Съвет на
Европейския съюз

Брюксел, 20 април 2023 г.
(OR. en)

8512/23

Междуинституционално досие:
2023/0109(COD)

CYBER 92
TELECOM 108
CADREFIN 51
FIN 448
BUDGET 6
IND 181
JAI 471
MI 314
DATAPROTECT 110
RELEX 481
CODEC 662

ПРЕДЛОЖЕНИЕ

От:	Генералния секретар на Европейската комисия, подписано от г-жа Martine DEPREZ, директор
Дата на получаване:	19 април 2023 г.
До:	Г-жа Thérèse BLANCHET, генерален секретар на Съвета на Европейския съюз
№ док. Ком.:	COM(2023) 209 final
Относно:	Предложение 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

Приложено се изпраща на делегациите документ COM(2023) 209 final.

Приложение: COM(2023) 209 final

ЕВРОПЕЙСКА
КОМИСИЯ

Страсбург, 18.4.2023 г.
COM(2023) 209 final

2023/0109 (COD)

Предложение 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

ОБЯСНИТЕЛЕН МЕМОРАНДУМ

1. КОНТЕКСТ НА ПРЕДЛОЖЕНИЕТО

• Основания и цели на предложението

Настоящият обяснителен меморандум придружава предложението за законодателен акт за киберсолидарност. Всички сектори на икономиката използват и се осланят на информационните и комуникационните технологии като съществен компонент на дейността си, тъй като нашите публични администрации, предприятия и граждани са повече от всякога тясно свързани и взаимозависими отвъд сектора и териториалните граници. По-голямото използване на цифрови технологии увеличава риска от излагане на киберинциденти и потенциалните последици от тях. Същевременно държавите членки са изправени пред нарастващи киберрискове и цялостна сложна картина на заплахите, с ясен риск от бързо разпространение на киберинциденти от една държава членка към други държави членки.

Освен това операциите в областта на киберсигурността все повече се интегрират в хибридните и военните стратегии, като оказват значително въздействие върху целта. По-специално военната агресия на Русия срещу Украйна беше предшествана и се придружава от стратегия за враждебни кибероперации — обстоятелство, което променя начина на възприемане и оценяване на колективната готовност на ЕС за управление на кризи в областта на киберсигурността и е призив за спешни действия. Заплахата от евентуален мащабен киберинцидент, причиняващ значителни смущения и вреди на критичните инфраструктури, изисква повишена готовност на всички нива на екосистемата на киберсигурност на ЕС. Тази заплаха надхвърля рамките на военната агресия на Русия в Украйна и включва постоянни киберзаплахи от страна на държавни и недържавни участници, които вероятно ще продължат да съществуват, като се има предвид многообразието от свързани с държави участници, престъпни участници и хактивисти, замесени в настоящото геополитическо напрежение. През последните години броят на кибератаките се увеличи значително, включително атаките на веригата за доставки, целящи кибершпионаж, софтуер за изнудване или смущения. През 2020 г. атаката на веригата за доставки SolarWinds засегна повече от 18 000 организации в световен мащаб, включително правителствени агенции, големи дружества. Значителните инциденти в областта на киберсигурността могат да нанесат прекалено големи вреди, с които засегнатите държави членки, било то една или няколко, не са в състояние да се справят сами. Поради тази причина е необходима засилена солидарност на равнището на Съюза, за да може по-ефективно да се откриват киберзаплахите и да се подобри подготовката и реагирането при киберинциденти.

Що се отнася до откриването на киберзаплахи и инциденти, съществува спешна необходимост от увеличаване на обмена на информация и подобряване на

колективните ни способности, за да се намали значително времето, необходимо за откриване на киберзаплахи, преди да могат да причинят мащабни вреди и разходи[1]. Въпреки че много киберзаплахи и инциденти имат потенциално трансгранично измерение поради взаимното свързване на цифровите инфраструктури, обменът на съответната информация между държавите членки остава ограничен. Изграждането на мрежа от трансгранични центрове за операции по сигурността (ЦОС) за подобряване на възможностите за откриване и реагиране има за цел да помогне за решаването на този проблем.

Що се отнася до готовността и реагирането при киберинциденти, понастоящем подкрепата на равнището на Съюза и солидарността между държавите членки са ограничени. В заключенията на Съвета от октомври 2021 г. беше подчертана необходимостта от преодоляване на тези недостатъци, като Комисията беше призована да представи предложение за нов фонд за реагиране при извънредни ситуации в областта на киберсигурността[2].

С настоящия регламент се изпълнява и Стратегията за киберсигурност за цифровото десетилетие, приета през декември 2020 г.[3], в която се обявява създаването на европейски киберщит, с който се укрепват способностите за откриване на киберзаплахи и обмен на информация в Европейския съюз чрез обединение на национални и трансгранични ЦОС.

Настоящият регламент се основава на първите стъпки, които вече са разработени в тясно сътрудничество с основните заинтересовани страни и са подкрепени от програмата „Цифрова Европа“. По-специално що се отнася до ЦОС, в рамките на работната програма за киберсигурност на програмата „Цифрово десетилетие“ за периода 2021—2022 г. бяха отправени покана за заявяване на интерес за съвместно закупуване на инструменти и инфраструктура за създаване на трансгранични ЦОС и покана за предоставяне на безвъзмездни средства, за да се даде възможност за изграждане на капацитет на ЦОС, обслужващи публични и частни организации. По отношение на готовността и реагирането при инциденти Комисията създаде краткосрочна програма за подпомагане на държавите членки чрез допълнително финансиране, отпуснато на Агенцията на Европейския съюз за киберсигурност (ENISA), с цел незабавно укрепване на готовността и способността за реагиране при големи киберинциденти. И двете действия бяха подготвени в тясна координация с

---

[1] Според доклад на Ponemon Institute и IBM Security средното време за идентифициране на нарушение на сигурността през 2022 г. е 207 дни, а за овладяването му са необходими още 70 дни. Същевременно през 2022 г. нарушенията на сигурността на данните с жизнен цикъл над 200 дни са довели до средни разходи от 4,86 милиона евро в сравнение с 3,74 милиона евро при нарушенията под 200 дни. („Cost of a data breach 2022“ — „Цената на нарушение на сигурността на данните през 2022 г.“, https://www.ibm.com/reports/data-breach).

[2] Заключения на Съвета относно установяването на позицията на Европейския съюз в киберпространството, одобрени от Съвета на заседанието му от 23 май 2022 г., 9364/22.

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

държавите членки. С настоящия регламент се отстраняват недостатъците и се интегрират резултатите от тези действия.

И накрая, с настоящото предложение се изпълнява ангажиментът, поет в съответствие със Съвместното съобщение относно киберотбраната[4], прието на 10 ноември, за изготвяне на предложение за инициатива за киберсолидарност на ЕС със следните цели: укрепване на общите способности на ЕС за откриване, ситуационна осведоменост и реагиране, постепенно изграждане на резерв за киберсигурност на равнището на ЕС от услуги от доверителни частни доставчици и подпомагане на изпитването на критични субекти.

В този контекст Комисията предлага настоящия законодателен акт за киберсолидарност, за да се засили солидарността на равнището на Съюза с цел по-добро откриване, подготовка и реагиране на киберзаплахи и киберинциденти чрез следните специфични цели:

- засилване на общото за ЕС откриване и ситуационна осведоменост за киберзаплахите и киберинцидентите, като по този начин се допринася за европейския технологичен суверенитет в областта на киберсигурността;
- укрепване на готовността на критичните субекти в целия ЕС и укрепване на солидарността чрез изграждане на общи способности за реагиране при значителни или мащабни киберинциденти, включително чрез предоставяне на подкрепа за реагиране при инциденти на трети държави~~,~~ асоциирани към програмата „Цифрова Европа“;
- повишаване на устойчивостта на Съюза и допринасяне за ефективно реагиране чрез преглед и оценка на значителни или мащабни киберинциденти, включително извличане на поуки и, когато е целесъобразно, препоръки.

Тези цели се изпълняват чрез следните действия:

- разгръщане на общоевропейска инфраструктура от ЦОС (европейски киберщит) за изграждане и подобряване на общите способности за откриване и ситуационна осведоменост;
- създаване на Механизъм за действие при извънредни ситуации в областта на киберсигурността, който да подпомага държавите членки при подготовката, реагирането и незабавното възстановяване след значителни и мащабни киберинциденти. Подкрепа за реагиране при инциденти се предоставя и на институциите, органите, службите и агенциите на ЕС (EUIBA);

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

- създаване на европейски Механизъм за преглед на киберинциденти, чрез който да се разглеждат и оценяват конкретни значителни или мащабни киберинциденти.

Европейският киберщит и Механизмът за действие при извънредни ситуации в областта на киберсигурността ще бъдат подкрепени с финансиране от програмата „Цифрова Европа“, която с настоящия законодателен акт ще бъде изменена, за да се установят горепосочените действия, да се осигури финансова подкрепа за тяхното разработване и да се изяснят условията за ползване на финансовата подкрепа.

•Съгласуваност с действащите разпоредби в тази област на политиката

Рамката на ЕС включва няколко законодателни акта, които вече са в сила или са предложени на равнището на Съюза с цел да се намалят уязвимостите, да се повиши устойчивостта на критичните субекти срещу киберрисковете и да се подпомогне координираното управление на мащабни киберинциденти и кризи, а именно Директивата относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (МИС 2)[5], Актът за киберсигурност[6], Директивата относно атаките срещу информационните системи[7] и Препоръка (ЕС) 2017/1584 на Комисията относно координирана реакция на мащабни киберинциденти и кризи[8].

Действията, предложени в рамките на законодателния акт за киберсолидарност, обхващат ситуационната осведоменост, обмена на информация, както и подкрепата за готовност и реагиране при киберинциденти. Тези действия са в съответствие с действащата регулаторна рамка на равнището на Съюза и подкрепят нейните цели, по-специално съгласно Директива (ЕС) 2022/2555 („Директивата МИС 2“). Законодателният акт за киберсолидарност ще надгражда и подкрепя съществуващите рамки за оперативно сътрудничество и управление на кризи в областта на киберсигурността, по-специално мрежата за връзка на организациите при кибернетични кризи (EU-CyCLONe) и мрежата на екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС).

---

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

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

[7] Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета.

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

Трансграничните платформи на ЦОС следва да изградят нова способност, допълваща мрежата на ЕРИКС, като обединяват и обменят данни за киберзаплахите от публични и частни субекти, повишават стойността на тези данни чрез експертен анализ и най-съвременните инструменти и допринасят за развитието на способностите и технологичния суверенитет на Съюза.

Накрая, настоящото предложение е в съответствие с препоръката на Съвета относно координиран подход на равнището на Съюза за укрепване на устойчивостта на инфраструктурата от критично значение[9], в която държавите членки се приканват да предприемат спешни и ефективни мерки и да си сътрудничат лоялно, ефикасно, солидарно и координирано помежду си, с Комисията и с други съответни публични органи, както и със съответните субекти, за да повишат устойчивостта на инфраструктурата от критично значение, използвана за предоставяне на основни услуги на вътрешния пазар.

- **Съгласуваност с други политики на Съюза**

Предложението е в съответствие с други механизми и протоколи за извънредни ситуации при кризи, като например-механизма за интегрирана реакция при политическа криза (ИРПК). Законодателният акт за киберсолидарност ще допълни тези рамки и протоколи за управление на кризи, като осигури специална подкрепа за готовността и реагирането при киберинциденти. Предложението ще бъде съгласувано и с външната дейност на ЕС в отговор на мащабни инциденти в рамките на общата външна политика и политика на сигурност (ОВППС), включително чрез инструментариума на ЕС за кибердипломация. Предложението ще допълни действията, изпълнявани в контекста на член 42, параграф 7 от Договора за Европейския съюз или в ситуации, определени в член 222 от Договора за функционирането на Европейския съюз.

