че към момента на одита, поради значителни забавяния при възлагането на обществени поръчки за инструменти и услуги, два киберхъба (ATHENA и ENSOC) все още не са започнали дейността си, както и че Европейската система за предупреждение в областта на киберсигурността все още не функционира (точки [62—70](#)).

- 15** Една от основните цели на Европейската система за предупреждение в областта на киберсигурността е да насърчава обмена на относима информация между групи от държави членки. Въпреки че това може да разреши някои от въпросите, свързани с обмена на информация, следва да се отбележи, че интегрирането на киберхъбове в и без това сложната среда за киберсигурност е значително предизвикателство. ЕСП установи, че необходимите споразумения за сътрудничество, обща таксономия и стандарти за оперативна съвместимост, необходими за пълноценното функциониране на Европейската система за предупреждение в областта на киберсигурността, все още не са налице (точки [71—74](#)).



Препоръка 3

Да се интегрира Европейската система за предупреждение в областта на киберсигурността в средата за киберсигурност на ЕС

Комисията, съвместно с ENISA и държавите членки, следва да направи необходимото за въвеждането на механизми за сътрудничество и стандарти за оперативна съвместимост, с оглед улесняването на обмена на информация между трансграничните киберхъбове, които са част от Европейската система за предупреждение в областта на киберсигурността, мрежата на екипите за реагиране при инциденти с компютърната сигурност (мрежа на ЕРИКС) и Европейската мрежа за връзка на организациите при киберкризи (EU-CyCLONe).

Целеви срок за изпълнение — 2028 г.

- 16** През 2018 г. Комисията предложи да се създаде Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността (ECCC), който да управлява компонента за киберсигурност на програма „Цифрова Европа“ от 2021 г. нататък. В [Регламента за ECCC](#) се призовава за създаването на Експертна общност в сферата на киберсигурността, състояща се от представители на промишления сектор, академични и научноизследователски организации. След това избрани членове от тази общност следва да сформират Стратегическа консултативна група (SAG) (точки [75—76](#)).

- 17** ЕСП установи закъснения както при придобиването на финансова самостоятелност от страна на ЕССС, така и при създаването на Експертната общност в сферата на киберсигурността и Стратегическата консултативна група. В резултат на това тези структури не са могли да допринесат за изготвянето на работните програми по програма „Цифрова Европа“. ЕСП счита това за пропусната възможност (точки 77—81).
- 18** Одиторите констатираха, че всички проверени проекти са преследвали подходящи цели, които допринасят за постигането на целите на програма „Цифрова Европа“ в областта на киберсигурността. Те установиха обаче случаи, в които качеството или постигнатите резултати не са задоволителни, главно поради закъснения при изпълнението (точки 82—87).
- 19** Регламентът за програма „Цифрова Европа“ предвижда, че от съображения за сигурност финансирането за киберсигурност може да бъде ограничено до субекти, установени в държавите членки и контролирани от тях или от техни граждани. Централната служба по валидиране към [Европейската изпълнителна агенция за научни изследвания](#) извършва оценка на структурата на собственост и контрол от името на ЕССС (точки 88—91).
- 20** В случаите, когато финансовата подкрепа се отпуска на трети страни, оценката на собствеността и контрола е отговорност на бенефициентите по съответния проект и се извършва въз основа на техния собствен подход и методология. ЕСП установи, че тяхната методология не подлежи на проверка от страна на ЕССС. Последният не извършва и проверки, за да се увери, че третите страни се притежават и контролират от ЕС. Одиторите считат, че съществува значителен риск бенефициентите да не разполагат с капацитет за задоволително извършване на тези проверки. Този риск не е смекчен в достатъчна степен и би могъл да доведе до разкриване на оперативни данни и информация за чувствителна инфраструктура и технологии от критично значение за сигурността (точки 92—96).



Препоръка 4

Да се осигури извършването на надеждна оценка на структурата на собственост и контрол на субектите, получаващи финансиране от ЕС по програма „Цифрова Европа“

Европейският център за експертни познания в областта на киберсигурността следва:

- а) да получи разумна увереност, че бенефициентите, отговарящи за предоставянето на финансова подкрепа на трети страни, притежават необходимия административен и технически капацитет за извършване на подходящи оценки на собствеността и контрола въз основа на съществуващата методология, с която разполагат.
- б) да проверява въз основа на извадка, дали финансиране от ЕС се отпуска единствено на субекти, отговарящи на условията за допустимост.

Целеви срок за изпълнение — буква а) — 2026 г., буква б) — 2027 г.

21 Бенефициентите, управляващи финансирани от ЕС проекти, следва да докладват на ЕССС за своя напредък и постигнатото от тях, като се ръководят от договорени междинни цели и резултати. Те са от ключово значение за мониторинга на проектите и следва да бъдат ясно определени. ЕСП установи, че при почти всички проекти от извадката междинните цели и резултати не са били определени в съответствие с инструкциите и че много от тях не са били полезни за проследяване на напредъка (точки [97](#)—[99](#)).

22 Беше установено също, че много от показателите за изпълнение, използвани от бенефициентите, не са подходящи или измерими и нямат целеви или базови стойности. Освен това докладването по тези показатели не е задоволително и поради това не може да служи като основа за оценка на изпълнението на проектите (точки [100](#)—[102](#)).

- 23** За да се наблюдава постигнатото общо за цялата програма „Цифрова Европа“, по всички проекти следва да се докладва по специфични програмни показатели, които се включват в [годишните декларации за изпълнението на програмите](#) на Комисията. ЕССС отговаря за събирането и проверката на данните, докладвани по тези показатели. ЕСП установи няколко проблема в начина на събиране на данните и тяхното качество като цяло. Одиторите не откриха доказателства, че точността на докладваните данни е била проверена от ЕССС. Резултатите от проверките на ЕСП, извършени въз основа на извадка, сочат че докладваните данни не отразяват точно постигнатите резултати (точки [103](#)—[106](#)).



Препоръка 5

Да се усъвършенства рамката за мониторинг на изпълнението на компонента за киберсигурност на програма „Цифрова Европа“

За да може да се извършва подходящ мониторинг на напредъка и изпълнението, Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността (ЕССС) трябва:

- a) да следи за това, преди подписването на договора за безвъзмездна финансова помощ, за всички проекти да бъдат определени междинни цели, резултати и показатели за изпълнение, които да отговарят на инструкциите, предоставени във формуляра за кандидатстване;
- b) да разработи и въведе надеждна система за събиране, проследяване, проверка и агрегиране на данните по показателите за изпълнение на компонента за киберсигурност на програма „Цифрова Европа“, с цел показателите да отразяват точно постигнатите резултати.

Целеви срок за изпълнение — 2027 г.

Подробни констатации и оценки

Мрежите и механизмите на ЕС за киберсигурност подпомагат сътрудничеството и действията за реакция, но ограниченият обмен на информация и непълното им прилагане намаляват тяхната ефективност

Мрежите на ЕС дават възможност за сътрудничество между държавите членки, но ограниченият обмен на информация намалява тяхната добавена стойност

- 24** Настоящата рамка на ЕС от мрежи и механизми за улесняване на откриването и реакцията при значителни киберинциденти е изградена постепенно и води началото си от [Директивата относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза](#)³ (Директива за МИС), която е влязла в сила през август 2016 г. ЕСП представя описание на настоящата среда за киберсигурност на ЕС в [приложение II](#).

³ Директива (ЕС) 2016/1148.

Мрежите на ЕС дават възможност за сътрудничество между държавите членки на техническо и оперативно равнище

- 25** С Директивата за МИС е създадена [мрежата на ЕРИКС](#), която обединява [CERT-EU](#) (Служба за киберсигурност за институциите, органите, службите и агенциите на Съюза) и екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС), определени от държавите членки. Тази мрежа има за цел да допринесе за изграждането на доверие между националните ЕРИКС и да насърчи бързото и ефективно оперативно сътрудничество между държавите членки.
- 26** [EU-CyCLONe](#) е създадена през 2020 г. като неформална мрежа за сътрудничество между националните органи, отговарящи за управлението на кризи в областта на киберсигурността. Тя изпълнява ролята на свързващо звено между техническото ниво, на което работи мрежата на ЕРИКС, и политическото ниво на Съвета на ЕС и [интегрираните договорености на ЕС за реакция на политическо равнище при кризи](#). Влизането в сила на Директивата за МИС 2 през 2023 г. официализира ролята на EU-CyCLONe и ѝ предоставя ясни правомощия.
- 27** ЕСП разглежда дали ролите и отговорностите на тези мрежи на равнището на ЕС са добре определени и дали улесняват сътрудничеството между държавите членки.
- 28** [ENISA](#) изпълнява функциите на секретариат на мрежата на ЕРИКС и EU-CyCLONe и им предоставя ресурси, експертен опит, инфраструктура и ИТ инструменти, необходими за сътрудничество и сигурен обмен на информация. В проучване на удовлетвореността на заинтересованите страни⁴, проведено от агенцията в началото на 2025 г., ENISA е получила висока оценка за работата си като секретариат на тези мрежи. Положителните отзиви бяха потвърдени и при одитните посещения на ЕСП, по време на които националните органи в областта на киберсигурността изразиха задоволство от подкрепата на агенцията.

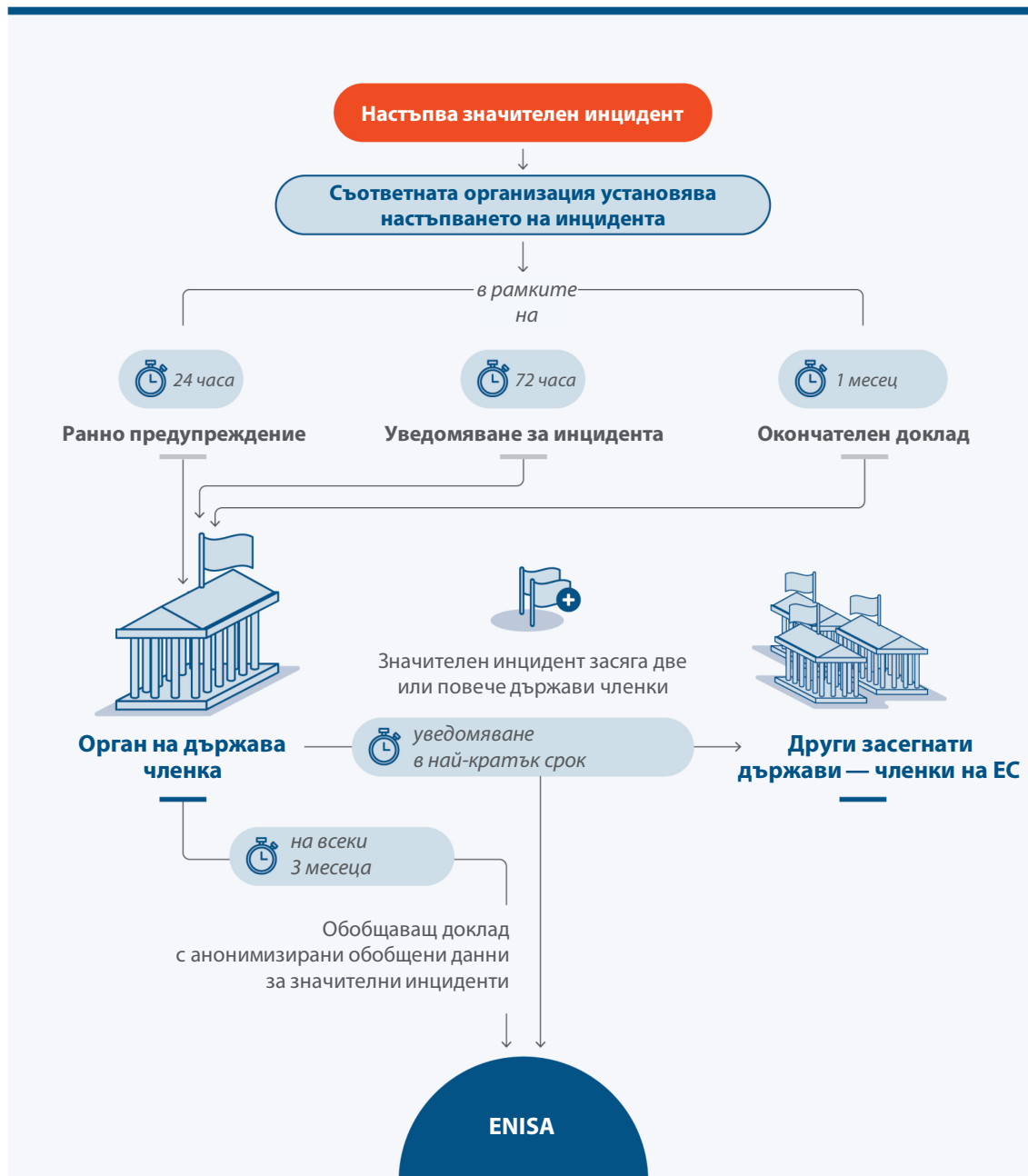
⁴ ENISA, [Консолидиран годишен отчет за дейността за 2024 г.](#), стр. 33 и 36.

- 29** През 2025 г. Съветът е приел **концепция за киберсигурността**, в която се определят ролите и отговорностите на основните участници (включително мрежата на ЕРИКС и EU-CyCLONe) и механизми, които се задействат при мащабни киберинциденти или киберкризи. ЕСП установи, че концепцията за киберсигурността до голяма степен изяснява ролите и отговорностите по отношение на управлението на кризи в областта на киберсигурността в ЕС и отчита промените в средата след първата концепция от 2017 г. В нея се определят три нива на сътрудничество: техническо, оперативно и политическо. Също така се описват подробно новите мрежи и структури, създадени от 2017 г. насам, като EU-CyCLONe, екипите на ЕС за бързо реагиране при хибридни заплахи и Европейската система за предупреждение в областта на киберсигурността. Разглежда се и начинът, по който управлението на кризи в областта на киберсигурността следва да бъде интегрирано в по-широката рамка на ЕС за реакция при кризи.
- 30** Въпреки официалното създаване на мрежата на ЕРИКС през 2016 г. и EU-CyCLONe през 2023 г. обаче двете мрежи все още не са формализирали процедурните правила относно съвместната си работа. Те също така не са се споразумели относно критериите, съгласно които мрежата на ЕРИКС следва да уведомява EU-CyCLONe дали даден наблюдаван киберинцидент представлява потенциален или текущ мащабен киберинцидент. Двете мрежи трябва също така да се споразумеят за обща таксономия по отношение на тежестта на инцидентите и основните понятия — като „заплаха“, „участник в заплаха“, „инцидент“ и „въздействие“ — която е необходима за осъществяването на автоматизиран обмен на информация. Понастоящем има различни възможности за тълкуване относно това кога даден инцидент се определя като значителен или мащабен. Липсата на обща таксономия беше посочена и от органите по киберсигурност на трите посетени от ЕСП държави членки.