То също така допълва Механизма за гражданска защита на Съюза (МГЗС)[10], създаден през декември 2013 г. и завършен с нов законодателен акт, приет през май 2021 г.[11], с който се укрепват стълбовете за превенция, готовност и реагиране на МГЗС и се предоставят допълнителни способности на ЕС за реагиране на нови рискове в Европа и света, както и се увеличава стратегическият резерв в rescEU.

---

[9] Препоръка на Съвета от 8 декември 2022 г. относно координиран подход на равнището на Съюза за укрепване на устойчивостта на инфраструктурата от критично значение (текст от значение за ЕИП), 2023/C 20/01.

[10] Решение № 1313/2013/ЕС на Европейския парламент и на Съвета от 17 декември 2013 г. относно Механизъм за гражданска защита на Съюза (текст от значение за ЕИП).

[11] Регламент (ЕС) 2021/836 на Европейския парламент и на Съвета от 20 май 2021 г. за изменение на Решение № 1313/2013/ЕС относно Механизъм за гражданска защита на Съюза (текст от значение за ЕИП).

2. ПРАВНО ОСНОВАНИЕ, СУБСИДИАРНОСТ И ПРОПОРЦИОНАЛНОСТ

• Правно основание

Правното основание за настоящото предложение е член 173, параграф 3 и член 322, параграф 1, буква а) от Договора за функционирането на Европейския съюз (ДФЕС). В съответствие с член 173 от ДФЕС Съюзът и държавите членки гарантират съществуването на условията, необходими за конкурентоспособността на промишлеността на Съюза. Настоящият регламент има за цел да укрепи конкурентната позиция на секторите на промишлеността и услугите в Европа в рамките на цифровизираната икономика, както и да подкрепи тяхната цифрова трансформация, като се повиши нивото на киберсигурността на цифровия единен пазар. По-специално целта му е да се повиши устойчивостта на гражданите, предприятията и субектите, извършващи дейност в критични и висококритични сектори, срещу нарастващите киберзаплахи, които могат да имат опустошително въздействие върху обществото и икономиката.

Предложението се основава и на член 322, параграф 1, буква а) от ДФЕС, тъй като съдържа специални правила за пренасяне чрез дерогация от принципа на ежегодност, установен в Регламент (ЕС, Евратом) 2018/1046 на Европейския парламент и на Съвета („Финансовия регламент“)[12]. С оглед на доброто финансово управление и като се има предвид непредвидимият, извънреден и специфичен характер на положението в областта на киберсигурността и киберзаплахите, Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да се ползва от известна степен на гъвкавост по отношение на бюджетното управление, и по-специално като се позволи неизползваните бюджетни кредити за поети задължения и за плащания за действия за постигане на целите, определени в регламента, да бъдат автоматично пренасяни за следващата финансова година. Тъй като това ново правило повдига въпроси, свързани с Финансовия регламент, тази тема може да бъде разгледана в контекста на текущите преговори за преработване на Финансовия регламент.

• Субсидиарност (при неизключителна компетентност)

Силно изразеният трансграничен характер на киберзаплахите и нарастващият брой на рисковете и инцидентите, които се разпространяват в други държави, сектори и продукти, означават, че целите на настоящата намеса не могат да бъдат постигнати ефективно само от държавите членки и изискват общи действия и солидарност на равнището на Съюза.

Опитът от противодействието на киберзаплахите, произтичащи от войната срещу Украйна, както и поуките, извлечени от учението в областта на киберсигурността, проведено по време на френското председателство (EU-CyCLES), показаха, че за

[12] Регламент (ЕС, Евратом) 2018/1046 на Европейския парламент и на Съвета от 18 юли 2018 г. за финансовите правила, приложими за общия бюджет на Съюза (ОВ L 193, 30.7.2018 г., стр. 1).

постигане на солидарност на равнището на ЕС следва да се разработят конкретни механизми за взаимна подкрепа, по-специално сътрудничество с частния сектор. В този контекст в заключенията на Съвета от 23 май 2022 г. относно установяването на позицията на Европейския съюз в киберпространството Комисията се призовава да представи предложение за нов фонд за реагиране при извънредни ситуации в областта на киберсигурността.

Подкрепата и действията на равнището на Съюза за по-добро откриване на киберзаплахите и за повишаване на готовността и способността за реагиране осигуряват добавена стойност, тъй като така се избягва дублиране на усилията в Съюза и държавите членки. Това би довело до по-добро използване на съществуващите активи и до по-добра координация и обмен на информация относно извлечените поуки. Механизмът за действие при извънредни ситуации в областта на киберсигурността предвижда и предоставяне на подкрепа на трети държави, асоциирани към програмата „Цифрова Европа“, от резерва за киберсигурност на ЕС.

Подкрепата, предоставяна чрез различните инициативи, които ще бъдат създадени и финансирани на равнището на Съюза, ще допълва и няма да дублира националните способности по отношение на откриването, ситуационната осведоменост, готовността и реагирането при киберзаплахи и инциденти.

• Пропорционалност

Действията не надхвърлят необходимото за постигане на общата и специфичните цели на регламента. Действията в настоящия регламент не засягат отговорностите на държавите членки по отношение на националната сигурност, обществената сигурност, превенцията, разследването, разкриването и наказателното преследване на престъпления. Те не засягат и правните задължения на субектите, извършващи дейност в критични и висококритични сектори, да приемат мерки в областта на киберсигурността в съответствие с Директивата МИС 2.

Действията, обхванати от настоящия регламент, допълват тези усилия и мерки, като подпомагат създаването на инфраструктури за по-добро откриване и анализиране на заплахите и осигуряват подкрепа за действия за готовност и реагиране в случай на значителни или мащабни киберинциденти.

• Избор на инструмент

Предложението е под формата на регламент на Европейския парламент и на Съвета Това е най-подходящият правен инструмент, тъй като само регламент с неговите пряко приложими правни разпоредби може да осигури необходимата степен на еднаквост за създаването и функционирането на европейски киберщит и Механизъм за действие при извънредни ситуации в областта на киберсигурността, като се осигури подкрепа от

програмата „Цифрова Европа“ за тяхното създаване, както и ясни условия за използването и разпределянето на тази подкрепа.

3. РЕЗУЛТАТИ ОТ ПОСЛЕДВАЩИТЕ ОЦЕНКИ, КОНСУЛТАЦИИТЕ СЪС ЗАИНТЕРЕСОВАНИТЕ СТРАНИ И ОЦЕНКИТЕ НА ВЪЗДЕЙСТВИЕТО

• Консултации със заинтересованите страни

Действията, предвидени в настоящия регламент, ще бъдат подкрепени от програмата „Цифрова Европа“, което беше предмет на широка консултация. Освен това те ще се основават на първите стъпки, които бяха подготвени в тясно сътрудничество с основните заинтересовани страни. Що се отнася до ЦОС, Комисията състави концептуален документ относно разработването на трансгранични платформи за ЦОС и покана за заявяване на интерес в тясно сътрудничество с държавите членки в рамките на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността (ECCC). В този контекст беше проведено проучване на способностите на националните ЦОС и бяха обсъдени общи подходи и технически изисквания в рамките на техническата работна група на ECCC, в която участват представители на държавите членки. Освен това беше осъществен обмен с отрасъла, по-специално чрез експертната група на ЦОС, създадена от ENISA и Европейската организация за киберсигурност (ECSO).

На второ място, по отношение на готовността и реагирането при инциденти Комисията създаде краткосрочна програма за подпомагане на държавите членки чрез допълнително финансиране, отпуснато на ENISA от програмата „Цифрова Европа“, с цел незабавно укрепване на готовността и способностите за реагиране при големи киберинциденти. Обратната информация, получена от държавите членки и отрасъла по време на изпълнението на тази краткосрочна програма, вече дава ценни сведения, които са използвани при изготвянето на предложения регламент за отстраняване на установените недостатъци. Това беше първа стъпка в съответствие със заключенията на Съвета относно установяването на позицията на Европейския съюз в киберпространството, в които от Комисията се изисква да представи предложение за нов фонд за реагиране при извънредни ситуации в областта на киберсигурността.

Освен това на 16 февруари 2023 г. въз основа на документ за обсъждане беше проведена работна среща с експерти от държавите членки относно Механизма за действие при извънредни ситуации в областта на киберсигурността. Всички държави членки участваха в тази работна среща, а единадесет държави членки предоставиха допълнителен принос в писмен формат.

- **Оценка на въздействието**

Поради спешния характер на предложението не беше направена оценка на въздействието. Действията, предвидени в настоящия регламент, ще бъдат подкрепени от програмата „Цифрова Европа“ и са в съответствие с определените в регламента за програмата „Цифрова Европа“, който беше предмет на специална оценка на въздействието. Настоящият регламент няма да доведе до значителни административни или екологични въздействия, освен вече оценените в оценката на въздействието на регламента за програмата „Цифрова Европа“.

Освен това той се основава на първите действия, разработени в тясно сътрудничество с основните заинтересовани страни, както е посочено по-горе, и е продължение на призива на държавите членки към Комисията да представи предложение за нов фонд за реагиране при извънредни реагиране в областта на киберсигурността до края на третото тримесечие на 2022 г.

По-конкретно по отношение на ситуационната осведоменост и откриването в рамките на европейския киберщит, като част от работната програма за киберсигурност на програмата „Цифрово десетилетие“ за периода 2021—2022 г. бяха отправени покана за заявяване на интерес за съвместна обществена поръчка за инструменти и инфраструктура с цел създаване на трансгранични ЦОС и покана за предоставяне на безвъзмездни средства, за да се даде възможност за изграждане на капацитет на ЦОС, обслужващи публични и частни организации.

В областта на готовността и реагирането при инциденти, както бе посочено по-горе, Комисията създаде краткосрочна програма за подпомагане на държавите членки от програмата „Цифрова Европа“, която се изпълнява от ENISA. Обхванатите услуги включват действия за готовност, като например изпитването на проникване за критични субекти с цел установяване на уязвимости. С програмата също така се засилват възможностите за подпомагане на държавите членки в случай на сериозен инцидент, засягащ критични субекти. Изпълнението на тази краткосрочна програма от страна на ENISA е в ход и вече са получени относими сведения, които са взети предвид при съставянето на настоящия регламент.

- **Основни права**

Като допринася за сигурността на цифровата информация, настоящото предложение ще допринесе за защитата на правото на свобода и сигурност в съответствие с член 6 от Хартата на основните права на ЕС и на правото на зачитане на личния и семейния живот в съответствие с член 7 от Хартата на основните права на ЕС. Като защитава предприятията от икономически вредни кибератаки, предложението ще допринесе и за свободата на стопанска инициатива в съответствие с член 16 от Хартата на основните

права на ЕС, както и за правото на собственост в съответствие с член 17 от Хартата на основните права на ЕС. И накрая, като защитава целостта на критичната инфраструктура от кибератаки, предложението ще допринесе за правото на закрила на здравето в съответствие с член 35 от Хартата на основните права на ЕС и за правото на достъп до услуги от общ икономически интерес в съответствие с член 36 от Хартата на основните права на ЕС.

4. ОТРАЖЕНИЕ ВЪРХУ БЮДЖЕТА

Действията, предвидени в настоящия регламент, ще бъдат подкрепени с финансиране в рамките на стратегическата цел „Киберсигурност“ на програмата „Цифрова Европа“.

Общият бюджет включва увеличение от 100 милиона евро, за които в настоящия регламент се предлага да бъдат преразпределени от други стратегически цели на програмата „Цифрова Европа“. Така общата сума, която ще бъде на разположение за действия в областта на киберсигурността в рамките на програмата „Цифрова Европа“, ще достигне 842,8 милиона евро.

С част от допълнителните 100 милиона евро ще бъде увеличен бюджетът, управляван от ЕССС, за изпълнение на действия по отношение на ЦОС и готовността като част от работната(ите) им програма(и). Допълнителното финансиране също така ще подпомогне създаването на резерва за киберсигурност на ЕС.

То допълва бюджета, който вече е предвиден за подобни действия в основната програма „Цифрова Европа“ и работните програми за „Киберсигурност“ по програмата „Цифрова Европа“ за периода 2023—2027 г., с което общата сума може да достигне 551 милиона евро за периода 2023—2027 г., като 115 милиона евро вече са били заделени под формата на пилотни проекти за периода 2021—2022 г. Като се включат вноските на държавите членки, общият бюджет може да достигне 1,109 милиарда евро.