Ограниченият обмен на информация и незадоволителното докладване значително намаляват добавената стойност на мрежите

- 31** Географските граници не могат да предотвратят възникването и разпространението на киберинциденти и кибератаки. Обменът на информация между държавите членки, например относно тактиките и техниките, използвани от участниците в заплахи, и относно цифровите индикатори за извършен пробив в дадена мрежа или информационна система („показатели за компрометиране на системите“), може да допринесе значително за повишаване на киберсигурността.
- 32** ЕСП установи, че обменът на информация е ограничен, което значително намалява добавената стойност на тези мрежи. Наблюдаваните от ЕСП ограничения са свързани главно със закъснения при транспонирането на Директивата за МИС 2, проблеми с определянето на това дали даден инцидент има трансгранично въздействие, ограничения на обмена на информация, наложени от националното законодателство в областта на сигурността, и липса на доверие. С Директивата за МИС 2 се въвеждат някои изисквания за докладване за субектите, попадащи в нейния обхват, и за органите на държавите членки, както е показано на [фигура 2](#).

Фигура 2 | Срок за докладване на инциденти съгласно Директивата относно мерки за високо общо ниво на киберсигурност в Съюза (МИС 2)



Източник: ЕСП, въз основа на информация от ENISA.

- 33** Държавите членки е следвало да [транспонират Директивата МИС 2](#) в националното си законодателство до октомври 2024 г., но само две от тях са спазили крайния срок. Закъсненията при транспонирането имат значително отражение върху обмена на информация, тъй като междувременно субектите, обхванати от Директивата за МИС 2, не са правно задължени да докладват за инциденти. Комисията е изчислила⁵, че Директивата за МИС е обхващала 15 500 субекта, докато в обхвата на Директивата за МИС 2 попадат над 110 000 субекта. Например публичната администрация — секторът, който най-често е обект на заплахи в ЕС според [доклада на ENISA относно картината на заплахите](#) за 2025 г. — не е била задължена да докладва за инциденти съгласно Директивата за МИС.
- 34** Докладването пред ENISA на данни за инциденти на всеки три месеца (което може да е дълго време след възникването на даден инцидент) намалява тяхната добавена стойност. Тези данни служат предимно за статистически цели и за открояване на тенденции в миналото, а не за по-бързо откриване и по-добра реакция при инциденти. ENISA предоставя на държавите членки [онлайн инструмент](#) за докладване. Образецът за докладване съдържа минимален набор от данни, които трябва да бъдат предоставени, като например вида на инцидента и съответния сектор. Освен това ENISA препоръчва държавите членки да предоставят допълнителна информация с цел по-задълбочен анализ на данните, например чрез установяване на връзка между инцидентите и конкретни уязвимости. Не всички държави членки предоставят тази информация, което значително намалява качеството и добавената стойност на събираните данни.
- 35** В своя [доклад за състоянието на киберсигурността в ЕС за 2024 г.](#) ENISA посочва, че вероятно не всички инциденти се съобщават, предвид сравнително малкия брой на докладваните инциденти. През периода 2018—2021 г. държавите членки са докладвали на ENISA между 100 и 500 инцидента годишно. Броят им постепенно се е увеличавал и през 2024 г. е достигнал до 1 276⁶.

⁵ Европейска комисия, [Доклад за оценка на въздействието](#) за 2020 г.

⁶ Данни от системата за докладване и анализ на киберинциденти (CIRAS) за 2024 г.

- 36** В своя доклад относно картината на заплахите за 2025 г., който обхваща периода от юни 2024 г. до юни 2025 г., ENISA е установила приблизително 4 800 киберинцидента⁷ въз основа на разузнавателни данни от открити източници, като например новини. Не всички от тези инциденти биха подлежали на докладване съгласно Директивата за МИС 2, тъй като при събирането на данни ENISA обхваща по-широк спектър от инциденти. От друга страна, за много значителни инциденти не може да се намери информация в разузнавателните данни от открити източници. Тъй като данните, докладвани от държавите членки, са анонимизирани, ENISA не е в състояние да съпостави установените от нея инциденти с тези, докладвани от държавите членки. Поради това не е възможно да се определи до каква степен докладването е занижено, но ЕСП счита, че разликата между броя на инцидентите, докладвани от държавите членки, и тези, установени в доклада относно картината на заплахите, показва, че не всички значими инциденти се докладват.
- 37** Друг признак за занижено докладване е броят на уведомленията до други засегнати държави членки и ENISA относно значителни трансгранични инциденти. Такова изискване е съществувало съгласно Директивата за МИС, но е счетено за неефективно, тъй като през 2020 г. Комисията е заключила⁸, че рядко се изпращат уведомления въпреки задължението. Тя отдава неизпълнението му на липсата на ясни условия за обмен на информация и на общи цели, които да го насърчават.
- 38** Задължението за информиране на другите държави членки е от решаващо значение за предотвратяване на разпространението на инциденти — неговото неизпълнение оказва отрицателно влияние върху киберсигурността на ЕС. През 2025 г. са били докладвани само 14 значителни трансгранични инцидента от седем държави членки. През 2024 г. държавите членки са представили два доклада за инциденти с потенциално трансгранично въздействие, през 2023 г. няма представени доклади, а през 2022 г. са представени три доклада. Това показва, че броят на докладваните значителни трансгранични инциденти е много занижен и не отразява действителния мащаб на тези атаки. За сравнение, в своя доклад относно картината на заплахите за 2024 г. ENISA е установила 322 инцидента, насочени конкретно към две или повече държави членки. Инцидентът в Collins Aerospace (вж. [каре 1](#)) е пример за недокладван инцидент от страна на държава членка въпреки значителното му трансгранично въздействие.

⁷ Доклад на ENISA относно картината на заплахите за 2025 г.

⁸ Европейска комисия, Доклад за оценка на въздействието за 2020 г.

Каре 1

Киберинцидент, който е нарушил функционирането на летищата

През септември 2025 г. Collins Aerospace, основен доставчик на технологии за авиационната промишленост, е засегнат от значителна атака със софтуер за изнудване, насочена срещу ИТ системата на предприятието за обработка на информация за пътници. Нападението е принудило големите европейски летища да се върнат към ръчни операции, което е довело до масови закъснения и отмяна на полети. Нарушението на дейността е било най-сериозно на летищата Хийтроу в Лондон, Брюксел, Берлин Бранденбург и Дъблин.

Съгласно Директивата за МИС 2 един от критериите даден инцидент да бъде определен като „значителен“ е дали той води до сериозни оперативни смущения в предоставянето на услуги или финансова загуба за съответния субект. Въпреки това нито една държава членка не е класифицирала горепосочения случай като значителен или широкомащабен трансграничен инцидент. Поради това нито една от засегнатите държави членки не е уведомила официално ENISA или други държави членки за него. Мрежата на ЕРИКС не е уведомила EU-CyCLONe относно инцидента, поради което последната не е съдействала за координираното му управление.

Източник: Анализ на ЕСП, въз основа на събеседвания с ENISA.

- 39** Друга причина за ограничаването на докладване на трансгранични инциденти е, че съответните компетентни органи на държавите членки трябва да определят дали докладваният инцидент има трансгранично въздействие, както и да установят кои други държави членки са засегнати. В зависимост от информацията, с която разполага, докладващият субект или съответният орган на държавата членка може да не знае за трансграничния характер на някои атаки. Понастоящем не съществува общоевропейска платформа, в която да се докладва за инциденти в реално време от всички държави членки и да се съпоставя информация за сектори или показатели за компрометиране на системите, с цел откриване на трансгранични инциденти. Поради това съществува значителен риск някои трансгранични инциденти да не бъдат установени и докладвани като такива.
- 40** От 2016 г. насам държавите членки не са счели нито един киберинцидент за „мощен“. По принцип всеки инцидент, който има значително отражение върху най-малко две държави членки, попада в обхвата на това определение. Въпреки това дори киберинциденти, които са причинили глобални прекъсвания на дейността и значителни щети, като например показаните на [фигура 3](#), не са били счестени за мощни. В резултат на това поэтапната процедура в рамките на EU-CyCLONe никога не е била напълно задействана вследствие на мощен киберинцидент.

Фигура 3 | Примери за сериозни киберинциденти



Източник: ЕСП, въз основа на материали от [Cloudflare](#), [ENISA](#), [Европол](#), [Wired](#), [IBM](#), [CrowdStrike](#).

- 41** Освен въвеждането на задължение за докладване на субектите и държавите членки, създадена е и мрежата на ЕРИКС с оглед на улесняването на обмена на информация. Доверието между държавите членки е в основата на функционирането на мрежата на ЕРИКС, в която информацията се споделя на доброволен принцип. Добавената стойност на мрежата значително намалява, когато държавите членки не желаят да споделят навременна практическа информация.
- 42** Националното законодателство в областта на сигурността на всяка държава членка налага ограничения върху обмена на информация на равнището на ЕС. Ако дадена държава членка прецени, че свързана с кибератака информация относно критичен субект е класифицирана или че докладването на конкретен инцидент би застрашило нейната национална сигурност, тя не е задължена да споделя информацията. По време на посещенията на ЕСП в държавите членки представители на мрежата на ЕРИКС и EU-CyCLONe заявиха, че информация може да се съобщава само съгласно националното законодателство в областта на сигурността. На равнището на ЕС не е извършен анализ на правните рамки на отделните държави членки и тяхното отражение върху обмена на информация.

- 43** През 2016 г. мрежата на ЕРИКС се е състояла от 28 национални екипа за реагиране при инциденти с компютърната сигурност (ЕРИКС) с по двама представители от всяка държава членка. Недостатъчният обмен на информация е траен проблем — в [оценката на Комисията](#) на Директивата за МИС се отбелязва, че държавите членки не обменят систематично информация помежду си, което особено силно засяга ефективността на мерките за киберсигурност и нивото на съвместната ситуационна осведоменост на равнището на ЕС. Съгласно Директивата за МИС 2 много държави членки са назначили секторни ЕРИКС в допълнение към своите национални ЕРИКС, вследствие на което мрежата се е разширила значително. Към момента на одита тя се състоеше от 42 ЕРИКС и над 700 отделни участници. Това усложнява още повече изграждането на доверие, тъй като поддържането на тесни връзки между всички членове е трудно.
- 44** Мрежата на ЕРИКС е запозната с проблема, свързан с обмена на информация, и обмисля различни действия за повишаване на доверието между участниците в разрастващата се мрежа. Създаването на по-малки групи от държави членки, които да формират трансгранични хъбове, както е описано подробно в точки [62—74](#), е алтернативен подход на изграждането на общоевропейска мрежа и може да спомогне за справяне с това предизвикателство.

Услугите, предоставяни по договор на Центъра за киберситуации, частично се припокриват със съществуващия капацитет, а бъдещата му дейност е неясна

- 45** Съгласно Директивата за МИС 2 в случаите, когато потенциален или текущ мащабен киберинцидент има или е вероятно да окаже значително въздействие, Комисията се включва в EU-CyCLONe като неин член⁹. Предвид тази нова роля и промените в картината на заплахите, през 2022 г. Комисията е създала работна група за киберкоординация в рамките на ГД „Съобщителни мрежи, съдържание и технологии“. Тази работна група включва Центъра за киберситуации, който следва да помага на Комисията да повишава ситуационната си осведоменост с оглед подпомагане на изпълнението на институционалните ѝ задължения за управление на кризи. Той също така следва да подпомага ГД „Съобщителни мрежи, съдържание и технологии“ при предоставянето на консултации на политическо равнище.

⁹ Член 16, параграф 2 от [Директивата за МИС 2](#).

- 46** За изграждането на Центъра за киберситуации Комисията разчита до голяма степен на външни доставчици на услуги, с които през декември 2022 г. са **сключени договори** за близо 18 млн. евро с продължителност от четири години. ЕСП извърши оценка на изграждането на Центъра, резултатите от дейността му и планове на Комисията за бъдещата му дейност.
- 47** Като част от предоставяните услуги изпълнителите са разработили информационно табло въз основа на търговски разузнавателни данни за киберзаплахи, с цел представяне и споделяне на информация за тези заплахи. Те изготвят и различни разузнавателни доклади за киберзаплахи, включително ежедневни и седмични доклади, както и тематични доклади за определени държави или сектори на икономиката. Центърът за киберситуации е разположен в една от сградите на Комисията и представлява помещение с оборудвани работни места, дистанционно свързани с информационното табло, хоствано от изпълнителите. Към момента на одита Центърът включваше малък брой служители на Комисията, подпомагани в работата си от многоброен екип от анализатори от дружеството външен изпълнител и експерти от ENISA.
- 48** ЕСП установи, че услугите, които външните доставчици предоставят на Центъра, частично се припокриват със съществуващия капацитет на ENISA. ENISA разполага с постоянен капацитет за ситуационна осведоменост и наблюдение на заплахи. Тя редовно публикува доклади за киберзаплахите, включително експресни доклади за конкретни инциденти, както и седмични доклади, в които се прави преглед на заплахите. Докладите се основават на разузнавателни данни от открити източници и са сходни с тези, изготвяни от външните изпълнители. Освен това ENISA изготвя или допринася за изготвянето на информационни документи на високо равнище за създателите на политики по време на криза, които също са сходни с докладите, издавани от Центъра за киберситуации.
- 49** Освен това информацията, използвана от Центъра за киберситуации за изготвянето на тези доклади, се основава на търговски разузнавателни данни за киберзаплахи и е сходна с информацията, използвана от други служби на Комисията, като например генерална дирекция „Цифрови услуги“ и CERT-EU. ЕСП счита, че при създаването на Центъра за киберситуации не е оползотворен в достатъчна степен потенциалът за рационализация, тъй като не е взета предвид информацията, с която Комисията и ENISA вече разполагат.

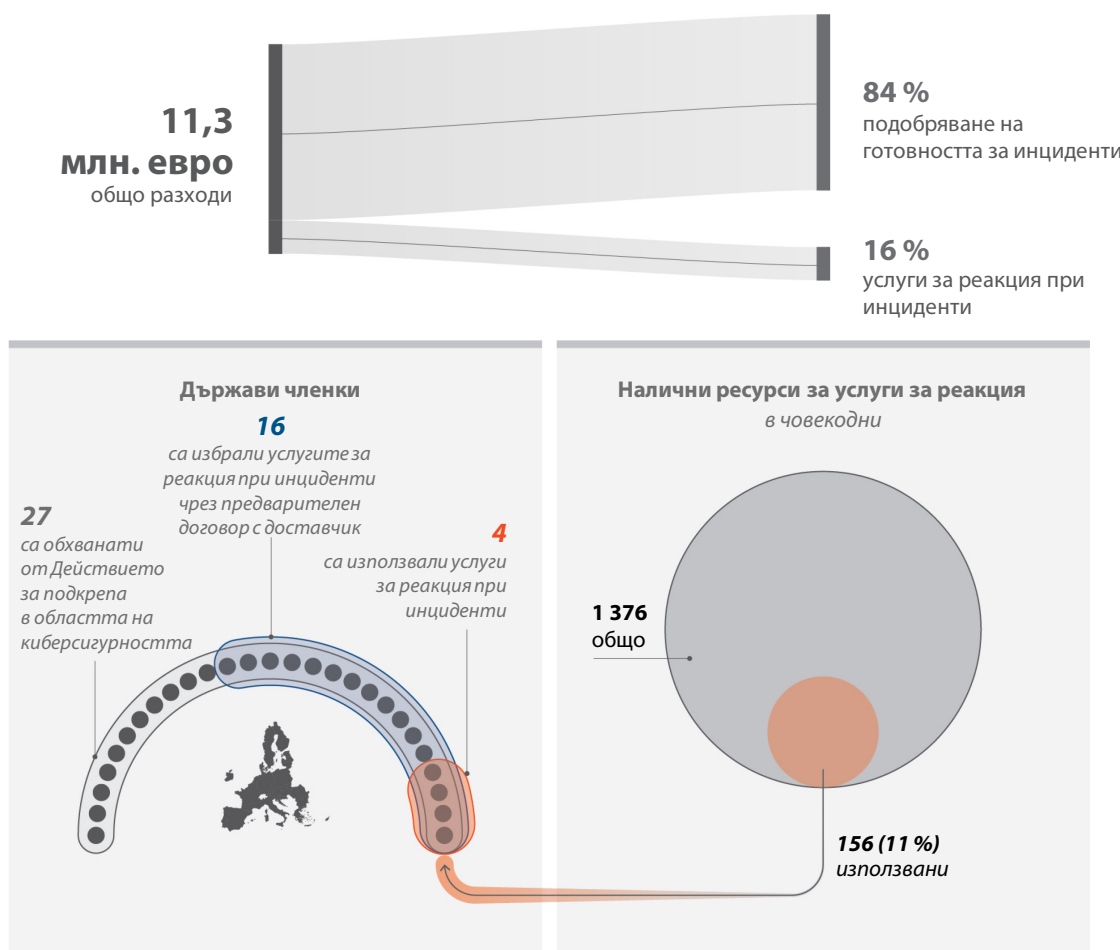
- 50** Договорът за Центъра за киберситуации изтича през декември 2026 г., след което се преустановява предоставянето на услуги от външните изпълнители. Услугите включват предоставяне на данни за информационното табло, изготвяне на доклади за заплахите и осигуряване на по-голямата част от персонала на Центъра. Информационното табло ще бъде предадено на Комисията, но ще загуби своята добавена стойност, ако не се актуализира непрекъснато с разузнавателни данни за киберзаплахи.
- 51** Към момента на одита Комисията не разполагаше с планове относно това как функционирането на Центъра ще продължи да бъде подпомагано от външни доставчици на услуги след изтичането на договора. ЕСП счита, че липсата на всеобхватен и подробен план за бъдещето на Центъра за киберситуации след изтичането на горепосочения договор излага на риск дейността му в периода след 2026 г.

Резервът за киберсигурност на ЕС дава възможност за бързо активиране на услуги за реакция при инциденти

- 52** През 2022 г., непосредствено след започването на военната агресия на Русия срещу Украйна и вследствие на нарастването на случаите на широкомащабни кибератаки, Комисията е предоставила на ENISA извънредно финансиране в размер на 15 млн. евро за пилотно [Действие за подкрепа на киберсигурността](#), което е стартирано през 2023 г. През 2023 г. Комисията е предоставила допълнително финансиране (приблизително 20 млн. евро) за удължаване на тази програма до края на 2026 г.
- 53** Комисията е направила също предложение за [Законодателен акт в областта на киберсолидарността](#), приет през декември 2024 г., с цел да се подготви за реакция при мащабни киберинциденти. С Акта се създава Резерв за киберсигурност на ЕС, който включва услуги за реакция при инциденти от доверителни доставчици. Той е започнал постепенно дейността си през 2025 г. с бюджет от 36 млн. евро за периода 2025—2027 г.
- 54** ЕСП разглежда как е организирана програмата „Действие за подкрепа на киберсигурността“, тъй като тя е в основата на изпълнението на функциите на Резерва за киберсигурност на ЕС. ЕСП провери също така дали поуките, извлечени от 2022 г. насам, са взети предвид при разработването на Резерва за киберсигурност на ЕС.

- 55** ENISA е разработила Действието за подкрепа на киберсигурността като механизъм за предоставяне на услуги за подпомагане на готовността и реакцията на държавите членки при мащабни киберинциденти или кризи. Всички услуги се договарят предварително от ENISA, което означава, че доставчиците на услуги могат да отговорят незабавно на отправени от държавите членки искания. Това е възможно и благодарение на организацията на ENISA, която осигурява денонощен достъп до служител на повикване, който да отговаря на исканията на държавите членки.
- 56** ENISA е взела решение да разпредели наличния бюджет поравно между държавите членки. За тази цел агенцията е стартирала открита тръжна процедура, разделена на 27 обособени позиции, по една за всяка държава членка, за да избере до трима доставчици на услуги в областта на сигурността от частния сектор, които да предоставят услуги до края на 2026 г. Освен това ENISA е избрала няколко доставчици в рамките на общоевропейска обособена позиция, които да предоставят услуги на допустими държави извън ЕС, както и на институции, органи и агенции на ЕС, или да подпомагат реакцията при трансгранични инциденти.
- 57** Този подход е позволил на ENISA да вземе предвид специфичните национални изисквания, включително езика, националните разрешения за достъп до класифицирана информация или установеното присъствие в държавите членки. От друга страна, предвид факта, че подборът на доставчици не се извършва така, че да им позволява да предоставят услуги в целия ЕС, основен недостатък на този подход е, че ако дадена държава членка не използва предварително договорените услуги, заделеният за нея бюджет не може да бъде преразпределен в полза на друга държава членка.
- 58** По отношение на Действието за подкрепа на киберсигурността държавите членки могат да избират между услуги за готовност или реакция, или да изберат комбинация от двата вида услуги. Повечето държавите членки са решили да използват наличното финансиране, за да подобрят готовността си (84 % от разходите през 2023 г.). Държавите членки, избрали да се възползват от услугите за реакция при инциденти чрез предварителен договор с доставчик, даващ право на достъп до услугите при поискване от страна на държавата членка, с цел своевременна реакция при киберинциденти, са ги използвали в ограничена степен, както е показано на [фигура 4](#). В трите посетени държави членки органите изразиха задоволство от начина, по който ENISA управлява Действието за подкрепа на киберсигурността.

Фигура 4 | Действие за подкрепа на киберсигурността на ENISA в периода до 2023 г.



Източник: ЕСП, въз основа на данни на ENISA.

- 59** За периода 2024—2026 г. само девет държави членки са поискали да сключат предварителен договор с доставчик за реакция при инциденти. Събеседванията, които ЕСП проведе с ENISA и органите в три държави членки, потвърдиха силното предпочитание към дейности за повишаване на готовността.
- 60** Въпреки че Резервът за киберсигурност на ЕС има за цел преди всичко да подпомага действията за реакция и възстановяване от големи киберинциденти, предоставяните услуги от Резерва за киберсигурност на ЕС, за които е сключен предварителен договор, но не се използват за реакция при инциденти, могат да бъдат превърнати в услуги за подобряване на готовността. Този гъвкав подход може да предотврати неизползването на предплатените услуги.

- 61** ЕСП счита, че избраният модел за Резерва за киберсигурност на ЕС се основава на поуките, извлечени от програмата „Действие за подкрепа на киберсигурността“. Въпреки това данните за използването на програмата сочат, че съществува риск Резервът за киберсигурност на ЕС да бъде използван предимно за повишаване на готовността, а не за реакция, в противоречие с целта, определена в Законодателния акт в областта на киберсолидарността.

Европейската система за предупреждение в областта на киберсигурността има за цел да подобри капацитета за откриване на заплахи, но все още не функционира

- 62** Една от основните цели на Европейската система за предупреждение в областта на киберсигурността е да насърчава обмена на относима информация с цел по-добро откриване, анализ и реакция при киберзаплахи. Участието в системата за предупреждение е доброволно, но държавите членки, които решат да се присъединят към трансграничен киберхъб, трябва да се ангажират да споделят съответната информация с другите членове. Чрез съвместна работа в групи в надеждна и сигурна среда държавите членки могат да избегнат някои от проблемите, свързани с обмена на информация, посочени в точки [31—44](#).
- 63** Към момента на одита 13 държави членки бяха взели решение да участват в Европейската система за предупреждение в областта на киберсигурността, и бяха създали два трансгранични киберхъба: ATHENA и ENSOC. През 2026 г. е отпуснато финансиране за създаването на трети трансграничен киберхъб — NBCC, с което броят на участващите в мрежата държави е станал общо 20 (18 държави членки и Исландия и Норвегия¹⁰), както е показано на [фигура 5](#).

¹⁰ Асоциирани държави извън ЕС в съответствие с член 10, параграф 1, буква а) от Регламент (ЕС) 2021/694.

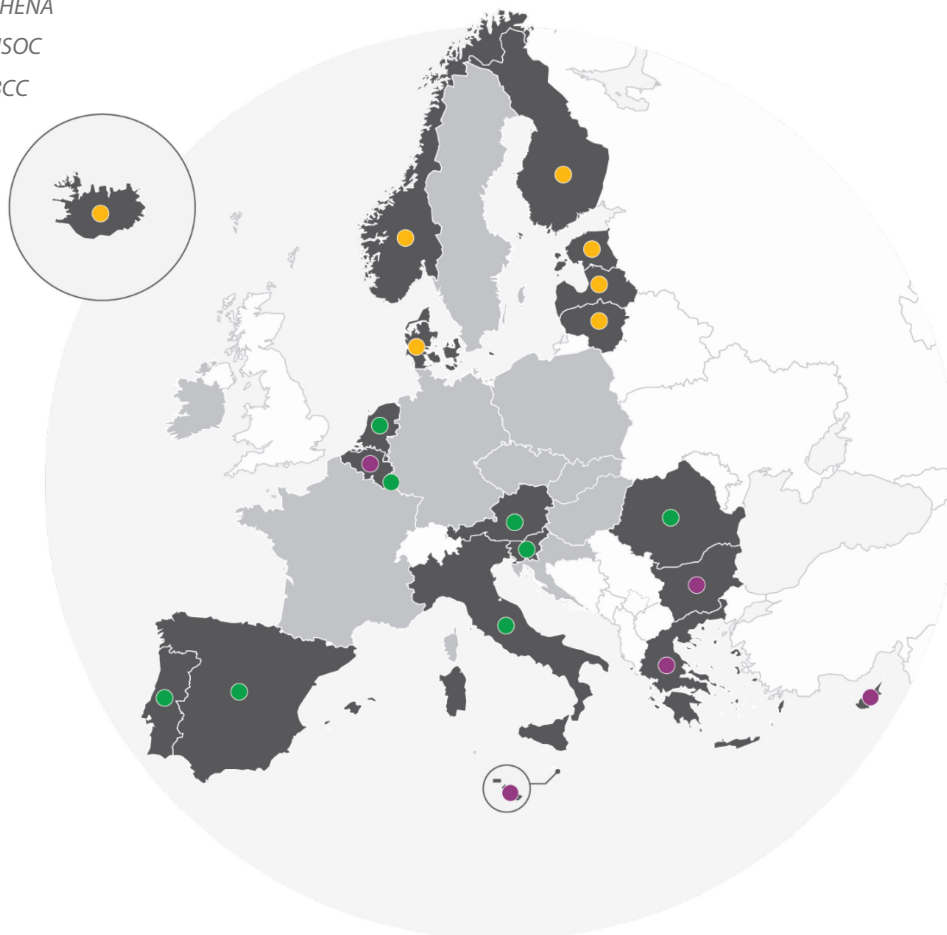
Фигура 5 | Държави, участващи в Европейската система за предупреждение в областта на киберсигурността

■ Държави, участващи в Европейската система за предупреждение в областта на киберсигурността

● ATHENA

● ENSOC

● NBCC



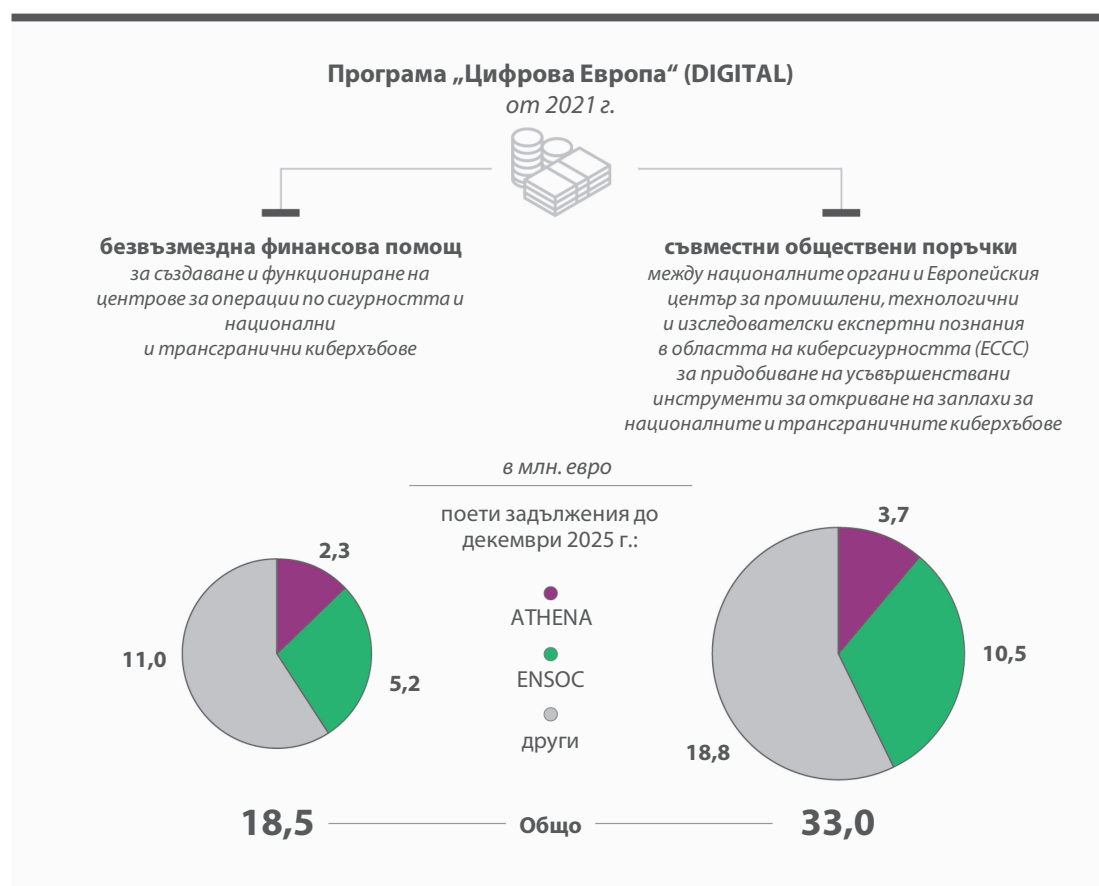
Източник: ЕСП.