Преглед на свързаните разходи е включен в частта „Законодателна финансова обосновка“, придружаваща настоящото предложение.

5. ДРУГИ ЕЛЕМЕНТИ

- **Планове за изпълнение и механизъм за наблюдение, оценка и докладване**

Комисията ще наблюдава изпълнението, прилагането и спазването на новите разпоредби, за да оцени тяхната ефективност. До четири години след датата на прилагането на настоящия регламент Комисията представя на Европейския парламент и на Съвета доклад относно оценката и прегледа на настоящия регламент.

- **Подробно разяснение на конкретните разпоредби на предложението**

Общи цели, предмет и определения (глава I)

В глава I се определят целите на регламента за укрепване на солидарността на равнището на Съюза с цел по-добро откриване, подготовка и реагиране при киберзаплахи и инциденти, и по-специално за засилване на общото за Съюза откриване и ситуационна осведоменост за киберзаплахите и инцидентите, за засилване на готовността на субектите, извършващи дейност в критични и висококритични сектори в целия Съюз, и за укрепване на солидарността чрез развитие на общи способности за реагиране при значителни или мащабни киберинциденти, както и за повишаване на устойчивостта на Съюза чрез преглед и оценка на значителни или мащабни киберинциденти. В тази глава са посочени и действията, чрез които ще бъдат постигнати тези цели: разгръщането на Европейски киберщит, създаването на Механизъм за действие при извънредни ситуации в областта на киберсигурността и на Механизъм за преглед на киберинциденти. В нея са посочени и определенията, използвани в целия инструмент.

Европейски киберщит (глава II)

С глава II се създава европейски киберщит и се посочват различните негови елементи и условията за участие. Първо, в нея е представена общата цел на европейския киберщит, която е да се развият авангардни способности на Съюза за откриване, анализиране и обработване на данни за киберзаплахи и инциденти в Съюза, както и конкретните оперативни цели. В нея се посочва, че финансирането от Съюза на европейския киберщит се осъществява в съответствие с регламента за програмата „Цифрова Европа“.

Освен това в главата се описват видовете субекти, които формират европейския киберщит. Той се състои от национални центрове за операции по сигурността („национални ЦОС“) и трансгранични оперативни центрове по сигурността („трансгранични ЦОС“). Всяка участваща държава членка определя национален ЦОС. Той ще действа като отправна точка и портал за други публични и частни организации на национално равнище за събиране и анализиране на информация относно киберзаплахите и инцидентите и ще допринася за даден трансграничен ЦОС. След покана за заявяване на интерес националният ЦОС може да бъде избран от ЕССС да участва в съвместна обществена поръчка с ЕССС за инструменти и инфраструктури и да получи безвъзмездни средства за управлението на инструментите и инфраструктурите. Ако даден национален ЦОС се възползва от подкрепата на Съюза, той поема ангажимент да кандидатства за участие в трансграничен ЦОС в рамките на две години.

Трансграничните ЦОС се състоят от консорциум от най-малко три държави членки, представени от национални ЦОС, които са поели ангажимент да работят заедно, за да координират своите дейности по откриване и наблюдение на киберзаплахи и инциденти. След първоначална покана за заявяване на интерес ЕССС може да избере консорциум, осигуряващ хостинг, който да участва в съвместна обществена поръчка с ЕССС за инструменти и инфраструктури и да получи безвъзмездни средства за управление на инструментите и инфраструктурите. Членовете на консорциума, осигуряващ хостинг, сключват писмено споразумение за консорциум, в което се определят вътрешните им договорености. След това в тази глава се описват подробно изискванията за обмен на информация между участниците в трансграничен ЦОС и за обмен на информация между трансграничен ЦОС и други трансгранични ЦОС, както и със съответните субекти на ЕС. Националните ЦОС, участващи в трансграничен ЦОС, обменят помежду си относимата информация, свързана с киберзаплахите, като подробностите, включително ангажиментът за обмен на значителен обем данни и съответните условия, следва да бъдат определени в споразумението за консорциум. Трансграничните ЦОС гарантират високо ниво на оперативна съвместимост помежду си. Трансграничните ЦОС следва също така да сключват споразумения за сътрудничество с други трансгранични ЦОС, в които се посочват принципите за обмен на информация. Когато трансграничните ЦОС получат информация, свързана с потенциален или текущ мащабен киберинцидент, те предоставят относимата информация на EU-CyCLONe, мрежата на ЕРИКС и Комисията с оглед на съответните им функции по управление на кризи в съответствие с Директива (ЕС) 2022/2555. Глава II завършва с уточняване на условията за сигурност за участие в европейския киберщит.

Механизъм за действие при извънредни ситуации в областта на киберсигурността (глава III)

С глава III се създава Механизъм за действие при извънредни ситуации в областта на киберсигурността с цел да се подобри устойчивостта на Съюза на големи киберзаплахи и да се подготви и смекчи, с оглед на солидарността, краткосрочното въздействие на значителни и мащабни киберинциденти или кризи. Действията по изпълнение на Механизма за действие при извънредни ситуации в областта на киберсигурността се подкрепят с финансиране от програмата „Цифрова Европа“. С механизма се предвиждат действия в подкрепа на готовността, включително координирано изпитване на субекти, извършващи дейност във висококритични сектори, реагиране и незабавно възстановяване след значителни или мащабни киберинциденти или смекчаване на значителни киберзаплахи и действия за взаимопомощ.

Действията за готовност в рамките на Механизма за действие при извънредни ситуации в областта на киберсигурността включват координирано изпитване на готовността на субектите, извършващи дейност във висококритични сектори. След консултации с ENISA и групата за сътрудничество за МИС Комисията следва редовно да определя съответните сектори или подсектори измежду секторите с висока степен на критичност,

изброени в приложение I към Директива (ЕС) № 2022/2555, от които субектите могат да подлежат на координирано изпитване за готовност на равнището на ЕС.

За целите на прилагането на предложените действия за реагиране при инциденти с настоящия регламент се създава резерв за киберсигурност на ЕС, който се състои от услуги за реагиране при инциденти, предоставяни от доверителни доставчици, избрани в съответствие с критериите, определени в настоящия регламент. Ползвателите на услугите от резерва за киберсигурност на ЕС включват органите за управление на киберкризи и ЕРИКС на държавите членки, както и институциите, органите, службите и агенциите на ЕС. Комисията носи цялостна отговорност за изпълнението на резерва за киберсигурност на ЕС и може да възложи изцяло или частично на ENISA функционирането и управлението на резерва за киберсигурност на ЕС.

За да получат подкрепа от резерва за киберсигурност на ЕС, ползвателите следва да предприемат собствени мерки за смекчаване на последиците от инцидента, във връзка с който е поискана подкрепата. Исканията за подкрепа от резерва за киберсигурност на ЕС следва да включват необходимата относима информация за инцидента и вече предприетите от ползвателите мерки. В тази глава са описани и условията за изпълнение, включително оценката на исканията до резерва за киберсигурност на ЕС.

В регламента се предвиждат и принципите за обществените поръчки и критериите за подбор по отношение на доверителните доставчици на резерва за киберсигурност на ЕС.

Трети държави могат да поискат подкрепа от резерва за киберсигурност на ЕС, когато това е предвидено в споразуменията за асоцииране, сключени във връзка с участието им в програмата „Цифрова Европа“. В тази глава са описани допълнителните условия и ред за това участие.

Механизъм за преглед на киберинциденти (глава IV)

По искане на Комисията, EU-CyCLONe или мрежата на ЕРИКС ENISA следва да направи преглед и оценка на заплахите, уязвимостите и действията за смекчаване на последиците по отношение на конкретен значителен или мащабен киберинцидент. Прегледът и оценката следва да бъдат предоставени от ENISA под формата на доклад за преглед на инцидента на мрежата на ЕРИКС, EU-CyCLONe и Комисията, за да бъдат подпомогнати при изпълнението на техните задачи. Когато инцидентът се отнася до трета държава, Комисията следва да сподели доклада с върховния представител. Докладът следва да включва извлечените поуки и, когато е целесъобразно, препоръки за подобряване на състоянието на киберсигурността на Съюза.

Заключителни разпоредби (глава V)

Глава V съдържа изменения на регламента за програмата „Цифрова Европа“ и задължението на Комисията да изготвя редовни доклади за оценка и преглед на регламента до Европейския парламент и до Съвета. На Комисията се предоставя правомощието да приема актове за изпълнение в съответствие с процедурата по разглеждане, посочена в член 21 за: определяне на условията за тази оперативна съвместимост между трансграничните ЦОС; определяне на процедурните правила за обмен на информация, свързана с потенциален или текущ мащабен киберинцидент, между трансграничните ЦОС и субектите на Съюза; определяне на технически изисквания за осигуряване на високо ниво на сигурност на данните и физическа сигурност на инфраструктурата и за защита на интересите на Съюза, свързани със сигурността, при обмен на информация със субекти, които не са публични органи на държавите членки; определяне на видовете и броя на услугите за реагиране, необходими за резерва за киберсигурност на ЕС; и допълнително уточняване на подробните договорености за разпределяне на услугите за подкрепа от резерва за киберсигурност на ЕС.

2023/0109 (COD)

Предложение 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

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз, и по-специално член 173, параграф 3 и член 322, параграф 1, буква а) от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Сметната палата[1],

като взеха предвид становището на Европейския икономически и социален комитет[2],

като взеха предвид становището на Комитета на регионите[3],

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

(1) Всички сектори на икономиката използват и се осланят на информационните и комуникационните технологии като съществен компонент на дейността си, тъй като нашите публични администрации, предприятия и граждани са повече от всякога тясно свързани и взаимозависими отвъд секторните и териториалните граници.

(2) Мащабът, честотата и въздействието на киберинцидентите се увеличават, включително атаките по веригата на доставки, целящи кибершпионаж, софтуер за изнудване или смущения. Те представляват съществена заплаха за функционирането на мрежовите и информационните системи. С оглед на бързо променящата се картина на заплахите, заплахата от възможни мащабни инциденти, причиняващи значителни смущения или вреди на критичните инфраструктури, изисква повишена готовност на всички нива на рамката за киберсигурност на Съюза. Тази заплаха надхвърля рамките на военната агресия на Русия в Украйна и е вероятно да продължи да съществува, като се има предвид многообразието от свързани с държави участници, престъпни

[1] ОВ С […], […] г., стр. […].
[2] ОВ С , , стр. .
[3] ОВ С , , стр. .

участници и хактивисти, замесени в настоящото геополитическо напрежение. Такива инциденти могат да възпрепятстват предоставянето на обществени услуги и осъществяването на икономически дейности, включително в критични или висококритични сектори, 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. Освен това киберинцидентите са непредвидими, тъй като често възникват и се развиват за много кратък период от време, не се ограничават в рамките на определен географски район и се случват едновременно или се разпространяват мигновено в много държави.

(3) Необходимо е да се укрепи конкурентната позиция на промишлеността и сектора на услугите в Съюза в рамките на цифровизираната икономика, както и да се подкрепи тяхната цифрова трансформация, като се повиши нивото на киберсигурност на цифровия единен пазар. Както се препоръчва в три различни предложения на Конференцията за бъдещето на Европа[4], необходимо е да се повиши устойчивостта на гражданите, предприятията и субектите, извършващи дейност в критични инфраструктури, срещу нарастващите киберзаплахи, които могат да имат опустошителни последици за обществото и икономиката. Ето защо са необходими инвестиции в инфраструктури и услуги, които ще подпомогнат по-бързото откриване и реагиране при киберзаплахи и инциденти, а държавите членки се нуждаят от помощ, за да се подготвят, както и да реагират по-добре в случай на значителни и мащабни киберинциденти. Съюзът следва също така да увеличи способностите си в тези области, особено по отношение на събирането и анализирането на данни за киберзаплахите и инцидентите.