64 ЕСП анализира как са създадени първите два трансгранични киберцентъра и какъв е техният напредък към постигането на целите на Европейската система за предупреждение в областта на киберсигурността. ЕСП провери също така как създадените трансгранични киберцентрове се вписват в по-широката среда за киберсигурност и взаимодействат със съществуващите мрежи и структури.

До момента не са постигнати конкретни резултати поради значителни забавяния при възлагането на обществени поръчки

- 65** От 2021 г. насам чрез програма „Цифрова Европа“ се предоставя финансиране за създаването на национални и трансгранични киберхъбове. Това финансиране се предоставя чрез сложна процедура, състояща се от два паралелни потока: традиционна безвъзмездна финансова помощ за създаване и функциониране на киберхъбове, от една страна, и съвместно възлагане на обществени поръчки за придобиване на усъвършенствани инструменти за откриване на заплахи, от друга страна, както е показано на [фигура 6](#). След публикуването на покана за представяне на предложения през ноември 2022 г. ATHENA и ENSOC са започнали дейност през януари 2024 г.

Фигура 6 | Финансиране на киберхъбове по програма „Цифрова Европа“



Източник: ЕСП, въз основа на данни на ECCC.

- 66** Двуетапните ограничени процедури за възлагане на обществени поръчки¹¹ са организирани от членовете на ATHENA и ENSOC, както и от ГД „Съобщителни мрежи, съдържание и технологии“ (първи етап) и новосъздадения ECCC (втори етап). Двуетапният подход има за цел да ограничи разпространението на чувствителна информация, като предостави подробни технически спецификации само на кандидатите, избрани на първия етап.
- 67** Първият етап е започнал през май 2024 г. за ENSOC и през юли 2024 г. за ATHENA. Заинтересованите дружества са разполагали с един месец, за да кандидатстват. Успешните кандидати обаче са били уведомени едва през април 2025 г., почти година след започването на процедурата.
- 68** Също така по това време нито процедурата за възлагане на обществени поръчки за ENSOC, нито тази за ATHENA са могли да преминат на втория етап, тъй като членовете на киберцентровете и ECCC не са били в състояние да предоставят на подбраните дружества техническите спецификации, необходими за представяне на оферта. Причината за това е била, че те все още са работели по финализирането им.
- 69** Вторият етап на процедурите за възлагане на обществени поръчки за някои обособени позиции е започнал едва през август 2025 г. в случая на ENSOC, а в случая на ATHENA е бил планиран за началото на 2026 г. Към момента на одита, 18 месеца след започването на процедурата, все още не беше подписан договор за нито една от обособените позиции. ЕСП счита, че липсата на достатъчна подготовка и сложността на процедурите за възлагане на обществени поръчки са възпрепятствали навременното им приключване.
- 70** Ето защо ЕСП констатира, че трансграничните киберхъбове не напредват по план за постигането на определените им цели. Поради липсата на инструменти за откриване на заплахи и споделяне на информация тяхната дейност е временно преустановена, а Европейската система за предупреждение в областта на киберсигурността все още не функционира, което забавя ефективното изграждане на усъвършенствани способности за откриване и предотвратяване на киберзаплахи и инциденти. Подписани са изменения за удължаване на срока на договора за безвъзмездна финансова помощ, за да се вземат предвид натрупаните до момента закъснения в процедурите за възлагане на обществени поръчки (15 месеца за ATHENA и 18 месеца за ENSOC).

¹¹ Покани за участие в тръжна процедура за [ENSOC](#) и [ATHENA](#).

Трансграничните киберхъбове създават допълнителни канали за комуникация, които още повече увеличават сложността на средата

- 71** Една от основните задачи на трансграничните киберхъбове е да подпомагат обмена на относима информация с цел по-добро откриване и реагиране при заплахи. Това включва информация за киберзаплахите, уязвимостите, показателите за компрометиране на системите и участниците в заплахите. Задачите на трансграничните киберхъбове отчасти се припокриват с тези на националните ЕРИКС и мрежата на ЕРИКС, особено по отношение на обмена на информация относно киберзаплахи и уязвимости. Няма ясно разграничение между ролите на трансграничните киберхъбове и на ЕРИКС. Съгласно концепцията за киберсигурността от 2025 г. (точка [29](#)) трансграничните киберхъбове са предназначени да функционират както на техническо (например националните ЕРИКС и мрежата на ЕРИКС), така и на оперативно равнище (например EU-CyCLONe).
- 72** Законодателният акт в областта на киберсолидарността изисква трансграничните киберхъбове да подписват споразумения за сътрудничество помежду си, за да се улесни обменът на информация. ENISA е следвало да издаде насоки за оперативна съвместимост между трансграничните киберхъбове до февруари 2026 г., както се изисква от Законодателния акт в областта на киберсолидарността. Междувременно през декември 2025 г. ЕССС е отпуснал безвъзмездна финансова помощ на консорциум (включващ някои членове на ENSOC и ATHENA) за определяне на техническа рамка за оперативна съвместимост между трансграничните киберхъбове. Насоките и рамката обаче ще бъдат завършени едва след като трансграничните киберхъбове започнат да функционират. Както ЕСП посочи в становището си от 2023 г. относно предложението за Законодателен акт в областта на киберсолидарността¹², ако не бъде сключено споразумение в близко бъдеще, съществува риск да бъдат разработени системи, които са несъвместими помежду си, което ще доведе до увеличаване на разходите.

¹² Становище 02/2023 на ЕСП относно предложението за Регламент на Европейския парламент и на Съвета за определяне на мерки за укрепване на солидарността и способностите на Съюза за откриване, подготовка и реагиране при киберзаплахи и инциденти, точка 26.

- 73** От трансграничните киберхъбове се изисква също така да споделят съответната информация относно мащабни киберинциденти с EU-CyCLONe и мрежата на ЕРИКС в най-кратък срок. На равнището на държавите членки изграждането на национални киберхъбове и участието в трансгранични киберхъбове създават допълнителни нива на комуникация. Координацията с държави извън ЕС¹³, които не са членове на мрежата на ЕРИКС или EU-CyCLONe, също увеличава сложността на средата.
- 74** Необходими са ясни споразумения за сътрудничество, за да се постигне съгласие по обща таксономия и за начините за споделяне на информация, както и за да се осигури оперативна съвместимост. Поуките, извлечени от дейността на мрежата на ЕРИКС, показват, че това представлява значително предизвикателство. ЕСП установи, че към момента на одита не са били договорени процедурни правила за сътрудничество и обмен на информация. Одиторите считат, че създаването на национални и трансгранични киберхъбове би могло да допринесе за по-ефективен обмен на информация. Интегрирането на трансграничните киберхъбове в средата за киберсигурност, която и без това е сложна, ще бъде обаче предизвикателство и ще изисква допълнителни канали за комуникация и правила за сътрудничество.

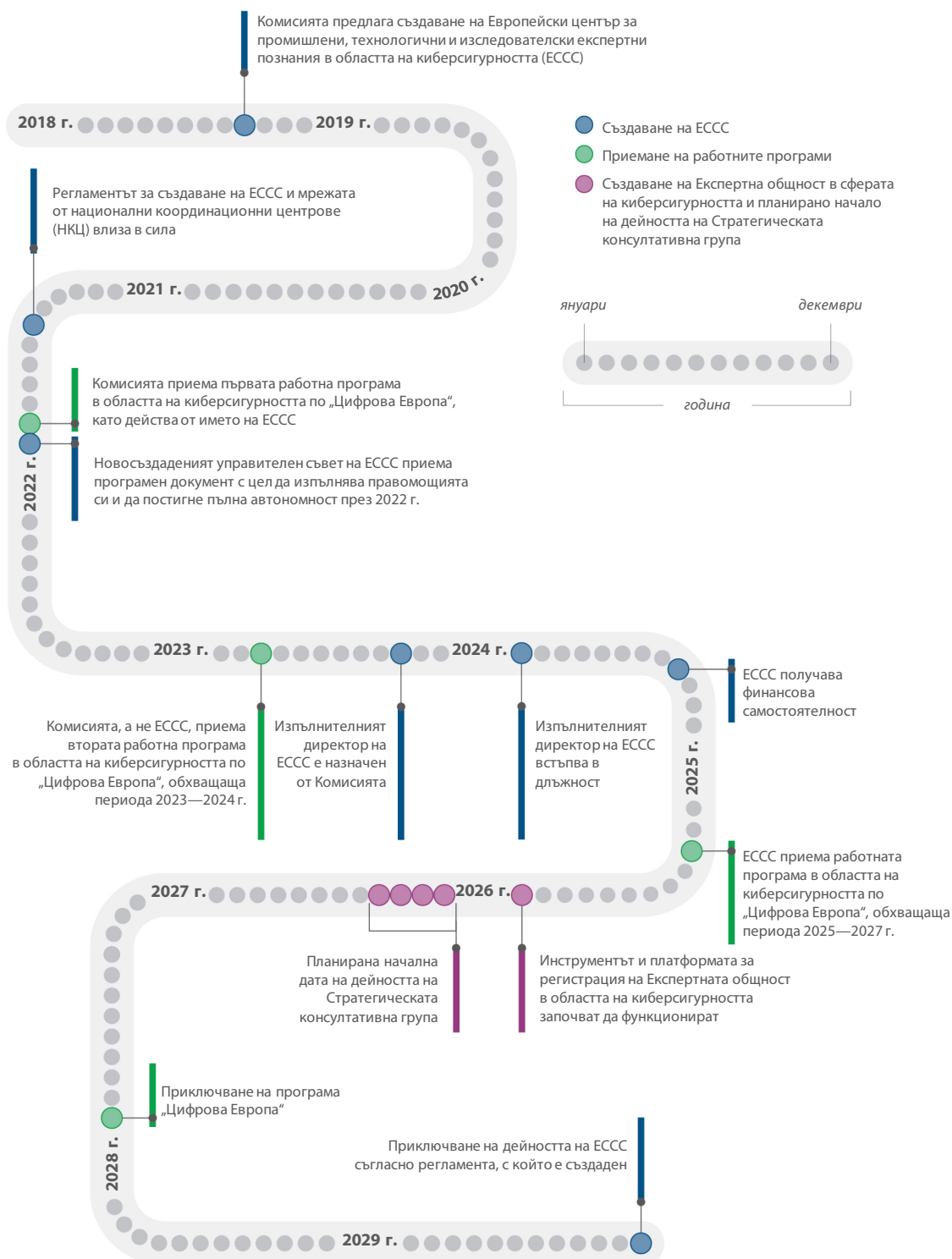
¹³ Исландия и Норвегия.

Финансираните от ЕС проекти по програма „Цифрова Европа“ имат за цел да укрепят киберсигурността, но срещат трудности, свързани с изпълнението и докладването

Забавянията при създаването на Експертната общност в сферата на киберсигурността са попречили нуждите ѝ да бъдат взети предвид при изготвянето на програма „Цифрова Европа“

- 75** С оглед на управлението на компонента за киберсигурност на програма „Цифрова Европа“, през 2018 г. Комисията е предложила да бъде създаден Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността (ECCC). В Регламента за ECCC се предвижда той да бъде подпомаган от мрежа от 29 национални координационни центъра (НКЦ), по един за всяка държава членка, както и по един за Исландия и Норвегия. В него също така се призовава да бъде създадена Експертната общност в сферата на киберсигурността (Общността), състояща се от представители на промишления сектор, академичните и научноизследователските организации, както и други сдружения на гражданското общество в тази област.
- 76** Предвижда се до 20 членове на Общността да бъдат назначени в Стратегическата консултативна група (SAG), която е един от трите компонента в структурата на ECCC. Една от основните задачи на Стратегическата консултативна група е да организира обществени консултации, които да бъдат включени в програмата на ECCC и работните програми на „Цифрова Европа“.
- 77** ЕСП анализира дали програма „Цифрова Европа“ и съответните ѝ работни програми са били приети след извършен задълбочен анализ на нуждите и дали ECCC, мрежата от НКЦ, Общността и Стратегическата консултативна група са могли да допринесат към работните програми. На практика ECCC, мрежата от НКЦ, Общността и Стратегическата консултативна група са били изградени постепенно в продължение на няколко години (вж. [фигура 7](#)).

Фигура 7 | Хронология на изграждането на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността, мрежата от национални координационни центрове, Общността и Стратегическата консултативна група



Източник: ЕСП.

- 78** Тъй като ЕССС е започнал да функционира пълноценно едва през септември 2024 г., Комисията е приела от негово име работните програми за периодите 2021—2022 г. и 2023—2024 г. Общността не е могла да допринесе с експертния си опит към двете работни програми, приети от Комисията.
- 79** Междувременно държавите членки са започнали да изграждат своите НКЦ, които функционират като звена за контакт на национално равнище за Общността. Създаването и дейността на НКЦ са съфинансирани от програма „Цифрова Европа“, като до момента на одита предоставените от ЕС средства са в размер на над 90 млн. евро, включително близо 44 млн. евро, които ще бъдат разпределени допълнително чрез финансова подкрепа за трети страни. До 2027 г. е предвидено да бъдат отпуснати допълнителни 38 млн. евро за подкрепа на НКЦ.
- 80** ЕСП констатира, че през декември 2025 г., четири години след създаването на ЕССС и мрежата от НКЦ, Общността все още не беше създадена, а членовете на Стратегическата консултативна група все още не бяха назначени. ЕССС е приел последната работна програма в областта на киберсигурността по програма „Цифрова Европа“ на 14 март 2025 г., като тя обхваща периода 2025—2027 г. Въпреки че е изготвил и приел работната си програма след обширни консултации с държавите членки и мрежата от НКЦ, той не е могъл да се възползва от приноса и съветите на Общността или на Стратегическата консултативна група, което противоречи на разпоредбите на регламента за неговото създаване. ЕСП счита, че това представлява пропусната възможност.
- 81** Срокът на действие на програма „Цифрова Европа“ изтича през 2027 г. и ако правомощията му не бъдат удължени, се очаква ЕССС да приключи дейността си през 2029 г. Поради това има вероятност подкрепата на мрежата от НКЦ, Общността и Стратегическата консултативна група, след като бъде осигурена, да може да се използва само за кратък период от време.

Финансираните от ЕС проекти имат подходящи цели, но много от тях са засегнати от оперативни проблеми

82 ЕСП подбра извадка от 11 проекта, свързани с откриването и реакцията при киберинциденти, финансирани по програма „Цифрова Европа“ през периода 2022—2025 г. (вж. [фигура 5](#) в [приложение I](#) и [приложение III](#)). Одиторите разгледаха дали:

- целите на проектите са в съответствие с очакваните крайни ефекти, посочени в поканите за представяне на предложения, както и дали отговарят на общите цели на програма „Цифрова Европа“;
- досега са постигнати планираните крайни продукти и резултати по проектите;
- планираните крайни продукти по проектите са постигнати навреме.

Резултатите от тази оценка са представени в [приложение IV](#).

По някои от проектите са постигнати първоначални резултати, но при много от тях има оперативни предизвикателства и закъснения

83 ЕСП установи, че целите на всички проекти допринасят за постигането на целите на програма „Цифрова Европа“ в областта на киберсигурността¹⁴, както и че отговарят на повечето от целите на поканите за представяне на предложения¹⁵.

84 От 11-те проекта в извадката два бяха на ранен етап на изпълнение и поради това ЕСП не можа да стигне до заключение относно резултатите от изпълнението им. При четири от останалите проекти реализираните крайни продукти и резултати бяха оценени като задоволителни спрямо планираните. ЕСП счита, че два проекта показват известни слабости, а резултатите при други три бяха оценени като незадоволителни (вж. [приложение IV](#)).

¹⁴ Член 6 от [Регламент \(ЕС\) 2021/694](#) за създаване на програма „Цифрова Европа“.

¹⁵ Показани за представяне на предложения: „Изграждане на капацитет на центровете за операции по сигурността“; „Разгръщане на мрежата от национални координационни центрове с държавите членки“; „Подкрепа за взаимопомощ и повишаване на готовността“; и „Нови приложения на изкуствения интелект и други базови технологии за центрове за операции по сигурността“.

- 85** Програма „Цифрова Европа“ е специално насочена към повишаване на нивото на киберсигурност на малките и средните предприятия (МСП). В тази връзка по няколко проекта се предлагат конкретни решения за МСП (вж. [каре 2](#)).

Каре 2

Примери за проекти, които водят до осезаеми резултати за МСП

Проектът [GR-SME-SOC](#) (проект 6 в [приложение III](#)) има за цел да предостави на МСП в Гърция инструменти и услуги в областта на киберсигурността чрез създаване на център за операции по сигурността (ЦОС), съобразен с техните нужди. Проектът е стартиран през януари 2024 г. и се изпълнява от консорциум от пет гръцки организации. Предвижда се да се предоставят безплатно услуги в областта на киберсигурността на 120 МСП в продължение на една година, след което услугите да започнат да се предлагат на пазара. По проекта се предлагат усъвършенствани услуги за МСП, като например наблюдение в реално време, откриване на заплахи, основано на изкуствен интелект, и гъвкава реакция при инциденти.

В рамките на проект [NCC-IE](#) (проект 3 в [приложение III](#)) координаторът на проекта е предоставил около 1,8 млн. евро под формата на безвъзмездна финансова помощ на над 50 МСП в Ирландия с цел подобряване на киберсигурността им. От схемата за безвъзмездна финансова помощ са се възползвали дружества с по двама до около 200 служители, включително семейни предприятия, стартиращи предприятия и световни износители в различни сектори. Безвъзмездната финансова помощ е била предназначена изключително за дружества, преминали през преглед на мерките за киберсигурност под ръководството на държавната агенция Enterprise Ireland. Безвъзмездната финансова помощ покрива 80 % от разходите (до 60 000 евро) за изпълнение на препоръките от прегледа.

Източник: ЕСП.

- 86** Много проекти от извадката на ЕСП се сблъскват с трудности при спазването на сроковете или оперативни предизвикателства (вж. [приложение IV](#)). ЕСП установи, че при четири проекта са налице значителни закъснения. Сред тях са ENSOC и ATHENA, както е описано подробно в точки [65—70](#). Други примери са представени в [каре 3](#).

Каре 3

Примери за проекти, при които са налице оперативни предизвикателства и закъснения

В Ирландия Агенцията за управление на органите на местната власт (Local Government Management Authority — LGMA) е единственият бенефициент на безвъзмездна финансова помощ по проекта **ILG-SOC** (проект 8 в [приложение III](#)). Целта на проекта е да се създаде общ център за операции по сигурността за 31 органа на местната власт, който да използва усъвършенствани инструменти за откриване и реакции при заплахи. Проектът е започнал да се изпълнява през октомври 2023 г. и е с продължителност от три години. При междинния преглед всички резултати са отхвърлени. Проектът включва няколко процедури за възлагане на обществени поръчки, които са били неуспешни или са съпътствани от закъснения. Продължителността на проекта ще бъде удължена (без допълнително финансиране), с което се цели да се осигури достатъчно време за успешното му приключване.

В Гърция проектът **EL-SOC** (проект 5 в [приложение III](#)) има за цел да създаде консолидиран център за операции по сигурността на национално равнище, който да обедини информацията от секторните центрове. Това ще осигури всеобхватен преглед в реално време на ситуацията в областта на киберсигурността. Проектът се изпълнява в периода от януари 2024 г. до декември 2026 г. Планираното възлагане на обществена поръчка за хардуер и услуги е било забавено поради проблеми с финализирането и публикуването на техническите спецификации към поканата за представяне на оферти. Сред причините за забавянето, посочени от координатора на проекта, са и въпроси, свързани с осигуряването на национално съфинансиране и недостатъчната наличност на служители, отговорни за процедурите за възлагане на обществени поръчки.

Източник: ЕСП.

- 87** При два други проекта от извадката на ЕСП са налице известни закъснения. По три проекта крайните продукти са били реализирани навреме. И на последно място, два проекта са на ранен етап на изпълнение, поради което ЕСП не може да направи заключение относно изпълнението им.

Ограниченията, свързани със сигурността, създават оперативни предизвикателства, а извършването на проверки от бенефициентите поражда рискове

- 88** Регламентът за програма „Цифрова Европа“ предвижда, от съображения за сигурност финансирането за киберсигурност да може да се ограничава до субекти, които са установени в ЕС и се контролират от държави членки или граждани на ЕС. Това ограничение има за цел да намали риска от проникване или влияние от държави извън ЕС и да предотвратява споделянето на чувствителна информация, свързана със сигурността, с органи на държави извън ЕС.
- 89** Задължението на ЕС за оценка на собствеността и контрола се прилага не само за бенефициентите на безвъзмездна финансова помощ, но и за техните подизпълнители и получателите на финансова подкрепа за трети страни. С изключение на последната категория (вж. точки [92—96](#)), оценката се извършва от Централната служба по валидиране към [Европейската изпълнителна агенция за научни изследвания](#). Окончателното решение относно допустимостта за участие в ограничените покани за представяне на предложения обаче все още зависи от предоставящия финансирането орган, т.е. ГД „Съобщителни мрежи, съдържание и технологии“ или ECCC.
- 90** По време на одитната дейност на ЕСП бенефициентите многократно изтъкнаха практическите предизвикателства, породени от оценките на собствеността и контрола. Оценката на собствеността и контрола на ЕС може да бъде сложен и продължителен процес. Тя изисква анализ на цялостната структура на собствеността и веригата на контрол на всяка организация, включително всички нива до крайните собственици. Централната служба по валидиране изисква от всеки субект да предостави подробни [документни доказателства](#) за своята структура на собственост и конкретни права, корпоративно управление и всякакви търговски, финансови или други връзки, предоставящи контрол.

- 91** В три финансиращи от ЕС проекта в извадката на ЕСП поне един бенефициент от консорциум е бил изключен на по-късен етап, тъй като е било счетено, че той е собственост на държави извън ЕС или се контролира от такива. Фактът, че членове на консорциуми биват изключвани показва, че понятието за собственост и контрол на ЕС не е напълно ясно за всички участници в програмата „Цифрова Европа“. Като цяло, въз основа на данни от Централната служба по валидиране, 7 % от всички кандидати или подизпълнители на безвъзмездна финансова помощ в областта на киберсигурността по програмата „Цифрова Европа“ не са отговорили на изискванията на оценката през периода 2022—2025 г. Подаването на заявления по покани за представяне на предложения от недопустими участници води до забавяния, както е показано в [каре 4](#).

Каре 4

Пример за случай, при който бенефициенти са били изключени, поради това че не са преминали успешно проверките, свързани със сигурността

Двама от членовете на консорциума по проект [NG-SOC](#) (проект 7 в [приложение III](#)) не са изпълнили изискванията на оценките на собствеността и контрола. Резултатът от оценката е бил обявен около един месец преди крайния срок за подписване на договора за безвъзмездна финансова помощ. Координаторът на проекта е бил принуден да поеме работата, възложена на двамата изключени членове, тъй като не е имало време да бъде намерен нов партньор. Един от изключените членове е извършвал дейност в конкретния отрасъл, в който разработеното решение е трябвало да бъде изпробвано. Поради това една значителна част от проекта, която се е отнасяла до изпитване на решенията в практиката, не е могла да се осъществи съгласно планираното. Впоследствие тази ситуация е била коригирана чрез изменение на условията на договора за безвъзмездна финансова помощ с цел включване на нови членове.

Източник: ЕСП.

- 92** Два от разгледаните от ЕСП проекти (NCC-IE и CYberSynchrony) предоставят финансова подкрепа на трети страни. Този механизъм за финансиране дава възможност на бенефициентите на безвъзмездна финансова помощ да използват част от помощта за финансиране на други субекти чрез открити покани за представяне на предложения. Финансовата подкрепа за трети страни може да улесни достъпа до финансиране от ЕС. В този случай бенефициентите носят цялата отговорност за извършването на оценката собствеността и контрола и Централната служба за валидиране не участва в процеса.
- 93** През 2021 г. Комисията е издала общи публично достъпни насоки за кандидати по ограничени покани за представяне на предложения, които са актуализирани през 2026 г. Въпреки че финансовата подкрепа за трети страни се прилага в покани за представяне на предложения по програма „Цифрова Европа“ от 2021 г., нито Комисията, нито ЕССС са предоставили на бенефициентите подробна методология за извършване на проверките при оценката на третите страни, на които предоставят финансова подкрепа. През юли 2025 г. ЕССС е издал незадължителни насоки, като е предоставил на мрежата от НКЦ структуриран подход към оценката на собствеността и контрола. Те съдържат общи принципи и стъпки, които могат да бъдат предприети. В насоките обаче не се уточнява как следва да се извършват проверките, което натоварва бенефициентите с отговорност за разработването на техен собствен подход.
- 94** ЕСП установи, че ЕССС нито валидира методологията, възприета от бенефициентите, нито извършва проверки въз основа на извадки, за да гарантира, че тя е достатъчно надеждна и че избраните получатели на финансова подкрепа действително са собственост на ЕС и се контролират от него.

- 95** Освен това в своя [Годишен доклад за 2024 г.](#) ЕСП установи, че бенефициентите, на които Комисията е възложила да управляват финансовата подкрепа, отпускана на трети страни (в областта на научните изследвания), не са задължени да доказват ефективността на проверките, чрез които следят за редовността на разходите на ЕС. Това е случаят и с ЕССС, който не извършва оценка на административния и техническия капацитет на бенефициентите за извършване на адекватна оценка на собствеността и контрола. Както е описано подробно в точка [90](#), тази оценка може да бъде сложна и се извършва на равнището на ЕС от специализирана служба със задълбочен експертен опит в тази област.
- 96** Предвид гореизложеното ЕСП счита, че съществува значителен риск бенефициентите да не разполагат с необходимия капацитет за ефективно извършване на проверките за оценка на собствеността и контрола, за които отговарят. Като се има предвид естеството на финансираните дейности, този недостатък би могъл да изложи на риск чувствителна инфраструктура, оперативни данни и критични за сигурността технологии.

Повечето финансирани от ЕС проекти не разполагат с подходящи рамки за изпълнение, а данните за изпълнението на програма „Цифрова Европа“, свързани с киберсигурността, са неточни

Рамките за изпълнение на повечето финансирани от ЕС проекти са незадоволително разработени

- 97** Бенефициентите, управляващи финансирани от ЕС проекти, следва да докладват на ЕССС за своя напредък и постигнатото от тях, като се ръководят от договорени междинни цели, резултати и показатели, както е показано на [фигура 8](#). ЕСП провери дали междинните цели и резултатите, определени за всеки проект, дават възможност за подходящ мониторинг. ЕСП също така анализира дали техните показатели за изпълнение са подходящи и измерими и дали за тях са определени базови и целеви стойности.