(4) Съюзът вече е предприел редица мерки за намаляване на уязвимостта и повишаване на устойчивостта на критичните инфраструктури и субектите срещу киберрисковете, по-специално Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета[5], Препоръка (ЕС) 2017/1584 на Комисията[6], Директива 2013/40/ЕС на Европейския парламент и на Съвета[7] и Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета[8]. В допълнение в препоръката на Съвета относно координиран подход на равнището на Съюза за укрепване на устойчивостта на инфраструктурата от критично значение държавите членки се приканват да предприемат спешни и ефективни мерки и да си сътрудничат лоялно, ефикасно, солидарно и координирано помежду си, с Комисията и с други съответни публични органи, както и със съответните

4 https://futureu.europa.eu/bg/

5 Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (ОВ L 333, 27.12.2022 г.).

6 Препоръка (ЕС) 2017/1584 на Комисията от 13 септември 2017 г. относно координирана реакция на мащабни киберинциденти и кризи (ОВ L 239, 19.9.2017 г., стр. 36).

7 Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета (ОВ L 218, 14.8.2013 г., стр. 8.).

8 Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019 г., стр. 15).

субекти, за да повишат устойчивостта на инфраструктурата от критично значение, използвана за предоставяне на основни услуги на вътрешния пазар.

(5) Нарастващите киберрискове и цялостната сложна картина на заплахите, с ясен риск от бързо разпространение на киберинциденти от една държава членка към други държави членки и от трета държава към Съюза, изискват засилена солидарност на равнището на Съюза за по-добро откриване, подготовка и реагиране при киберзаплахи и инциденти. В заключенията на Съвета относно установяването на позицията на Европейския съюз в киберпространството[9] държавите членки също приканиха Комисията да представи предложение за нов фонд за реагиране при извънредни ситуации в областта на киберсигурността.

(6) В съвместното съобщение „Политика на ЕС за киберотбрана“[10], прието на 10 ноември 2022 г., беше обявена инициатива на ЕС за киберсолидарност със следните цели: укрепване на общите способности на ЕС за откриване, ситуационна осведоменост и реагиране чрез насърчаване на разгръщането на инфраструктура на ЕС от центрове за операции по сигурността (ЦОС), подпомагане на постепенното изграждане на резерв за киберсигурност на равнището на ЕС от услуги от доверителни частни доставчици и изпитване на критични субекти за потенциални уязвимости въз основа на оценки на риска на ЕС.

(7) Необходимо е да се подобрят откриването и ситуационната осведоменост по отношение на киберзаплахите и инцидентите в целия Съюз, както и да се укрепи солидарността чрез повишаване на готовността и способностите на държавите членки и на Съюза за реагиране при значителни и мащабни киберинциденти. Поради това следва да бъде разгърната общоевропейска инфраструктура от ЦОС (европейски киберщит) за изграждане и подобряване на общите способности за откриване и ситуационна осведоменост; следва да бъде създаден Механизъм за действие при извънредни ситуации в областта на киберсигурността, който да подпомага държавите членки при подготовката, реагирането и незабавното възстановяване след значителни и мащабни киберинциденти; следва да бъде създаден европейски Механизъм за преглед на киберинциденти, чрез който да се разглеждат и оценяват конкретни значителни или мащабни киберинциденти. Тези действия не засягат членове 107 и 108 от Договора за функционирането на Европейския съюз („ДФЕС“).

(8) За постигането на тези цели е необходимо също така да се измени Регламент (ЕС) 2021/694 на Европейския парламент и на Съвета[11] в някои области. По-специално с настоящия регламент следва да се измени Регламент (ЕС) 2021/694 по отношение на добавянето на нови оперативни цели, свързани с европейския киберщит и Механизма за действие при извънредни ситуации в областта на киберсигурността в рамките на специфична цел 3 на

---

9 Заключения на Съвета относно установяването на позицията на Европейския съюз в киберпространството, одобрени от Съвета на заседанието му от 23 май 2022 г. (9364/22).

10 Съвместно съобщение до Европейския парламент и Съвета „Политика на ЕС за киберотбрана“, JOIN/2022/49 final.

11 Регламент (ЕС) 2021/694 на Европейския парламент и на Съвета от 29 април 2021 г. за създаване на програмата „Цифрова Европа“ и за отмяна на Решение (ЕС) 2015/2240 (ОВ L 166, 11.5.2021 г., стр. 1).

програмата „Цифрова Европа“, която е насочена към гарантиране на устойчивостта, целостта и надеждността на цифровия единен пазар, към укрепване на способностите за наблюдение и реагиране на кибератаките и заплахите, както и към засилване на трансграничното сътрудничество в областта на киберсигурността. Това ще бъде допълнено от конкретните условия, при които може да бъде отпусната финансова подкрепа за тези действия, и следва да бъдат определени механизмите за управление и координация, необходими за постигане на планираните цели. Други изменения на Регламент (ЕС) 2021/694 следва да включват описания на предложените действия в рамките на новите оперативни цели, както и измерими показатели за наблюдение на изпълнението на новите оперативни цели.

(9) Финансирането на действията, посочени в настоящия регламент, следва да бъде предвидено в Регламент (ЕС) 2021/694, който следва да остане съответният основен законодателен акт за тези действия, заложени в специфична цел 3 на програмата „Цифрова Европа“. Конкретните условия за участие по отношение на всяко действие ще бъдат предвидени в съответните работни програми съгласно приложимата разпоредба на Регламент (ЕС) 2021/694.

(10) Към настоящия регламент се прилагат хоризонталните финансови правила, приети от Европейския парламент и Съвета на основание член 322 от ДФЕС. Тези правила са установени във Финансовия регламент и определят по-специално процедурата за съставяне и изпълнение на бюджета на Съюза, както и предвиждат проверки на отговорността на финансовите участници. Правилата, приети на основание член 322 от ДФЕС, включват и общ режим на обвързаност с условия за защита на бюджета на Съюза, установен в Регламент (ЕС, Евратом) 2020/2092 на Европейския парламент и на Съвета.

(11) За целите на доброто финансово управление следва да се определят специални правила за пренасяне на неизползваните бюджетни кредити за поети задължения и за плащания. При спазване на принципа, че бюджетът на Съюза се определя ежегодно, в настоящия регламент следва, предвид непредвидимия, извънреден и специфичен характер на положението в областта на киберсигурността, да се предвидят възможности за пренасяне на неизползвани средства извън определените във Финансовия регламент, като по този начин се увеличи максимално капацитетът на Механизма за действие при извънредни ситуации в областта на киберсигурността за подпомагане на държавите членки в ефективното противодействие на киберзаплахите.

(12) С оглед на по-ефективната превенция, оценяване и реагиране на киберзаплахите и инцидентите, е необходимо да се развият по-всеобхватни познания за заплахите за критичните активи и инфраструктури на територията на Съюза, включително тяхното географско разпределение, взаимосвързаност и потенциални последици в случай на кибератаки, засягащи тези инфраструктури. Следва да бъде разгърната широкомащабна инфраструктура на Съюза от ЦОС („европейски киберщит“), състояща се от няколко оперативно съвместими трансгранични платформи, всяка от които обединява няколко национални ЦОС. Тази инфраструктура следва да обслужва националните интереси и нуждите на Съюза в областта на киберсигурността, като използва най-съвременни технологии за авангардно събиране на данни и инструменти за анализ, подобрява способностите за откриване и управление на кибератаки и

осигурява ситуационна осведоменост в реално време. Тази инфраструктура следва да служи за по-добро откриване на киберзаплахи и инциденти и по този начин да допълва и подпомага субектите и мрежите на Съюза, отговарящи за управлението на кризи в Съюза, по-специално мрежата за връзка на организациите при кибернетични кризи („EU-CyCLONe“), както е определена в Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета[12].

(13) Всяка държава членка следва да определи публичен орган на национално равнище, натоварен със задачата да координира дейностите по откриване на киберзаплахи в тази държава членка. Тези национални ЦОС следва да действат като отправна точка и портал на национално равнище за участие в европейския киберщит и следва да гарантират, че информацията за киберзаплахите от публични и частни субекти се споделя и събира на национално равнище по ефективен и рационализиран начин.

(14) Като част от европейския киберщит следва да бъдат създадени редица трансгранични центрове за операции по сигурността („трансгранични ЦОС“). Те следва да обединяват национални ЦОС от поне три държави членки, за да могат да се постигнат всички ползи от трансграничното откриване на заплахи и от обмена и управлението на информация. Общата цел на трансграничните ЦОС следва да бъде укрепване на способностите за анализ, превенция и откриване на киберзаплахи и подпомагане на изготвянето на висококачествена разузнавателна информация за киберзаплахите, по-специално чрез обмен на данни от различни източници, публични или частни, както и чрез споделяне и съвместно използване на най-съвременни инструменти и съвместно развитие на способности за откриване, анализ и превенция в доверителна среда. Те следва да осигурят нов допълнителен капацитет, който да надгражда и допълва съществуващите ЦОС и екипите за реагиране при инциденти с компютърната сигурност („ЕРИКС“), както и други съответни участници.

(15) На национално равнище наблюдението, откриването и анализът на киберзаплахите обикновено се осигуряват от ЦОС от публични и частни субекти в комбинация с ЕРИКС. Освен това ЕРИКС обменят информация в контекста на мрежата на ЕРИКС в съответствие с Директива (ЕС) 2022/2555. Трансграничните ЦОС следва да представляват нов капацитет, който допълва мрежата на ЕРИКС, като обединяват и обменят данни за киберзаплахите от публични и частни субекти, повишават стойността на тези данни чрез експертен анализ и съвместно придобити инфраструктури и най-съвременни инструменти и допринасят за развитието на способностите и технологичния суверенитет на Съюза.

(16) Трансграничните ЦОС следва да действат като централно звено, позволяващо широко обединяване на относимите данни и разузнавателната информация за киберзаплахите, да дават възможност за разпространение на информация за заплахите сред голям и разнообразен набор от участници (напр. екипи за незабавно реагиране при компютърни инциденти („CERT“), ЕРИКС, центрове за

[12] Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2) (ОВ L 333, 27.12.2022 г., стр. 80).

обмен на информация и анализ („ISAC“), оператори на критични инфраструктури). Информацията, която се обменя между участниците в трансграничен ЦОС, може да включва данни от мрежи и сензори, разузнавателни сведения за заплахи, показатели за компрометиране на системите и контекстуална информация за инциденти, заплахи и уязвимости. Освен това трансграничните ЦОС следва да сключват и споразумения за сътрудничество с други трансгранични ЦОС.

(17) Споделената ситуационна осведоменост между съответните органи е необходима предпоставка за готовността и координацията в целия Съюз по отношение на значителни и мащабни киберинциденти. С Директива (ЕС) 2022/2555 се създава EU-CyCLONe с цел подпомагане на координираното управление на мащабни киберинциденти и кризи на оперативно равнище и осигуряване на редовния обмен на относимата информация сред държавите членки и институциите, органите, службите и агенциите на Съюза. В Препоръка (ЕС) 2017/1584 относно координирана реакция на мащабни киберинциденти и кризи се разглежда ролята на всички съответни участници. В Директива (ЕС) 2022/2555 се припомнят и отговорностите на Комисията в рамките на Механизма за гражданска защита на Съюза („МГЗС“), създаден с Решение 1313/2013/ЕС на Европейския парламент и на Съвета, както и тези за предоставянето на аналитични доклади за механизма за интегрирана реакция при политическа криза („ИРПК“) съгласно Решение за изпълнение (ЕС) 2018/1993. Следователно в ситуации, когато трансграничните ЦОС получат информация, свързана с потенциален или текущ мащабен киберинцидент, те следва да предоставят относимата информация на EU-CyCLONe, мрежата на ЕРИКС и Комисията. По-специално в зависимост от ситуацията, информацията, която трябва да бъде споделена, може да включва техническа информация, информация за естеството и мотивите на нападателя или потенциалния нападател, както и нетехническа информация от по-високо ниво за потенциален или текущ мащабен киберинцидент. В този контекст следва да се обърне надлежно внимание на принципа „необходимост да се знае“ и на потенциално чувствителния характер на споделяната информация.