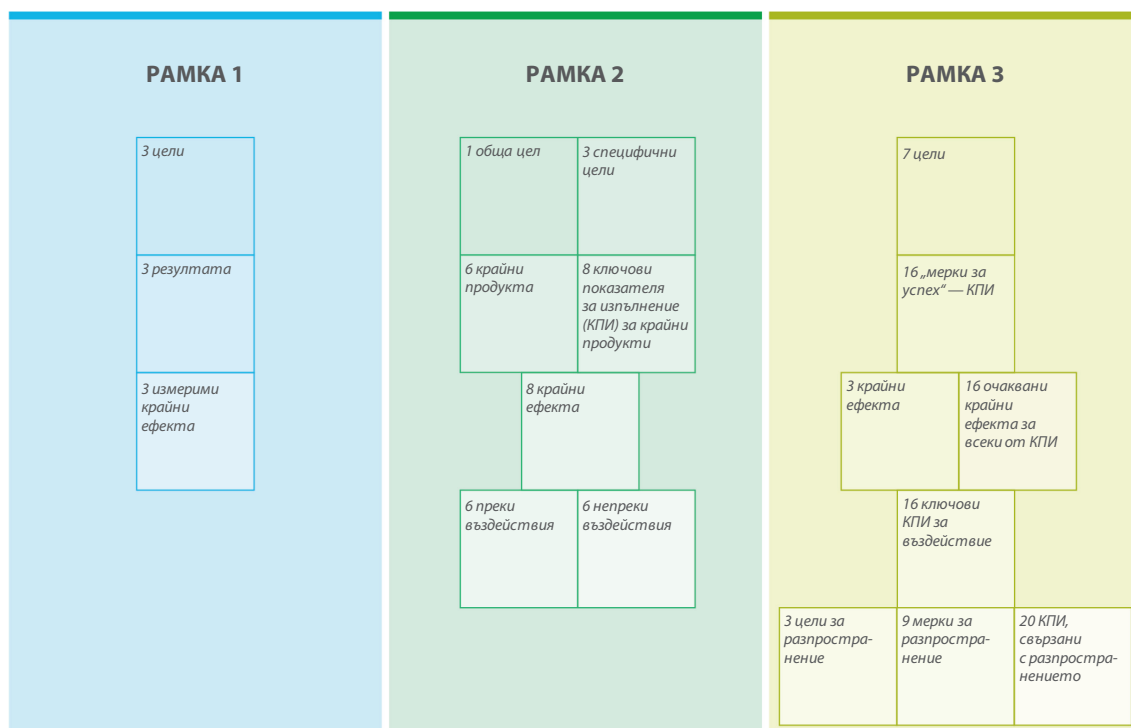
Фигура 8 | Междинни цели, резултати и показатели за изпълнение в проектите по програма „Цифрова Европа“

	 Междинни цели	 Резултати	 Показатели за изпълнение
Какво представляват	контролни етапи през целия живот на проекта за проследяване на напредъка	реализирани крайни продукти за отчитане на постигнатия напредък	използват се за измерване на резултатите
Как следва да се определят	свързани само с основните крайни продукти (ограничен брой)	само основни крайни продукти (максимум 10 до 15 на проект)	специфични, измерими, достижими, целесъобразни и обвързани със срокове
Примери	„стартиране на пилотната фаза на платформата“	„ръководство за потребителите на платформата“	„намаляване с 30 % на времето за реакция при инциденти“
	Структуриран подход, част от онлайн системата за управление на безвъзмездната финансова помощ		Неструктуриран подход

Източник: ЕСП, въз основа на [формуляра за подаване на заявление за безвъзмездна финансова помощ](#).

- 98** В своето предложение за проект бенефициентите трябва да определят поредица от междинни цели и резултати, като следват структуриран подход, посочен в инструкциите за кандидатите. Всички междинни цели и резултати са включени в онлайн системата за управление на безвъзмездната финансова помощ, за да се улесни проследяването на изпълнението им. ЕССС обикновено извършва преглед на всеки проект по два пъти: веднъж в средата на изпълнението му и веднъж след приключването му. По време на тези прегледи външни експерти проверяват напредъка по междинните цели и резултатите, а ЕССС ги потвърждава. Междинните цели и резултати са от ключово значение за мониторинга на проектите и следва да бъдат ясно определени.
- 99** ЕСП установи, че почти при нито един от проектите в извадката не са били следвани инструкциите по отношение на броя на междинните цели и резултатите: междинните цели варират от 8 до 39 на проект, а резултатите — от 8 до 45. Много от междинните цели и резултатите не отговарят на инструкциите по отношение на начина, по който следва да бъдат изготвени, и поради тази причина не са полезни за проследяване на напредъка (например „среща за инициране на изготвянето на покана за представяне на предложения в областта на научните изследвания“ „или „официален протокол от срещата по проекта“). При три проекта комисията за оценка е установила тези проблеми преди подписването на договора за безвъзмездна финансова помощ. В два случая бенефициентите са предложили само незначителни промени (например по отношение на сроковете), без да се насочат към основните проблеми, а в третия случай не са предприети промени. За шест други проекта от извадката на ЕСП анализът показва, че междинните цели или резултатите не съответстват на инструкциите и невинаги са подходящи. ЕСП счита, че когато резултатите или междинни цели не са добре определени или броят им е твърде голям, проследяването на напредъка се затруднява.
- 100** За разлика от междинните цели и резултатите, показателите за изпълнение не следват структуриран подход и не са консолидирани в таблица в системата за управление на безвъзмездната финансова помощ, а са разпръснати в различни раздели на предложението. Този подход е довел до предлагането на множество различни рамки за изпълнение от страна на бенефициентите. Докато някои са определили само проектни цели, които са обвързали с показателите за изпълнение, други са разработили много по-сложни рамки за изпълнение. Примери за това са представени на [фигура 9](#).

Фигура 9 | Пример за разнородни рамки за изпълнение, разработени по проектите



Източник: Европейска сметна палата (ЕСП).

101 Въз основа на своя анализ ЕСП заключава, че много от показателите за изпълнение, използвани за проектите, не са подходящи или измерими и нямат целеви или базови стойности (вж. [каре 5](#)). Освен това по седем проекта са определени 20 или повече показателя, като по един проект техният брой е 52. Резултатите от тази оценка са представени в [приложение IV](#).

Каре 5

Примери за неподходящи показатели за изпълнение

Показатели, които не са измерими:

- „Показателите за компрометиране на системите и други предоставяни услуги укрепват капацитета на МСП в областта на киберсигурността“
- „Предоставяне на инструменти и подходи за реагиране при инциденти, позволяващи интегриране с комуникационните канали на EU-CyCLONe“

Показатели, за които не са определени базови или целеви стойности:

- „Подобряване на подготвеността на персонала с $\geq 20\%$ “
- „намаляване с $\geq 20\%$ на усилията, необходими за съгласуване и спазване на съответните инициативи на ЕС в областта на киберсигурността“

Показатели, които не са свързани с изпълнението:

- „Окончателен доклад по проекта при приключване на етапа на финансиране“
- „Брой на обучаващите се, които ще участват във всички обучения“

Източник: ЕСП, въз основа на проектната документация.

102 ЕСП счита като цяло, че многото различни рамки за изпълнение, неподходящата формулировка на показателите и прекомерният им брой значително усложняват мониторинга на изпълнението. Поради това не е възможно да се направи задоволителна оценка на изпълнението на проектите. Това се усложнява допълнително от факта, че образецът за докладване не съдържа специален раздел относно показателите за изпълнение на проектите и в резултат на това по повечето проекти в извадката на ЕСП не е докладвано за тях.

Данните за изпълнението на компонента за киберсигурност на програма „Цифрова Европа“ са неточни

- 103** За да се наблюдава постигнатото по програма „Цифрова Европа“, в регламента са предвидени показатели, по които трябва да се докладва по всички проекти, както е описано подробно в [каре 6](#).

Каре 6

Показатели, свързани с киберсигурността, по програма „Цифрова Европа“

- 1.а Брой на съвместно придобитите инфраструктури или инструменти за киберсигурност, или и двете, включително в контекста на Европейската система за предупреждение в областта на киберсигурността
- 1.б Брой на изградените инфраструктури или инструменти за киберсигурност, или и двете
- 2. Брой на ползвателите и общностите от ползватели, получаващи достъп до европейски съоръжения за киберсигурност
- 3. Брой на действията в подкрепа на готовността и реагирането при киберинциденти в рамките на Механизма за действие при извънредни ситуации в областта на киберсигурността

Източник: Приложение II към [Регламент \(ЕС\) 2021/694 за създаване на програмата „Цифрова Европа“](#); рамка за мониторинг и оценка на програма „Цифрова Европа“ (SWD (2024) 37).

- 104** ЕСП разглежда дали в рамките на проектите в извадката е докладвано по тези показатели и как ЕССС събира и проверява тези данни.
- 105** По всички проекти се изисква да се докладва за показателите по програма „Цифрова Европа“ преди извършването на междинните и окончателните им прегледи в системата за управление на безвъзмездната финансова помощ. ЕСП установи, че при седем проекта периодът на изпълнение е бил преполовен към момента на одита и следователно е трябвало да се докладва по тези показатели, но такова докладване е извършено само по три от тях. По два от тези три проекта не е докладвана точна информация: по единия е докладвано по грешен показател, а по другия са посочени целеви стойности, а не постигнати резултати.

106 Комисията ежегодно докладва по тези показатели в [декларациите за изпълнението на програмите](#). Това позволява на заинтересованите страни да преценят дали съответната програма постига целите си. Според декларациите за изпълнението на програмите за 2024 г. напредъкът по показателите за програма „Цифрова Европа“, свързани с киберсигурността, съответства на планираното. ЕССС обясни на ЕСП, че е използвал поредица от проучвания сред бенефициентите по проектите, за да изготви тези показатели, вместо да използва като база системата за управление на безвъзмездната финансова помощ. ЕСП разгледа дезагрегираните данни, предоставени от ЕССС, и констатира редица проблеми в начина им на събиране на данните и цялостното им качество. Беше установено, че събраните данни не съответстват на стойностите, представени в декларациите за изпълнението на програмите и поради това не е ясно как са изчислени докладваните стойности. Одиторите не откриха доказателства, че точността на докладваните данни е била проверена от ЕССС. Проверките на ЕСП на проектите в извадката ѝ сочат, че докладваните данни не отразяват правилно постигнатите резултати, тъй като повечето стойности липсват или са неточни.

Настоящият доклад беше приет от Одитен състав III с ръководител George-Marius Hyzler — член на Европейската сметна палата, в Люксембург на заседанието му от 16 юни 2026 г.

За Европейската сметна палата

Tony Murphy
Председател

Приложения

Приложение I — Относно настоящия одит

- 01** Киберсигурността се определя като „дейностите, необходими за защита от киберзаплахи на мрежите и информационните системи, на ползвателите на такива мрежи и системи и други лица, засегнати от киберзаплахи“¹. „Киберзаплаха“ е „всяко потенциално обстоятелство, събитие или действие, което може да навреди, наруши или по друг начин да окаже неблагоприятно въздействие върху мрежите и информационните системи, ползвателите на такива мрежи и системи и други лица“². Киберсигурността изисква цялостен подход, състоящ се от поредица от взаимосвързани дейности за предотвратяване, откриване, реагиране и възстановяване от киберзаплахи, както е показано на *фигура 1* по-долу.

¹ Регламент (ЕС) 2019/881 („Акт за киберсигурността“).

² Член 2 от Акта за киберсигурността.

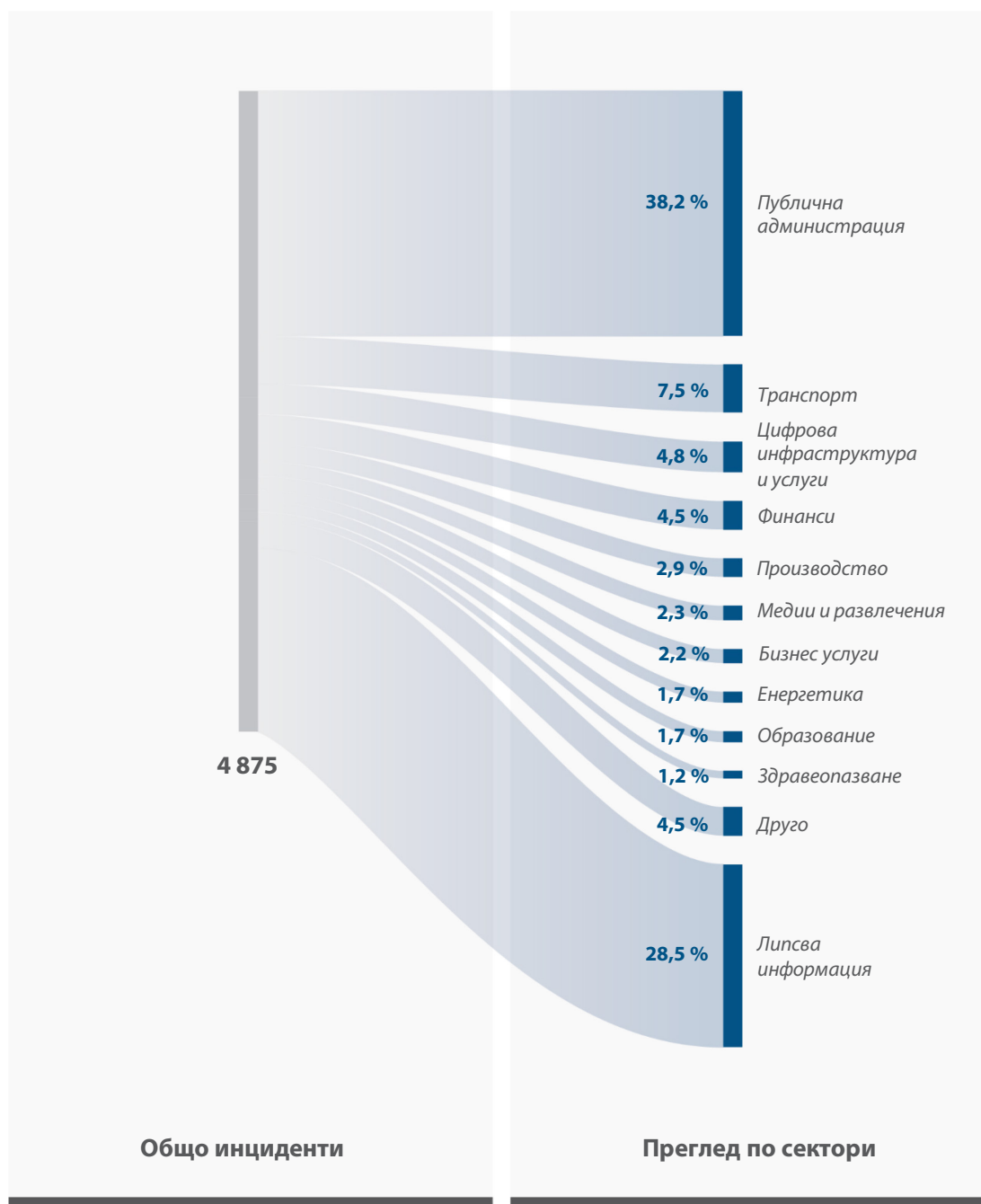
Фигура 1 | Примери за дейности в областта на киберсигурността

Предотвратяване 	Намаляване на риска от киберинциденти и свеждане до минимум на потенциалните последици от тях <i>антивирусни програми, защитни стени, криптиране, двуфакторна автентификация, управление на актуализирането на софтуера, обучение на персонала по въпросите на киберсигурността</i>
Откриване 	Откриване на злонамерени действия в киберпространството <i>Примери: наблюдение на мрежата, ситуационна осведоменост</i>
Реакция 	Управление и смекчаване на последиците от киберинциденти чрез ограничаване на заплахата и предотвратяване на по-нататъшни щети <i>Пример: отстраняване на заплахи, ограничаване чрез изолиране на сървъри, блокиране на компрометирани профили и задаване на нови пароли</i>
Възстановяване 	Възстановяване на сигурното и оперативното функциониране на засегнатите системи, данни и услуги <i>Примери: повторно инсталиране на операционни системи на засегнатите сървъри, възстановяване на данни от резервни копия, извличане на поуки, актуализиране на политиките</i>

Източник: ЕСП, въз основа на съображение 78 от Директива (ЕС) 2022/2555 относно мерки за високо общо ниво на киберсигурност (Директива МИС 2).

02 **Агенцията на Европейския съюз за киберсигурност (ENISA)** счита, че заплахите за киберсигурността са съществени, като същевременно отбелязва, че картината на тези заплахи е станала значително по-сложна и тази тенденция продължава³. Наличието на такива заплахи превръща киберсигурността във фактор от жизненоважно значение във все по-цифровизираните икономики и общества. В своя [доклад относно картината на заплахите за 2025 г.](#) ENISA е посочила софтуера за изнудване като най-критичната заплаха в ЕС. На [фигура 2](#) са представени секторите, които са обект на киберзаплахи.

³ Доклад на ENISA за състоянието на киберсигурността в Съюза за 2024 г.

Фигура 2 | Сектори, обект на кибератаки

Източник: ЕСП, въз основа на информация от [ENISA](#).

Значителни и мащабни киберинциденти

03 Киберинцидентите, които включват киберзаплахи и непреднамерени събития (като посочените на [фигура 3](#) и в точка [40](#)), „могат да възпрепятстват предоставянето на обществени услуги и осъществяването на икономически дейности,... да доведат до значителни финансови загуби, да нарушат доверието на потребителите, да нанесат големи вреди на икономиката на Съюза и дори да имат застрашаващи здравето или живота последици“⁴. Даден киберинцидент се счита за⁵:

- **значителен**, ако е причинил или би могъл да причини сериозни оперативни смущения на услугите или финансови загуби за съответния субект или ако е засегнал или би могъл да засегне други физически или юридически лица, като причини значителни имуществени или неимуществени вреди;
- **мащабен**, ако е причинил степен на смущение, надхвърляща способността на дадена държава членка да реагира на него, или има значително въздействие върху най-малко две държави членки.

04 Мащабният киберинцидент може да се разрасне и да се превърне в същинска **криза в областта на киберсигурността в ЕС**, ако възпрепятства правилното функциониране на вътрешния пазар или създава сериозни рискове за публичната сигурност и безопасност за субектите или гражданите в няколко държави членки или в Съюза като цяло⁶.

⁴ Съображение 2 от Регламент (ЕС) 2025/38 ([Законодателен акт в областта на киберсолидарността](#)).

⁵ Членове 6 и 23 от [Директивата за МИС 2](#), допълнително прецизирани в [регламент за изпълнение \(ЕС\) 2024/2690 на Комисията](#) за определени доставчици в сектора на цифровата инфраструктура.

⁶ Съображение 69 от [Директивата за МИС 2](#).

Рамка на политиката на ЕС

- 05** Екосистемата на киберсигурност на ЕС е сложна и многопластова и обхваща редица области на вътрешната политика като правосъдие и вътрешни работи, цифровия единен пазар и политиките в областта на научните изследвания⁷. Във външната политика киберсигурността е част от дипломацията и все по-значим елемент от формиращата се отбранителна политика на ЕС⁸.
- 06** През последните години ЕС е усъвършенствал нормативната си рамка в областта на киберсигурността. На [фигура 3](#) по-долу са представени най-значимите законодателни и политически инструменти на равнището на ЕС. В съответствие с обхвата на одита (вж. точки [13—14](#)) ЕСП се съсредоточи върху инструментите за откриване и реагиране при значителни и мащабни киберинциденти.

⁷ Информационно-аналитичен документ на ЕСП относно предизвикателствата пред ефективното прилагане на политиката за киберсигурност на ЕС, стр. 12.

⁸ Например позицията на Европейския съюз в киберпространството (2022 г.), рамката за координиран отговор на ЕС на хибридни кампании (2022 г.), политиката на ЕС в областта на киберотбраната (2023 г.) и преразгледания инструментариум за кибердипломация (2023 г.).

Фигура 3 | Важно законодателство и инструменти на политиката на ЕС в областта на киберсигурността

- Приемане на законодателство и инструменти на
- Създаване на мрежи и структури



Източник: ЕСП.

Роли и отговорности

- 07** Киберсигурността в ЕС е област, която обхваща множество частни и публични субекти на регионално, национално и европейско равнище в гражданската сфера, вкл. В правоприлагането. Тя е ключов елемент и на националната сигурност и отбрана⁹. ЕСП представя описание на настоящата среда за киберсигурност на ЕС в [приложение II](#).
- 08** Държавите членки носят основната отговорност за превенцията, готовността и реагирането при киберинциденти и кризи, които ги засягат. Съгласно [член 4, параграф 2 от Договора за Европейския съюз](#) националната сигурност остава единствено в рамките на отговорността на всяка държава членка. Тъй като тези инциденти могат да нарушат и увредят критичните информационни инфраструктури, от които зависи гладкото функциониране на вътрешния пазар, ЕС също играе важна роля в случай на значителен инцидент или криза¹⁰. Основните субекти в областта на киберсигурността на ниво ЕС са описани на [фигура 4](#) по-долу.

⁹ Становище 02/2023 на ЕСП относно предложения Законодателен акт в областта на киберсолидарността.

¹⁰ Концепция на ЕС относно управлението на кризи в областта на киберсигурността.

Фигура 4 | Субекти на равнище ЕС с ключова роля в киберсигурността



Източник: ЕСП.

Финансиране от ЕС

- 09** Съгласно настоящата многогодишна финансова рамка за периода 2021—2027 г. основният източник на финансиране за областта на киберсигурността е [програмата „Цифрова Европа“ \(DIGITAL\)](#). Стартирана през 2021 г., това е първата програма на ЕС, която е насочена специално към цифровата трансформация на ЕС, и разполага с общ бюджет от 8,1 млрд. евро¹¹.
- 10** Програма „Цифрова Европа“ финансира действия в областта на киберсигурността в рамките на специфична цел 3 „Киберсигурност и доверие“. По-конкретно, заделен е бюджет от 1,4 млрд. евро за:
- засилване на координацията в областта на киберсигурността между инструментите и инфраструктурата за данни на държавите членки;
 - подкрепа за широко внедряване на решения, свързани с киберсигурността, във всички сектори на икономиката.
- 11** По-голямата част от финансирането по програма „Цифрова Европа“ за киберсигурност се предоставя чрез покани за представяне на предложения, като в периода от ноември 2021 г. до декември 2025 г. са били публикувани 12 покани. Заделеното за тези покани финансиране възлиза общо на 825 млн. евро. За 2026 г. и 2027 г. са планирани нови покани за представяне на предложения за отпускане на допълнителни 212 млн. евро под формата на безвъзмездна финансова помощ.
- 12** Друга значима програма на ЕС в подкрепа на киберсигурността е [„Хоризонт Европа“](#). Проектите в областта на киберсигурността се финансират главно по [кълъстер 3 „Гражданска сигурност за обществото“](#) и обикновено са на ранен етап на развитие поради акцента на „Хоризонт Европа“ върху научните изследвания и иновациите. [Механизмът за възстановяване и устойчивост](#) също предоставя финансиране за мерки за киберсигурност.

¹¹ Програма „Цифрова Европа“.

Обхват и подход на одита

- 13** Увеличаването на киберзаплахите и тяхното потенциално въздействие засилват необходимостта от укрепване на колективната ни киберустойчивост. Целта на одита на ЕСП беше да провери дали действията на ЕС ефективно подпомагат откриването и реакцията при значителни и мащабни киберинциденти. По-специално, ЕСП разглежда този аспект по отношение на:

- мрежите и механизмите на равнището на ЕС (а именно мрежата на ЕРИКС, EU-CyCLONe, Европейската система за предупреждение в областта на киберсигурността, Центъра за киберситуации и Резерва за киберсигурност на ЕС);
- действията, финансирани по програма „Цифрова Европа“.

Одитът на ЕСП не включва сътрудничеството в областта на правоприлагането на равнището на ЕС, нито действията за кибервъзпиране, предприети на равнището на ЕС чрез дипломатически мерки или дейности в областта на отбраната.

- 14** Одитът обхваща периода 2022—2025 г. Той се основава на документна проверка и анализ на относимите документи, одитни посещения в три държави членки — Ирландия, Гърция и Италия, както и писмени въпросници и интервюта със съответните заинтересовани страни. На [фигура 5](#) е показано как ЕСП събра доказателствата за своите констатации и оценки.

Фигура 5 | Извършена одитна дейност

ЕСП провери

- **Правната рамка**, уреждаща откриването и реакцията при значителни и мащабни киберинциденти
- **Ролите и отговорностите** на мрежите и структурите, създадени на равнище ЕС

ЕСП анализира

- Документи относно функционирането на **мрежата на ЕРИКС и EU-CyCLONe**
- Документацията относно **рамката за програмиране и мониторинг на изпълнението на програмата „Цифрова Европа“**
- Документация за **13 избрани действия, финансирани от ЕС** (11 договора за безвъзмездна финансова помощ и 2 други договора — вж. подробния списък в приложение III)

* ЕСП избра финансирани от ЕС действия в три държави (Ирландия, Гърция и Италия), където е предоставено съществено по размер финансиране по програмата „Цифрова Европа“. 11-те договора за безвъзмездна финансова помощ бяха подбрани измежду 137 финансирани от ЕС проекта, свързани с откриването и реакцията при заплахи, с цел да се обхване комбинация от различни проекти.

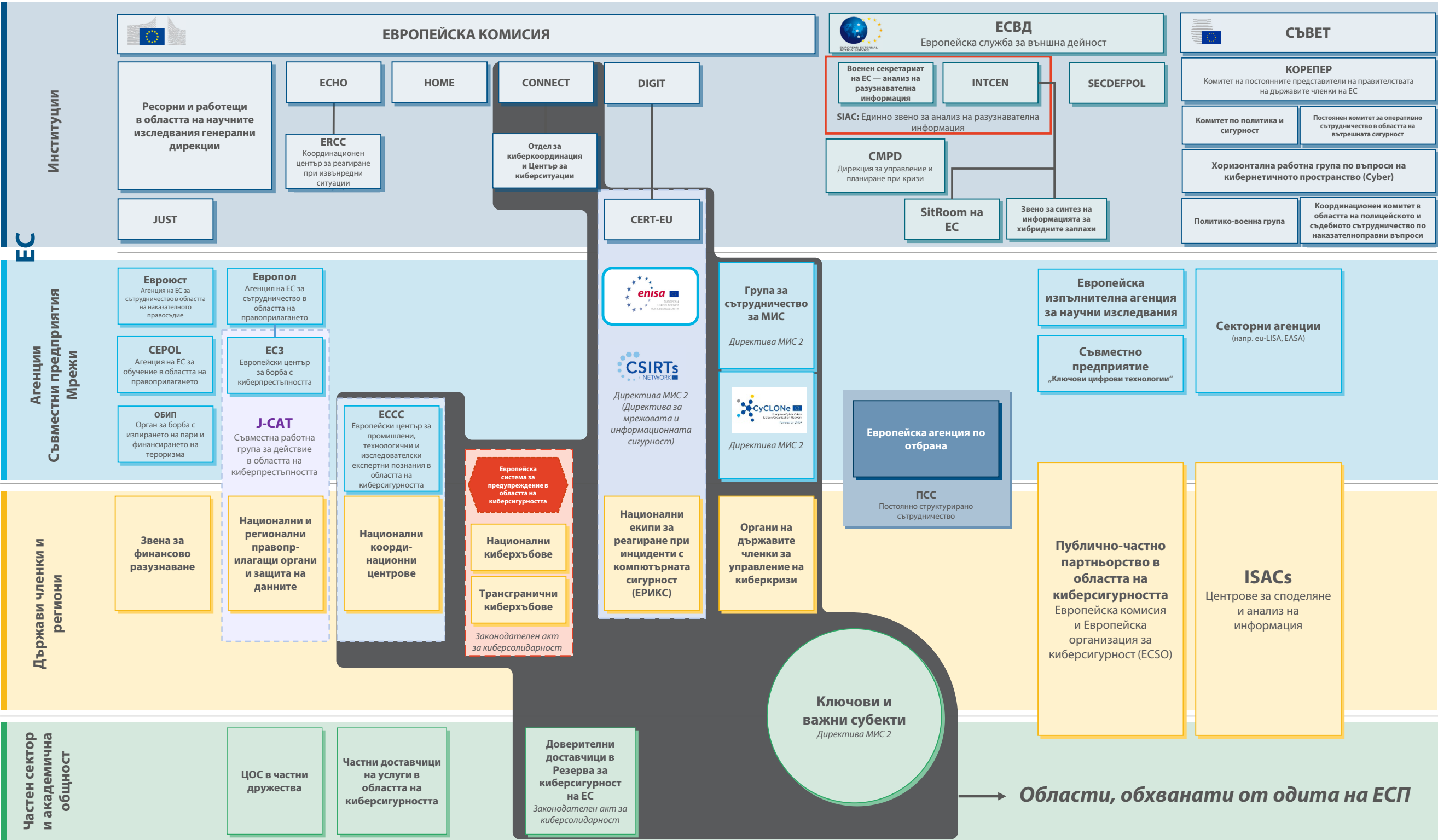
ЕСП проведе интервюта

- Бенефициенти на **11-те договора за безвъзмездна финансова помощ, финансирани от ЕС, включени в извадката**
- Представители на националните органи за киберсигурност в **три държави членки** (Ирландия, Гърция и Италия)
- Представители на Европейската комисия (**ГД „Съобщителни мрежи, съдържание и технологии“**), **ENISA** и **ЕССС**

Източник: ЕСП.

- 15** ЕСП очаква констатациите ѝ да допринесат за повишаване на ефективността и ефикасността на ЕС при откриването и реагирането при значителни и мащабни киберинциденти, както и за подобряване на начина, по който се подбират и наблюдават финансираните от ЕС действия. [Одитната методология](#) на ЕСП съответства на международните одитни стандарти, издадени от [Международната организация на върховните одитни институции \(ИНТОСАЙ\)](#).