(18) Субектите, участващи в европейския киберщит, следва да осигурят високо ниво на оперативна съвместимост помежду си, включително, по целесъобразност, по отношение на форматите на данните, таксономията, инструментите за обработка и анализ на данни и сигурните комуникационни канали, минимално ниво на сигурност на приложния слой, информационно табло за ситуационната осведоменост и показатели. Приемането на обща таксономия и разработването на образец за доклади за ситуацията с цел описване на техническите причини и въздействия на киберинцидентите следва да отчита текущата работа по уведомяването за инциденти в контекста на прилагането на Директива (ЕС) 2022/2555.

(19) За да се даде възможност за широкомащабен обмен на данни за киберзаплахите от различни източници в доверителна среда, субектите, участващи в европейския киберщит, следва да разполагат с най-съвременни инструменти, оборудване и инфраструктури с високо ниво на сигурност. Това следва да даде възможност за подобряване на колективните способности за откриване и за своевременно предупреждение на органите и съответните субекти, по-специално

чрез използване на най-новите технологии за изкуствен интелект и анализ на данни.

(20) Чрез събирането, споделянето и обмена на данни европейският киберщит следва да повиши технологичния суверенитет на Съюза. Обединяването на висококачествени подбрани данни следва да допринесе и за разработването на авангардни технологии за изкуствен интелект и анализ на данни. Това следва да бъде улеснено чрез свързването на европейския киберщит с общоевропейската инфраструктура за високопроизводителни изчислителни технологии, създадена с Регламент (ЕС) 2021/1173[13] на Съвета.

(21) Въпреки че европейският киберщит е граждански проект, общността за киберотбрана би могла да се възползва от по-силните граждански способности за откриване и ситуационна осведоменост, разработени за защита на критичната инфраструктура. Трансграничните ЦОС, с подкрепата на Комисията и Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността („ЕССС“) и в сътрудничество с върховния представител на Съюза по въпросите на външните работи и политиката на сигурност („върховния представител“), следва постепенно да разработят специални протоколи и стандарти, които да позволят сътрудничество с общността за киберотбрана, включително проверка и условия за сигурност. Разработването на европейския киберщит следва да бъде придружено от обмисляне, позволяващо бъдещо сътрудничество с мрежите и платформите, отговарящи за обмена на информация в общността за киберотбрана, в тясно сътрудничество с върховния представител.

(22) Обменът на информация между участниците в европейския киберщит следва да бъде в съответствие със съществуващите правни изисквания, и по-специално със законодателството на Съюза и националното законодателство за защита на данните, както и с правилата за конкуренция на ЕС, уреждащи обмена на информация. Получателят на информацията следва да приложи, доколкото е необходимо обработването на лични данни, технически и организационни мерки, които гарантират правата и свободите на субектите на данни, и да унищожи данните веднага щом те вече не са необходими за посочената цел, и да информира органа, който предоставя данните, че данните са унищожени.

(23) Без да се засяга член 346 от ДФЕС, обменът на информация, която е поверителна съгласно правилата на Съюза или националните правила, следва да бъде ограничен до информацията, която има значение за целите на този обмен и която е пропорционална на тези цели. Обменът на такава информация следва да се извършва при зачитане на нейната поверителност и на сигурността и търговските интереси на засегнатите субекти при пълно спазване на търговските и фирмените тайни.

(24) С оглед на нарастващите рискове и броя на киберинцидентите, които засягат държавите членки, е необходимо да се създаде инструмент за подкрепа при кризи, за да се подобри устойчивостта на Съюза на значителни и мащабни

[13] Регламент (ЕС) 2021/1173 на Съвета от 13 юли 2021 г. за създаване на Съвместно предприятие за европейски високопроизводителни изчислителни технологии и за отмяна на Регламент (ЕС) 2018/1488, (ОВ L 256, 19.7.2021 г., стр. 3).

киберинциденти и да се допълнят действията на държавите членки чрез спешна финансова подкрепа за готовност, реагиране и незабавно възстановяване на основни услуги. Този инструмент следва да дава възможност за бързо използване на помощта при определени обстоятелства и при ясни условия, както и да позволява внимателно наблюдение и оценка на използването на ресурсите. Въпреки че държавите членки носят основната отговорност за превенцията, готовността и реагирането при киберинциденти и кризи, Механизмът за действие при извънредни ситуации в областта на киберсигурността насърчава солидарността между държавите членки в съответствие с член 3, параграф 3 от Договора за Европейския съюз (ДЕС).

(25) Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да предоставя подкрепа на държавите членки в допълнение към техните собствени мерки и ресурси, както и към други съществуващи възможности за подкрепа в случай на реагиране и незабавно възстановяване след значителни и мащабни киберинциденти, като например услугите, предоставяни от Агенцията на Европейския съюз за киберсигурност („ENISA“) в съответствие с нейния мандат, координираното реагиране и помощта от мрежата на ЕРИКС, подкрепата за смекчаване на последиците от EU-CyCLONe, както и взаимната помощ между държавите членки, включително в контекста на член 42, параграф 7 от ДЕС, екипите за бързо реагиране в областта на киберсигурността на ПСС[14] и хибридните екипи за бързо реагиране. Следва да се разгледа необходимостта да се гарантира наличието на специализирани средства за подпомагане на готовността и реагирането при киберинциденти в целия Съюз и в трети държави.

(26) Настоящият инструмент не засяга процедурите и рамките за координиране на реагирането при кризи на равнището на Съюза, по-специално МГЗС[15], ИРПК[16], и Директива (ЕС) 2022/2555. Той може да подкрепи или да допълни действията, осъществявани в контекста на член 42, параграф 7 от ДЕС или в ситуации, определени в член 222 от ДФЕС. Използването на този инструмент следва също така да бъде координирано с прилагането на мерките от инструментариума за кибердипломация, когато това е уместно.

(27) Помощта, предоставяна съгласно настоящия регламент, следва да подкрепя и допълва действията, предприети от държавите членки на национално равнище. За тази цел следва да се осигури тясно сътрудничество и консултации между Комисията и засегнатата държава членка. При подаване на искане за подкрепа в рамките на Механизма за действие при извънредни ситуации в областта на киберсигурността държавата членка следва да предостави относима информация, обосноваваща необходимостта от подкрепа.

---

14 Решение (ОВППС) 2017/2315 на Съвета от 11 декември 2017 г. за установяване на постоянно структурирано сътрудничество (ПСС) и определяне на списъка на участващите държави членки.

15 Решение № 1313/2013/ЕС на Европейския парламент и на Съвета от 17 декември 2013 г. относно Механизъм за гражданска защита на Съюза (ОВ L 347, 20.12.2013 г., стр. 924).

16 Договорености за интегрирана реакция на ЕС при политическа криза (ИРПК) и в съответствие с Препоръка (ЕС) 2017/1584 на Комисията от 13 септември 2017 г. относно координирана реакция на мащабни киберинциденти и кризи.

(28) Директива (ЕС) 2022/2555 изисква от държавите членки да определят или създадат един или повече органи за управление на киберкризи и да гарантират, че те разполагат с достатъчно ресурси за изпълнение на възложените им задачи по ефективен и ефикасен начин. В нея също така се изисква държавите членки да определят способностите, активите и процедурите, които могат да бъдат използвани в случай на криза, както и да приемат национален план за реагиране при мащабни киберинциденти и кризи, в който се определят целите и условията и редът за управлението на мащабни киберинциденти и кризи. От държавите членки се изисква също така да създадат един или повече ЕРИКС, натоварени с отговорности за действия при инцидент в съответствие с добре определен процес и обхващащи най-малко секторите, подсекторите и видовете субекти, попадащи в обхвата на посочената директива, както и да гарантират, че те разполагат с достатъчно ресурси за ефективно изпълнение на възложените им задачи. Настоящият регламент не засяга ролята на Комисията за осигуряване на спазването от страна на държавите членки на задълженията по Директива (ЕС) 2022/2555. Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да предоставя помощ за действия, насочени към укрепване на готовността, както и за действия в отговор на инциденти с цел смекчаване на въздействието на значителни и мащабни киберинциденти, подпомагане на незабавното възстановяване и/или възстановяване на функционирането на основните услуги.

(29) Като част от действията за готовност, за да се насърчи последователен подход и да се укрепи сигурността в целия Съюз и неговия вътрешен пазар, следва да се предостави подкрепа за координирано изпитване и оценка на киберсигурността на субектите, извършващи дейност във висококритични сектори, определени съгласно Директива (ЕС) 2022/2555. За тази цел Комисията, с подкрепата на ENISA и в сътрудничество с групата за сътрудничество за МИС, създадена с Директива (ЕС) 2022/2555, следва редовно да определя съответните сектори или подсектори, които следва да отговарят на условията за получаване на финансова подкрепа за координирани изпитвания на равнището на Съюза. Секторите или подсекторите следва да бъдат избрани от приложение I към Директива (ЕС) 2022/2555 („Сектори с висока степен на критичност“). Координираните изпитвания следва да се основават на общи сценарии на риска и методологии. При подбора на секторите и разработването на сценариите на риска следва да се вземат предвид съответните оценки на риска и сценарии на риска за целия Съюз, включително необходимостта от избягване на дублиране, като например оценката на риска и сценариите на риска, за които се призовава в заключенията на Съвета относно установяването на позицията на Европейския съюз в киберпространството и които трябва да бъдат извършени от Комисията, върховния представител и групата за сътрудничество за МИС, в координация със съответните граждански и военни органи и агенции и установените мрежи, включително EU-CyCLONe, както и оценката на риска на комуникационните мрежи и инфраструктури, поискана от съвместния призив на министрите от Невер и извършена от групата за сътрудничество за МИС, с подкрепата на Комисията и ENISA и в сътрудничество с Органа на европейските регулатори в областта на електронните съобщения (ОЕРЕС), координираните оценки на риска, които ще бъдат извършени съгласно член 22 от Директива (ЕС) 2022/2555, и изпитването на оперативната устойчивост на

цифровите технологии, както е предвидено в Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета[17]. При подбора на секторите следва да се вземе предвид и препоръката на Съвета относно координиран подход на равнището на Съюза за укрепване на устойчивостта на инфраструктурата от критично значение.

(30) Освен това Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да предлага подкрепа за други действия за готовност и да подпомага готовността в други сектори, които не са обхванати от координираното изпитване на субектите, извършващи дейност във висококритични сектори. Тези действия може да включват различни видове дейности за готовност на национално равнище.

(31) Механизмът за действие при извънредни ситуации в областта на киберсигурността следва също така да предоставя подкрепа за действия в отговор на инциденти с цел смекчаване на въздействието на значителни и мащабни киберинциденти, подпомагане на незабавното възстановяване или възстановяване на функционирането на основните услуги. Когато е целесъобразно, той следва да допълва МГЗС, за да се осигури всеобхватен подход за реагиране на последиците от киберинцидентите върху гражданите.

(32) Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да подкрепя помощта, предоставяна от държавите членки на дадена държава членка, засегната от значителен или мащабен киберинцидент, включително от мрежата на ЕРИКС, посочена в член 15 от Директива (ЕС) 2022/2555. На държавите членки, които предоставят помощ, следва да бъде разрешено да подават искания за покриване на разходите, свързани с изпращането на експертни екипи в рамките на взаимопомощта. Допустимите разходи може да включват пътни разходи, разходи за настаняване и дневни надбавки на експертите по киберсигурност.

(33) Постепенно следва да бъде създаден резерв за киберсигурност на равнището на Съюза, състоящ се от услуги на частни доставчици на управлявани услуги за сигурност, който да подпомага действията за реагиране и незабавно възстановяване в случаи на значителни или мащабни киберинциденти. Резервът за киберсигурност на ЕС следва да гарантира наличността и готовността на услугите. Услугите от резерва за киберсигурност на ЕС следва да подпомагат националните органи при предоставянето на помощ на засегнатите субекти, извършващи дейност в критични или висококритични сектори, като допълнение към собствените им действия на национално равнище. Когато искат подкрепа от резерва за киберсигурност на ЕС, държавите членки следва да посочат подкрепата, предоставена на засегнатия субект на национално равнище, която следва да бъде взета предвид при оценката на искането на държавата членка. Услугите от резерва за киберсигурност на ЕС могат да служат и за подкрепа на институциите, органите, службите и агенциите на ЕС при сходни условия.

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

(34) За целите на подбора на частни доставчици на услуги, които да предоставят услуги в контекста на резерва за киберсигурност на ЕС, е необходимо да се установи набор от минимални критерии, които следва да бъдат включени в поканата за участие в търг за подбор на тези доставчици, за да се гарантира, че са удовлетворени нуждите на органите и субектите на държавите членки, извършващи дейност в критични или висококритични сектори.

(35) За да подкрепи създаването на резерва за киберсигурност на ЕС, Комисията би могла да обмисли възможността да поиска от ENISA да изготви схема за сертифициране на кандидати съгласно Регламент (ЕС) 2019/881 за управлявани услуги за сигурност в областите, обхванати от Механизма за действие при извънредни ситуации в областта на киберсигурността.

(36) За да се подкрепят целите на настоящия регламент за насърчаване на споделената ситуационна осведоменост, повишаване на устойчивостта на Съюза и осигуряване на ефективно реагиране на значителни и мащабни киберинциденти, EU-CyCLONe, мрежата на ЕРИКС или Комисията следва да могат да поискат от ENISA да направи преглед и оценка на заплахите, уязвимостите и действията за смекчаване на последиците по отношение на конкретен значителен или мащабен киберинцидент. След приключване на прегледа и оценката на даден инцидент ENISA следва да изготви доклад за преглед на инцидента в сътрудничество със съответните заинтересовани страни, включително представители на частния сектор, държавите членки, Комисията и други съответни институции, органи, служби и агенции на ЕС. Що се отнася до частния сектор, ENISA разработва канали за обмен на информация със специализирани доставчици, включително доставчици на управлявани решения за сигурност и потенциални оференти, за да допринесе за мисията на ENISA за постигане на високо общо ниво на киберсигурност в целия Съюз. Въз основа на сътрудничеството със заинтересованите страни, включително частния сектор, докладът за преглед на конкретни инциденти следва да има за цел да оцени причините, въздействията и мерките за смекчаване от даден инцидент след неговото възникване. Особено внимание следва да се обърне на приноса и изводите, споделени от доставчиците на управлявани услуги за сигурност, които отговарят на условията за най-висока професионална почтеност, безпристрастност и необходим технически опит, както се изисква в настоящия регламент. Докладът следва да бъде представен и използван в работата на EU-CyCLONe, мрежата на ЕРИКС и Комисията. Когато инцидентът се отнася до трета държава, Комисията споделя доклада също с върховния представител.

(37) Като се има предвид непредвидимият характер на атаките срещу киберсигурността и фактът, че те често не се ограничават в определен географски район и пораждат висок риск от разпространение, укрепването на устойчивостта на съседните държави и способностите им да реагират ефективно на значителни и мащабни киберинциденти допринася за защитата на Съюза като цяло. Поради това трети държави, асоциирани към програмата „Цифрова Европа“, могат да бъдат подпомагани от резерва за киберсигурност на ЕС, когато това е предвидено в съответното споразумение за асоцииране към програмата „Цифрова Европа“. Финансирането на асоциираните трети държави следва да се подпомага от Съюза в рамките на съответните партньорства и инструменти за финансиране за тези държави. Подкрепата следва да обхваща услуги в областта на реагирането и незабавното възстановяване след значителни

или мащабни киберинциденти. Условията, определени за резерва за киберсигурност на ЕС и доверителните доставчици в настоящия регламент, следва да се прилагат при предоставянето на подкрепа на трети държави, асоциирани към програмата „Цифрова Европа“.

(38) За да се осигурят еднакви условия за прилагането на настоящия регламент, на Комисията следва да се предоставят изпълнителни правомощия за определяне на условията за оперативна съвместимост между трансграничните ЦОС; определяне на процедурните правила за обмен на информация, свързана с потенциален или текущ мащабен киберинцидент, между трансграничните ЦОС и субектите на Съюза; определяне на технически изисквания за гарантиране на сигурността на европейския киберщит; определяне на видовете и броя на услугите за реагиране, необходими за резерва за киберсигурност на ЕС; и допълнително уточняване на подробните договорености за разпределяне на услугите за подкрепа от резерва за киберсигурност на ЕС. Тези правомощия следва да бъдат упражнявани в съответствие с Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета.

(39) Целта на настоящия регламент може да бъде постигната по-добре на равнището на Съюза, отколкото от държавите членки. Поради това Съюзът може да приеме мерки в съответствие с принципите на субсидиарност и пропорционалност, уредени в член 5 от Договора за Европейския съюз. Настоящият регламент не надхвърля необходимото за постигането на тази цел,

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

Глава I

ОБЩИ ЦЕЛИ, ПРЕДМЕТ И ОПРЕДЕЛЕНИЯ

Член 1

Предмет и цели

1. С настоящия регламент се установяват мерки за укрепване на способностите на Съюза за откриване, подготовка и реагиране на киберзаплахи и инциденти, по-специално чрез следните действия:

а) разгръщане на общоевропейска инфраструктура от центрове за операции по сигурността („европейски киберщит“) за изграждане и подобряване на общите способности за откриване и ситуационна осведоменост;

б) създаване на Механизъм за действие при извънредни ситуации в областта на киберсигурността, който да подпомага държавите членки при подготовката,

реагирането и незабавното възстановяване след значителни и мащабни киберинциденти;

в) създаване на европейски Механизъм за преглед на киберинциденти, който да разглежда и оценява значителни или мащабни киберинциденти.

2. Настоящият регламент преследва целта за укрепване на солидарността на равнището на Съюза чрез следните специфични цели:

а) засилване на общото за Съюза откриване на киберзаплахи и инциденти и ситуационна осведоменост, като по този начин се дава възможност за укрепване на конкурентната позиция на промишлеността и сектора на услугите в Съюза в цифровата икономика и се допринася за технологичния суверенитет на Съюза в областта на киберсигурността;

б) повишаване на готовността на субектите, извършващи дейност в критични и висококритични сектори в целия Съюз, и укрепване на солидарността чрез изграждане на общи способности за реагиране при значителни или мащабни киберинциденти, включително чрез предоставяне на подкрепа от Съюза за реагиране при киберинциденти на трети държави, асоциирани към програмата „Цифрова Европа“;

в) повишаване на устойчивостта на Съюза и допринасяне за ефективно реагиране чрез преглед и оценка на значителни или мащабни киберинциденти, включително извличане на поуки и, когато е уместно, препоръки.

3. Настоящият регламент не засяга основната отговорност на държавите членки за националната сигурност, обществената сигурност, както и за превенцията, разследването, разкриването и наказателното преследване на престъпления.

Член 2

Определения

За целите на настоящия регламент се прилагат следните определения:

(1) **„трансграничен център за операции по сигурността“ („трансграничен ЦОС“)** означава многонационална платформа, която обединява в координирана мрежова структура национални ЦОС от най-малко три държави членки, които образуват консорциум, осигуряващ хостинг, който е предназначен да предотвратява киберзаплахи и инциденти и да подпомага изготвянето на висококачествена разузнавателна информация, по-специално чрез обмен на данни от различни източници, публични и частни, както и чрез споделяне на най-съвременни инструменти и съвместно развиване на способности за откриване на киберинциденти, анализ, превенция и защита в доверителна среда**;**

(2) **„публичен орган“** означава публичноправна организация съгласно определението в член 2, параграф 1, точка 4 от Директива 2014/24/ЕС на Европейския парламент и на Съвета[18];

(3) **„консорциум, осигуряващ хостинг“** означава консорциум, съставен от участващи държави, представлявани от национални ЦОС, които са се споразумели да създадат и допринесат за придобиването на инструменти и инфраструктура за трансграничен ЦОС и за неговото функциониране;

(4) **„субект“** означава субект съгласно определението в член 6, точка 38 от Директива (ЕС) 2022/2555*;*

(5) **„субекти, извършващи дейност в критични или висококритични сектори“** означава видовете субекти, изброени в приложения I и II към Директива (ЕС) 2022/2555;

(6) **„киберзаплаха“** означава киберзаплаха съгласно определението в член 2, точка 8 от Регламент (ЕС) 2019/881;

(7) **„значителен киберинцидент“** означава киберинцидент, който отговаря на критериите, посочени в член 23, параграф 3 от Директива (ЕС) 2022/2555;

(8) **„мащабен киберинцидент“** означава инцидент съгласно определението в член 6, точка 7 от Директива (ЕС) 2022/2555;

(9) **„готовност“** означава състояние на готовност и способност за ефективно бързо реагиране на значителен или мащабен киберинцидент, постигнато в резултат на предварително предприети действия за оценка на риска и наблюдение;

(10) **„реагиране“** означава действие в случай на значителен или мащабен киберинцидент, или по време на или след такъв инцидент, с цел справяне с неговите незабавни и краткосрочни неблагоприятни последици;

(11) **„доверителни доставчици“** означава доставчици на управлявани услуги за сигурност съгласно определението в член 6, точка 40 от Директива (ЕС) 2022/2555, избрани в съответствие с член 16 от настоящия регламент.

[18] Директива 2014/24/ЕС на Европейския парламент и на Съвета от 26 февруари 2014 г. за обществените поръчки и за отмяна на Директива 2004/18/ЕО (ОВ L 94 28.3.2014 г., стр. 65).

Глава II

ЕВРОПЕЙСКИ КИБЕРЩИТ

Член 3

Създаване на европейски киберщит

1. Създава се взаимосвързана общоевропейска инфраструктура от центрове за операции по сигурността („европейски киберщит“), с цел да се развият авангардни способности на Съюза за откриване, анализиране и обработване на данни за киберзаплахи и инциденти в Съюза. Щитът се състои от всички национални центрове за операции по сигурността („национални ЦОС“) и трансгранични центрове за операции по сигурността („трансгранични ЦОС“).

Действията за прилагане на европейския киберщит се подкрепят с финансиране от програмата „Цифрова Европа“ и се изпълняват в съответствие с Регламент (ЕС) 2021/694, и по-специално със специфична цел 3 от него.

2. Европейският киберщит:

а) обединява и обменя данни за киберзаплахи и инциденти от различни източници чрез трансграничните ЦОС;

б) изготвя висококачествена, приложима информация и разузнавателни сведения за киберзаплахите чрез използване на най-съвременни инструменти, по-специално технологии за изкуствен интелект и анализ на данни;

в) допринася за по-добра защита и реагиране на киберзаплахите;

г) допринася за по-бързото откриване на киберзаплахи и за ситуационната осведоменост в целия Съюз;

д) предоставя услуги и дейности за киберобщността в Съюза, включително допринася за разработването на авангардни инструменти за изкуствен интелект и анализ на данни.

Той се разработва в сътрудничество с общоевропейската инфраструктура за високопроизводителни изчислителни технологии, създадена съгласно Регламент (ЕС) 2021/1173.

Член 4

Национални центрове за операции по сигурността

1. За да участва в европейския киберщит, всяка държава членка определя поне един национален ЦОС. Националният ЦОС е публичен орган.

Той има способност да действа като отправна точка и портал за други публични и частни организации на национално равнище за събиране и анализиране на информация относно киберзаплахите и инцидентите и да допринася за работата на трансграничен ЦОС. Той е оборудван с най-съвременни технологии, способни да откриват, обобщават и анализират данни, свързани с киберзаплахите и инцидентите.

2. След покана за заявяване на интерес националните ЦОС се избират от Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността („ЕССС“), за да участват с ЕССС в съвместна обществена поръчка за инструменти и инфраструктури. ЕССС може да отпуска безвъзмездни средства на избраните национални ЦОС за финансиране на функционирането на тези инструменти и инфраструктури. Финансовото участие на Съюза покрива до 50 % от разходите за придобиване на инструментите и инфраструктурите и до 50 % от оперативните разходи, а останалите разходи се поемат от държавата членка. Преди да започнат процедурата за придобиване на инструментите и инфраструктурите, ЕССС и националният ЦОС сключват споразумение за хостинг и използване, което урежда използването на инструментите и инфраструктурите.