Приложение II — Среда за киберсигурност на ЕС



CONNECT: Генерална дирекция „Съобщителни мрежи, съдържание и технологии“ на Европейската комисия
ECCHO: Генерална дирекция „Европейска гражданска защита и европейски операции за хуманитарна помощ“ на Европейската комисия
HOME: Генерална дирекция „Миграция и вътрешни работи“
JUST: Генерална дирекция „Правосъдие и потребители“
DIGIT: Генерална дирекция „Цифрови услуги“
EASA: Агенция за авиационна безопасност на Европейския съюз
EU-CyCLONE: Европейска мрежа за връзка на организациите при киберкризи
eu-LISA: Агенция на Европейския съюз за оперативното управление на широкомащабни информационни системи в пространството на свобода, сигурност и правосъдие
INTSEN: Център на ЕС за анализ на информация
SECDEFPOL: Дирекция „Политика за сигурност и отбрана“
ЦОС: Център за операции по сигурността

Приложение III — Избрани действия в областта на киберсигурността

Идентификационен номер	Наименование	Държави	Начална дата	Крайна дата	Общо разходи (в млн. евро) и участие на ЕС (в проценти)	Връзка към Портала на ЕС за финансиране и обществени поръчки
Безвъзмездна финансова помощ за трансгранични киберхъбове, които са част от Европейската система за предупреждение в областта на киберсигурността						
1	Създаване на трансгранични центрове за операции по сигурността (ATHENA)	България, Гърция, Кипър, Малта	1.1.2024 г.	31.3.2028 г.	4,7 (50 %)	
2	ПЛАТФОРМА ENSOC-CROSSBORDER (ENSOC)	Испания, Италия, Люксембург, Нидерландия, Австрия, Португалия, Румъния	1.1.2024 г.	30.6.2028 г.	10,4 (50 %)	
Безвъзмездна финансова помощ за създаване на мрежата от национални координационни центрове (НКЦ) в държавите членки						
3	Разработване и изпълнение на Националния център за координация и развитие в областта на киберсигурността на Ирландия (NCC-IE)	Ирландия	2.10.2023 г.	1.10.2026 г.	4,2 (47 %)	
4	Национален координационен център на Италия (NCC-IT)	Италия	1.11.2023 г.	31.10.2025 г.	2,0 (50 %)	

Идентификационен номер	Наименование	Държави	Начална дата	Крайна дата	Общо разходи (в млн. евро) и участие на ЕС (в проценти)	Връзка към Портала на ЕС за финансиране и обществени поръчки
Безвъзмездна финансова помощ за изграждане на капацитета на центровете за операции по сигурността (ЦОС), насърчаване на нови приложения на ИИ и други базови технологии за центровете и предоставяне на подкрепа за подобряване на готовността и взаимопомощ						
5	Повишаване на капацитета на консолидирания център за операции по сигурността на Гърция (EL-SOC)	Гърция, Кипър	1.1.2024 г.	31.12.2026 г.	9,7 (50 %)	
6	Център за операции по сигурността за малки и средни предприятия в Гърция (GR-SME-SOC)	Гърция	1.1.2024 г.	31.12.2026 г.	12,1 (50 %)	
7	Центрове за операции по сигурността от следващо поколение (NG-SOC)	Гърция, Испания, Кипър, Люксембург, Словения, Норвегия	1.1.2024 г.	31.12.2026 г.	4,8 (50 %)	
8	Център за операции по сигурността на местното управление в Ирландия (ILG-SOC)	Ирландия	1.10.2023 г.	30.9.2026 г.	8,3 (50 %)	
9	Взаимосвързана екосистема от мрежи за координация и реагиране в областта на киберсигурността (Cyber-CORE-Network)	Ирландия	1.1.2024 г.	31.12.2026 г.	3,6 (50 %)	
10	Осигуряване на съгласуваност между хората, процесите и технологиите с оглед постигането на устойчива киберсигурност (CYberSynchrony)	Белгия, Гърция, Италия, Кипър, Нидерландия	1.6.2024 г.	31.5.2027 г.	7,0 (100 %)	
11	Усъвършенствани центрове за съвместни операции по сигурността (ACSOC)	Гърция, Италия, Румъния	1.1.2025 г.	31.12.2027 г.	3,0 (50 %)	

Идентификационен номер	Наименование	Държави	Начална дата	Крайна дата	Общо разходи (в млн. евро) и участие на ЕС (в проценти)	Връзка към Портала на ЕС за финансиране и обществени поръчки
Рамково споразумение за Действието на ENISA за подкрепа на киберсигурността						
12	Подпомагане за ENISA за предоставяне на услуги в рамките на Действието за подкрепа в областта на киберсигурността (28 обособени позиции)	обособени позиции на 27 държави членки 1 общоевропейска обособена позиция	1.12.2022 г. ¹	31.12.2025 г.	28,3 (100 %)	
Договор за услуги за Центъра за киберситуации на ГД „Съобщителни мрежи, съдържание и технологии“						
13	Специална служба за подкрепа на Центъра за киберситуации и анализ за Европейската комисия	—	30.12.2022 г.	30.12.2026 г.	18,0 (100 %)	

Източник: ЕСП.

¹ През декември 2022 г. са сключени множество договори.

Приложение IV — Оценка на ЕСП на финансираните от ЕС проекти в областта на киберсигурността

Идентификационен номер	Проект	Задоволителна оценка Незадоволителна оценка Установени известни слабости Не е възможно да се направи заключение (поради ранния етап на изпълнение)				Проектът отговаря на повечето от нуждите, посочени в поканата	Планираните крайни продукти и резултати по проекта са осъществени до момента	Крайните продукти по проекта са осъществени в определения срок	Показателите за изпълнение по проектите са подходящи и измерими и за тях са определени базови и целеви стойности
1	Създаване на трансгранични центрове за операции по сигурността (ATHENA)								
2	ПЛАТФОРМА ENSOC-CROSSBORDER (ENSOC)								
3	Разработване и внедряване на Националния център за координация и развитие в областта на киберсигурността на Ирландия (NCC-IE)								
4	Национален координационен център на Италия (NCC-IT)								
5	Повишаване на капацитета на консолидирания център за операции по сигурността на Гърция (EL-SOC)								
6	Център за операции по сигурността за малки и средни предприятия в Гърция (GR-SME-SOC)								
7	Центрове за операции по сигурността от следващо поколение (NG-SOC)								
8	Център за операции по сигурността на местното управление в Ирландия (ILG-SOC)								
9	Взаимосвързана екосистема от мрежи за координация и реагиране в областта на киберсигурността (Cyber-CORE-Network)								
10	Осигуряване на съгласуваност между хората, процесите и технологиите с оглед постигането на устойчива киберсигурност (CYberSynchrony)								
11	Усъвършенствани центрове за съвместни операции по сигурността (ACSOC)								

Съкращения

Съкращение	Определение/обяснение
CSIRT	Екип за реагиране при инциденти с компютърната сигурност
DIGITAL	Програма „Цифрова Европа“
ECCC	Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността
ENISA	Агенция на Европейския съюз за киберсигурност
EU-CyCLONe	Мрежа за връзка на организациите при кибернетични кризи
FSTP	Финансова подкрепа за трети страни
SAG	Стратегическа консултативна група
ГД „Съобщителни мрежи, съдържание и технологии“ (CONNECT)	Генерална дирекция „Съобщителни мрежи, съдържание и технологии“ на Европейската комисия
МИС	Мрежова и информационна сигурност
МСП	Малки и средни предприятия
НКЦ	Национален координационен център
ОКС	Оценка на собствеността и контрола
ЦОС	Център за операции по сигурността

Речник на термините

Термин	Определение/обяснение
Значителен инцидент, свързан с киберсигурността / значителен киберинцидент	Инцидент, свързан с киберсигурността, който е причинил или може да причини сериозни вреди или финансови загуби за дадена организация, или значителни вреди за други организации и лица.
Инцидент, свързан с киберсигурността / киберинцидент	Инцидент, който застрашава наличността, автентичността, целостта или поверителността на данните или информационните системи.
Киберзаплаха	Възможно използване на киберпространството за застрашаване на наличността, автентичността, целостта или поверителността на данните или информационните системи.
Киберхъб	Централна платформа, обединяваща различни услуги, инструменти и ИТ специалисти с цел подобряване на мониторинга, откриването и анализа на киберзаплахи, предотвратяване на киберинциденти и помощ за изготвянето на разузнавателни данни за киберзаплахи.
Масшабен инцидент, свързан с киберсигурността / масшабен киберинцидент	Киберинцидент, който нанася изключително големи вреди, с които една държава членка не може да се справи самостоятелно, или който засяга значително най-малко две държави членки.
Софтуер за изнудване	Зловреден софтуер, който не позволява на жертвите достъп до дадена компютърна система или прави файловете нечетими чрез криптиране, обикновено принуждавайки жертвата да плати откуп, за да възстанови достъпа.
Таксономия	В контекста на киберсигурността — схема за класификация, използвана за организиране, категоризиране и структуриране на знанията за основни понятия като заплахи и инциденти.
Участник в заплаха	Лице или група от лица, които умишлено причиняват вреда и прекъсване на услуги или извършват кражба на данни чрез използване на уязвимости в ИТ системи, мрежи и устройства.
Център за операции по сигурността	Организационно звено, чиято задача е да предотвратява киберзаплахи и инциденти и да събира свързана с това информация.

Отговори на Комисията

<https://www.eca.europa.eu/bg/publications/SR-2026-19>

Отговори на Европейския център за експертни познания в областта на киберсигурността (ЕССС)

<https://www.eca.europa.eu/bg/publications/SR-2026-19>

Отговори на Агенцията на Европейския съюз за киберсигурност (ENISA)

<https://www.eca.europa.eu/bg/publications/SR-2026-19>

Хронология

<https://www.eca.europa.eu/bg/publications/SR-2026-19>

Одитен екип

Специалните доклади на Европейската сметна палата представят резултатите от нейните одити на политики и програми на ЕС или теми, свързани с управлението, в конкретни бюджетни области. ЕСП подбира и разработва одитните си задачи така, че те да окажат максимално въздействие, като отчита рисковете за изпълнението или съответствието, проверявания обем приходи или разходи, предстоящите промени, както и политическия и обществен интерес.

Настоящият одит на изпълнението беше извършен от Одитен състав III „Външни действия, сигурност и правосъдие“, с ръководител George-Marius Hyzler — член на ЕСП. Одитът беше ръководен от члена на ЕСП George-Marius Hyzler, със съдействието на Romuald Kayibanda — ръководител на неговия кабинет, и Annette Farrugia — аташе в кабинета; Cyril Messein — главен ръководител; Frédéric Soblet — ръководител на задача; Jurgen Manjé и Flavia Di Marco — одитори. Zoe Amador Martínez предостави езикова подкрепа. Dunja Weibel предостави подкрепа за графичното оформление.



От ляво надясно: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé, Cyril Messein.

АВТОРСКО ПРАВО

© Европейски съюз, 2026 г.

Политиката на ЕСП относно повторната употреба на информация е определена в [Решение № 6-2019 на Европейската сметна палата](#) относно политиката за свободно достъпни данни и повторната употреба на документи.

Освен ако не е посочено друго (например в отделни известия за авторските права), създаденото от ЕСП съдържание, притежавано от ЕС, е лицензирано по [Creative Commons Attribution 4.0 International \(CC BY 4.0\)](#). Това означава, че като правило повторната употреба е позволена, при условие че са посочени първоначалните източници и всички извършени промени. Лицето, което използва информацията на ЕСП повторно, следва да не изменя първоначалния смисъл или послание на документите. ЕСП не носи отговорност за последствия, възникнали в резултат на повторната употреба.

Необходимо е да се получи допълнително разрешение в случаите, когато дадено съдържание изобразява разпознаваеми частни лица, например на снимки на персонала на ЕСП, или когато е включено съдържание на трети страни.

В случаите, когато е получено такова разрешение, то отменя и заменя горепосоченото общо разрешение и ясно посочва всички ограничения при използването.

За използването или възпроизвеждането на съдържание, което не е собственост на ЕС, може да е необходимо да се потърси разрешение директно от носителите на авторските права.

Снимка на корицата: © 4AXY – stock.adobe.com.

Фигури 6 и 8 — икони: Тези фигури са създадени с ресурси от [Flaticon.com](https://flaticon.com).

© Freepik Company S.L. Всички права са запазени.

Фигура 5 — карти: [Евростат](#).

Софтуер или документи, обхванати от правата на индустриална собственост, като патенти, търговски марки, регистрирани дизайни, лого и наименования, са изключени от политиката на ЕСП за повторно използване.

Уебсайтовете на всички институции на Европейския съюз, включени в домейна europa.eu, съдържат препратки към сайтове на трети страни. Тъй като ЕСП не контролира съдържанието им, моля, запознайте се с тяхната политика за поверителност на данните и с политиката за авторските права.

Използване на логото на ЕСП

Логото на ЕСП не може да бъде използвано без предварително разрешение.

HTML	ISBN 978-92-849-7849-6	ISSN 1977-5814	doi:10.2865/7957497	QJ-01-26-032-BG-Q
PDF	ISBN 978-92-849-7850-2	ISSN 1977-5814	doi:10.2865/2579900	QJ-01-26-032-BG-N

ЦИТИРАНЕ НА ПУБЛИКАЦИЯТА

Европейска сметна палата, [Специален доклад 19/2026](#) „Киберинциденти — откриване и реакция: рамката на ЕС за сътрудничество се усъвършенства, но все още не функционира пълноценно поради закъснения в изпълнението и ограничен обмен на информация“, Служба за публикации на Европейския съюз, 2026 г.

През последните години ЕС е усъвършенствал нормативната си рамка в областта на киберсигурността и е създал различни мрежи и механизми за борба с киберинциденти. Той финансира и проекти, свързани с киберсигурността, чрез програма „Цифрова Европа“.

Европейската сметна палата (ЕСП) заключи, че действията на ЕС само частично подпомагат откриването и реакцията при значителни и мащабни киберинциденти. Въпреки че необходимата рамка за сътрудничество постепенно се изгражда, тя все още не е изцяло завършена. Ограниченият обмен на информация, слабостите в докладването и значителните закъснения в изпълнението ѝ не позволяват на мрежите и механизмите на ЕС до достигнат пълния си потенциал. Въпреки че съдържат подходящи цели, много проекти са засегнати от оперативни трудности и забавяния. Освен това съществуват слабости в общата рамка за мониторинг на изпълнението. ЕСП отправя препоръки с оглед на преодоляването на тези недостатъци.

Специален доклад на ЕСП съгласно член 287, параграф 4, втора алинея от ДФЕС.



ЕВРОПЕЙСКА
СМЕТНА
ПАЛАТА



Служба за публикации
на Европейския съюз

ЕВРОПЕЙСКА СМЕТНА ПАЛАТА
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Тел. +352 4398-1

За запитвания: eca.europa.eu/bg/contact
Уебсайт: eca.europa.eu
Социални медии: @EUauditors