3. Националният ЦОС, избран съгласно параграф 2, се ангажира да подаде заявление за участие в трансграничен ЦОС в срок от две години от датата на придобиване на инструментите и инфраструктурите или от датата на получаване на безвъзмездните средства, в зависимост от това кое от двете събития настъпи по-рано. Ако до този момент национален ЦОС не е участник в трансграничен ЦОС, той няма право на допълнителна подкрепа от Съюза съгласно настоящия регламент.

Член 5

Трансгранични центрове за операции по сигурността

1. Консорциум, осигуряващ хостинг, състоящ се от най-малко три държави членки, представени от национални ЦОС, които са поели ангажимент да работят заедно, за да координират своите дейности по откриване и наблюдение на киберзаплахи, има право да участва в действията за създаване на трансграничен ЦОС.

2. След покана за заявяване на интерес ЕССС избира консорциум, осигуряващ хостинг, който да участва в съвместна обществена поръчка за инструменти и инфраструктури. ЕССС може да отпусне на консорциума, осигуряващ хостинг, безвъзмездни средства за финансиране на функционирането на инструментите и инфраструктурите. Финансовото участие на Съюза покрива до 75 % от разходите за придобиване на инструментите и инфраструктурите и до 50 % от оперативните разходи, а останалите разходи се поемат от консорциума, осигуряващ хостинг. Преди да започнат процедурата за придобиване на инструментите и инфраструктурите, ЕССС и консорциумът, осигуряващ хостинг, сключват споразумение за хостинг и използване, което урежда използването на инструментите и инфраструктурите.

3. Членовете на консорциума, осигуряващ хостинг, сключват писмено споразумение за консорциум, в което се посочват техните вътрешни договорености за изпълнение на споразумението за хостинг и използване.

4. Трансграничният ЦОС се представлява за правни цели от национален ЦОС, действащ като координиращ ЦОС, или от консорциума, осигуряващ хостинг, ако той е юридическо лице. Координиращият ЦОС отговаря за спазването на изискванията на споразумението за хостинг и използване и на настоящия регламент.

Член 6

Сътрудничество и обмен на информация в рамките на трансграничните ЦОС и между тях

1. Членовете на консорциума, осигуряващ хостинг, обменят помежду си относима информация в рамките на трансграничния ЦОС, включително информация относно киберзаплахи, ситуации, близки до инциденти, уязвимости, техники и процедури, показатели за компрометиране на системите, злонамерени тактики, специфична за източника на заплахата информация, предупреждения във връзка с киберсигурността и препоръки за конфигуриране на инструменти за киберсигурност за откриване на кибератаки, когато този обмен на информация:

а) има за цел превенция, откриване, реагиране или възстановяване от инциденти или смекчаване на тяхното въздействие;

б) подобрява нивото на киберсигурност, по-специално посредством повишаване на осведомеността във връзка с киберзаплахи, ограничаване или възпрепятстване на способността за разпространение на такива заплахи, поддържане на набор от отбранителни способности, отстраняване и оповестяване на уязвимости, техники за откриване, ограничаване и превенция на заплахи, стратегии за ограничаване или етапи за реагиране или възстановяване или насърчаване на съвместни научни изследвания относно заплахите между публични и частни субекти.

2. В писменото споразумение за консорциум, посочено в член 5, параграф 3, се установява:

а) ангажимент за обмен на значителен обем данни, посочени в параграф 1, и условията, при които ще се извършва обменът на информация;

б) рамка за управление, стимулираща обмена на информация от всички участници;

в) цели за принос към разработването на авангардни инструменти за изкуствен интелект и анализ на данни.

3. За насърчаването на обмена на информация между трансграничните ЦОС, трансграничните ЦОС гарантират високо ниво на оперативна съвместимост помежду

си. За улесняването на оперативната съвместимост между трансграничните ЦОС, Комисията може чрез актове за изпълнение, след като се консултира с ЕССС, да определи условията за тази оперативна съвместимост. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 21, параграф 2 от настоящия регламент.

4. Трансграничните ЦОС сключват споразумения за сътрудничество помежду си, в които се посочват принципите за обмен на информация между трансграничните платформи.

Член 7

Сътрудничество и обмен на информация със субектите на Съюза

1. Когато трансграничните ЦОС получат информация, свързана с потенциален или текущ мащабен киберинцидент, те незабавно предоставят съответната информация на EU-CyCLONe, мрежата на ЕРИКС и Комисията с оглед на съответните им функции по управление на кризи в съответствие с Директива (ЕС) 2022/2555.

2. Чрез актове за изпълнение Комисията може да определи процедурните разпоредби за обмена на информация, предвиден в параграф 1. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 21, параграф 2 от настоящия регламент.

Член 8

Сигурност

1. Държавите членки, участващи в европейския киберщит, осигуряват високо ниво на сигурност на данните и физическа сигурност на инфраструктурата на европейския киберщит и гарантират, че инфраструктурата се управлява и контролира по подходящ начин, така че да бъде защитена от заплахи и да се гарантира нейната сигурност и тази на системите, включително сигурността на данните, обменяни чрез инфраструктурата.

2. Държавите членки, участващи в европейския киберщит, гарантират, че обменът на информация в рамките на европейския киберщит със субекти, които не са публични органи на държава членка, не засяга отрицателно интересите на Съюза в областта на сигурността.

3. Комисията може да приема актове за изпълнение за определяне на техническите изисквания, които държавите членки трябва да спазват, за да изпълнят задълженията си по параграфи 1 и 2. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 21, параграф 2 от настоящия регламент. При това Комисията, подпомагана от върховния представител, взема предвид съответните стандарти за сигурност на ниво отбрана, за да улесни сътрудничеството с военните участници.

Глава III

МЕХАНИЗЪМ ЗА ДЕЙСТВИЕ ПРИ ИЗВЪНРЕДНИ СИТУАЦИИ В ОБЛАСТТА НА КИБЕРСИГУРНОСТТА

Член 9

Създаване на Механизъм за действие при извънредни ситуации в областта на киберсигурността

1. Създава се Механизъм за действие при извънредни ситуации в областта на киберсигурността с цел да се подобри устойчивостта на Съюза на големи киберзаплахи и да се подготви и смекчи, в дух на солидарност, краткосрочното въздействие на значителни и мащабни киберинциденти („Механизмът“).

2. Действията за прилагане на Механизма за действие при извънредни ситуации в областта на киберсигурността се подкрепят с финансиране от програмата „Цифрова Европа“ и се изпълняват в съответствие с Регламент (ЕС) 2021/694, и по-специално със специфична цел 3 от него.

Член 10

Вид действия

1. Механизмът подпомага следните видове действия:

а) действия за готовност, включително координирано изпитване на готовността на субектите, извършващи дейност във висококритични сектори в целия Съюз;

б) действия за реагиране, подпомагащи реагирането и незабавното възстановяване след значителни и мащабни киберинциденти, които да се предоставят от доверителни доставчици, участващи в резерва за киберсигурност на ЕС, създаден съгласно член 12;

в) действия за взаимопомощ, състоящи се в предоставяне на помощ от националните органи на една държава членка на друга държава членка, по-специално както е предвидено в член 11, параграф 3, буква е) от Директива (ЕС) 2022/2555.

Член 11

Координирано изпитване на готовността на субектите

1. С цел подпомагане на координираното изпитване на готовността на субектите, посочени в член 10, параграф 1, буква а), в целия Съюз, Комисията, след консултация с групата за сътрудничество за МИС и ENISA, определя съответните сектори или подсектори от секторите с висока степен на критичност, изброени в приложение I към Директива (ЕС) 2022/2555, от които могат да се избират субекти, които да се подлагат на координираното изпитване на готовността, като взема предвид съществуващите и планираните координирани оценки на риска и изпитвания на устойчивостта на равнището на Съюза.

2. Групата за сътрудничество за МИС, в сътрудничество с Комисията, ENISA и върховния представител, разработва общи сценарии за риска и методологии за координираните изпитвания.

Член 12

Създаване на резерва за киберсигурност на ЕС

1. Създава се резерв за киберсигурност на ЕС, за да се подпомагат ползвателите, посочени в параграф 3, при реагиране или осигуряване на подкрепа за реагиране на значителни или мащабни киберинциденти, както и за незабавно възстановяване след такива инциденти.

2. Резервът за киберсигурност на ЕС се състои от услуги за реагиране при инциденти, предоставяни от доверителни доставчици, избрани в съответствие с критериите, посочени в член 16. Резервът включва предварително заявени услуги. Услугите могат да бъдат предоставяни във всички държави членки.

3. Ползвателите на услугите от резерва за киберсигурност на ЕС включват:

а) органи за управление на киберкризи на държавите членки и ЕРИКС, както е посочено съответно в член 9, параграфи 1 и 2 и член 10 от Директива (ЕС) 2022/2555;

б) институции, органи, служби и агенции на Съюза.

4. Ползвателите, посочени в параграф 3, буква а), използват услугите от резерва за киберсигурност на ЕС с цел да реагират или да подпомогнат реагирането и незабавното възстановяване след значителни или мащабни инциденти, засягащи субекти, извършващи дейност в критични или висококритични сектори.

5. Комисията носи цялостна отговорност за изпълнението на резерва за киберсигурност на ЕС. Комисията определя приоритетите и развитието на резерва за киберсигурност на ЕС в съответствие с изискванията на ползвателите, посочени в параграф 3, и упражнява надзор върху неговото изпълнение, като осигурява взаимно допълване, съгласуваност, полезни взаимодействия и връзки с други действия за подкрепа съгласно настоящия регламент, както и с други действия и програми на Съюза.

6. Комисията може да възложи функционирането и управлението на резерва за киберсигурност на ЕС, изцяло или частично, на ENISA посредством споразумения за финансов принос.

7. За да подпомогне Комисията при създаването на резерва за киберсигурност на ЕС, ENISA изготвя картографиране на необходимите услуги, след като се консултира с държавите членки и Комисията. След консултация с Комисията ENISA изготвя подобно картографиране за определяне на нуждите на трети държави, които отговарят на условията за получаване на подкрепа от резерва за киберсигурност на ЕС съгласно член 17. Когато е уместно, Комисията се консултира с върховния представител.

8. Чрез актове за изпълнение Комисията може да определя видовете и броя на услугите за реагиране, необходими за резерва за киберсигурност на ЕС. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 21, параграф 2.

Член 13

Искания за подкрепа от резерва за киберсигурност на ЕС

1. Ползвателите, посочени в член 12, параграф 3, могат да поискат услуги от резерва за киберсигурност на ЕС, за да подпомогнат реагирането и незабавното възстановяване след значителни или мащабни киберинциденти.

2. За да получат подкрепа от резерва за киберсигурност на ЕС, ползвателите, посочени в член 12, параграф 3, трябва да предприемат мерки за смекчаване на последиците от инцидента, във връзка с който е поискана подкрепата, включително предоставяне на пряка техническа помощ и други ресурси за подпомагане на реагирането на инцидента и на усилията за незабавно възстановяване.

3. Исканията за подкрепа от ползвателите, посочени в член 12, параграф 3, буква а) от настоящия регламент, се предават на Комисията и на ENISA чрез единното звено за контакт, определено или създадено от държавата членка в съответствие с член 8, параграф 3 от Директива (ЕС) 2022/2555.

4. Държавите членки информират мрежата на ЕРИКС и, когато е целесъобразно, EU-CyCLONe за своите искания за подкрепа при реагиране на инциденти и незабавно възстановяване съгласно настоящия член.

5. Исканията за подкрепа за реагиране при инцидент и незабавно възстановяване включват:

а) подходяща информация относно засегнатия субект и потенциалните въздействия на инцидента и планираното използване на исканата подкрепа, включително посочване на очакваните нужди;

б) информация за предприетите мерки за смекчаване на последиците от инцидента, във връзка с който е поискана подкрепата, както е посочено в параграф 2;

в) информация за други форми на подкрепа, които са на разположение на засегнатия субект, включително действащи договорни споразумения за услуги за реагиране на инциденти и незабавно възстановяване, както и застрахователни договори, които потенциално покриват такъв тип инциденти.

6. ENISA, в сътрудничество с Комисията и групата за сътрудничество за МИС, разработва образец за улесняване на подаването на искания за подкрепа от резерва за киберсигурност на ЕС.

7. Чрез актове за изпълнение Комисията може допълнително да уточнява подробните условия за разпределяне на услугите за подкрепа от резерва за киберсигурност на ЕС. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 21, параграф 2.

Член 14

Изпълнение на подкрепата от резерва за киберсигурност на ЕС

1. Исканията за подкрепа от резерва за киберсигурност на ЕС се оценяват от Комисията с подкрепата на ENISA или както е определено в споразуменията за финансов принос по член 12, параграф 6, а отговорът се предава незабавно на ползвателите, посочени в член 12, параграф 3.

2. При определянето на приоритетни искания в случай на множество едновременни искания се вземат предвид следните критерии, когато е целесъобразно:

а) сериозността на киберинцидента;

б) вида на засегнатия субект, като по-висок приоритет се дава на инциденти, засягащи съществени субекти, както е определено в член 3, параграф 1 от Директива (ЕС) 2022/2555;

в) потенциалното въздействие върху засегнатата(ите) държава(и) членка(и) или ползвателите;

г) потенциалния трансграничен характер на инцидента и риска от разпространението му към други държави членки или ползватели;

д) мерките, предприети от ползвателя за подпомагане на реагирането и усилията за незабавно възстановяване, както е посочено в член 13, параграф 2 и член 13, параграф 5, буква б).

3. Услугите в рамките на резерва за киберсигурност на ЕС се предоставят в съответствие със специални споразумения между доставчика на услуги и ползвателя, на когото се предоставя подкрепата в рамките на резерва за киберсигурност на ЕС. Тези споразумения включват условия за отговорност.

4. Споразуменията, посочени в параграф 3, могат да се основават на образци, изготвени от ENISA след консултации с държавите членки.

5. Комисията и ENISA не носят договорна отговорност за вреди, причинени на трети лица от услугите, предоставяни в рамките на изпълнението на резерва за киберсигурност на ЕС.

6. В срок от един месец след края на действието за подкрепа ползвателите предоставят на Комисията и на ENISA обобщен доклад за предоставената услуга, постигнатите резултати и извлечените поуки. Когато ползвателят е от трета държава, както е посочено в член 17, този доклад се предоставя на върховния представител.

7. Комисията редовно докладва на групата за сътрудничество за МИС за използването и резултатите от подкрепата.

Член 15

Координация с механизмите за управление на кризи

1. В случаите, когато значителни или мащабни киберинциденти произтичат от или водят до бедствия, както е определено в Решение 1313/2013/ЕС[19], подкрепата по настоящия регламент за реагиране на такива инциденти допълва действията по Решение 1313/2013/ЕС, без да засяга неговите разпоредби.

2. В случай на мащабен трансграничен киберинцидент, при който са задействани договореностите за интегрирана реакция при политическа криза (ИРПК), подкрепата по настоящия регламент за реагиране на такъв инцидент се осъществява в съответствие със съответните протоколи и процедури по ИРПК.

3. След консултация с върховния представител подкрепата в рамките на Механизма за действие при извънредни ситуации в областта на киберсигурността може да допълва помощта, предоставяна в контекста на общата външна политика и политика на сигурност и общата политика за сигурност и отбрана, включително чрез екипите за бързо реагиране в областта на киберсигурността. Тя може също така да допълва или да допринася за помощта, предоставяна от една държава членка на друга държава членка в контекста на член 42, параграф 7 от Договора за Европейския съюз.

4. Подкрепата в рамките на Механизма за действие при извънредни ситуации в областта на киберсигурността може да бъде част от съвместното реагиране на Съюза и държавите членки в ситуациите, посочени в член 222 от Договора за функционирането на Европейския съюз.

Член 16

Доверителни доставчици

1. При процедурите за възлагане на обществени поръчки за целите на създаването на резерва за киберсигурност на ЕС възлагащият орган действа в съответствие с принципите, установени в Регламент (ЕС, Евратом) 2018/1046, и в съответствие със следните принципи:

[19] Решение № 1313/2013/ЕС на Европейския парламент и на Съвета от 17 декември 2013 г. относно Механизъм за гражданска защита на Съюза (ОВ L 347, 20.12.2013 г., стр. 924).

а) гарантиране, че резервът за киберсигурност на ЕС включва услуги, които могат да се използват във всички държави членки, като се вземат предвид по-специално националните изисквания за предоставяне на такива услуги, включително сертифициране или акредитация;

б) гарантиране на защитата на основните интереси на Съюза и неговите държави членки в областта на сигурността;

в) гарантиране, че резервът за киберсигурност на ЕС носи добавена стойност за ЕС, като допринася за постигането на целите, посочени в член 3 от Регламент (ЕС) 2021/694, включително за насърчаване на развитието на умения в областта на киберсигурността в ЕС.

2. При възлагане на поръчки за услуги за резерва за киберсигурност на ЕС възлагащият орган включва в документацията за обществената поръчка следните критерии за подбор:

а) доставчикът доказва, че неговият персонал притежава най-висока степен на професионална почтеност, независимост, отговорност и необходимата техническа компетентност за изпълнение на дейностите в конкретната област и осигурява постоянство/непрекъснатост на експертния опит, както и необходимите технически ресурси;

б) доставчикът, неговите дъщерни дружества и подизпълнители разполагат с действаща рамка за защита на чувствителната информация, свързана с услугата, и по-специално на доказателствата, констатациите и докладите, и е в съответствие с правилата на Съюза за сигурност относно защитата на класифицирана информация на ЕС;

в) доставчикът представя достатъчно доказателства, че неговата управленска структура е прозрачна и няма вероятност тя да застраши неговата безпристрастност и качеството на услугите му или да предизвика конфликти на интереси;

г) доставчикът разполага с подходящо разрешение за достъп, поне за персонала, предназначен за разгръщане на услугата;

д) ИТ системите на доставчика разполагат със съответното ниво на сигурност;

е) доставчикът разполага с хардуерно и софтуерно техническо оборудване, необходимо за поддържане на търсената услуга;

ж) доставчикът е в състояние да докаже, че има опит в предоставянето на подобни услуги на съответните национални органи или субекти, извършващи дейност в критични или висококритични сектори;

з) доставчикът е в състояние да достави услугата в кратък срок в държавата(ите) членка(и), в която(ито) може да я предоставя;

и) доставчикът е в състояние да достави услугата на местния език на държавата(ите) членка(и), в която(ито) може да я предоставя;

й) след като бъде въведена схема на ЕС за сертифициране на управлявани услуги за сигурност Регламент (ЕС) 2019/881, доставчикът се сертифицира в съответствие с тази схема.

Член 17

Подкрепа за трети държави

1. Трети държави могат да поискат подкрепа от резерва за киберсигурност на ЕС, когато това е предвидено в споразуменията за асоцииране, сключени във връзка с участието им в програмата „Цифрова Европа“.

2. Подкрепата от резерва за киберсигурност на ЕС е в съответствие с настоящия регламент и е съобразена с всички специфични условия, предвидени в споразуменията за асоцииране, посочени в параграф 1.

3. Ползвателите от асоциирани трети държави, които имат право да получават услуги от резерва за киберсигурност на ЕС, включват компетентни органи, като например ЕРИКС и органи за управление на киберкризи.

4. Всяка трета държава, която отговаря на условията за получаване на подкрепа от резерва за киберсигурност на ЕС, определя орган, който да действа като единно звено за контакт за целите на настоящия регламент.

5. Преди да получат каквато и да е подкрепа от резерва за киберсигурност на ЕС, третите държави предоставят на Комисията и на върховния представител информация за способностите си за киберустойчивост и управление на риска, включително най-малко информация за предприетите национални мерки за подготовка за значителни или мащабни киберинциденти, както и информация за отговорните национални субекти, включително ЕРИКС или равностойни субекти, техните способности и предоставените им ресурси. Когато разпоредбите на членове 13 и 14 от настоящия регламент се отнасят за държави членки, те се прилагат и за трети държави, както е посочено в параграф 1.

6. Комисията координира с върховния представител получените искания и изпълнението на подкрепата, предоставена на трети държави от резерва за киберсигурност на ЕС.

Глава IV

МЕХАНИЗЪМ ЗА ПРЕГЛЕД НА КИБЕРИНЦИДЕНТИ

Член 18

Механизъм за преглед на киберинциденти

1. По искане на Комисията, EU-CyCLONe или мрежата на ЕРИКС ENISA извършва преглед и оценка на заплахите, уязвимостите и действията за смекчаване на

последиците по отношение на конкретен значителен или мащабен киберинцидент. След приключване на прегледа и оценката на даден инцидент ENISA предоставя доклад за прегледа на инцидента на мрежата на ЕРИКС, EU-CyCLONe и Комисията, за да ги подкрепи при изпълнението на техните задачи, по-специално с оглед на посочените задачи в членове 15 и 16 от Директива (ЕС) 2022/2555. Когато е целесъобразно, Комисията предоставя доклада на върховния представител.

2. За изготвянето на доклада за преглед на инцидент, посочен в параграф 1, ENISA си сътрудничи с всички съответни заинтересовани страни, включително представители на държавите членки, Комисията, други съответни институции, органи, служби и агенции на ЕС, доставчиците на управлявани услуги за сигурност и ползвателите на услуги за киберсигурност. Когато е целесъобразно, ENISA си сътрудничи и със субекти, засегнати от значителни или мащабни киберинциденти. За да подпомогне прегледа, ENISA може да се консултира и с други видове заинтересовани страни. Консултираните представители оповестяват всеки потенциален конфликт на интереси.

3. Докладът обхваща преглед и анализ на конкретния значителен или мащабен киберинцидент, включително основните причини, уязвимостите и извлечените поуки. Поверителната информация в него е защитена в съответствие с правото на Съюза или националното право относно защитата на чувствителна или класифицирана информация.

4. Когато е целесъобразно, докладът съдържа препоръки за подобряване на състоянието на киберсигурността на Съюза.

5. Когато е възможно, версия на доклада се оповестява публично. Тази версия включва само публична информация.

Глава V

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 19

Изменения на Регламент (ЕС) 2021/694

Регламент (ЕС) 2021/694 се изменя, както следва:

(1) Член 6 се изменя, както следва:

а) параграф 1 се изменя, както следва:

(1) вмъква се следната буква аа):

„аа) подкрепяне на разработването на киберщит на ЕС, включително разработването, разгръщането и функционирането на национални и трансгранични платформи за ЦОС, които допринасят за ситуационната осведоменост в Съюза и за повишаване на способностите на Съюза за разузнаване на киберзаплахи“;

(2) добавя се следната буква ж):

„ж) създаване и управление на Механизъм за действие при извънредни ситуации в областта на киберсигурността в подкрепа на държавите членки при подготовката и реагирането на значителни киберинциденти, в допълнение към националните ресурси и способности и други форми на подкрепа, налични на равнището на Съюза, включително създаването на резерв за киберсигурност на ЕС“;

а) параграф 2 се заменя със следното:

„2. Действията по специфична цел 3 се изпълняват основно чрез Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Мрежата от национални координационни центрове в съответствие с Регламент (ЕС) 2021/887 на Европейския парламент и на Съвета[20], с изключение на действията за изпълнение на резерва за киберсигурност на ЕС, които се изпълняват от Комисията и ENISA.“**;**

2) Член 9 се изменя, както следва:

а) в параграф 2 букви б), в) и г) се заменят със следното:

„б) 1 776 956 000 евро за специфична цел 2 — Изкуствен интелект;

в) 1 629 566 000 евро за специфична цел 3 — Киберсигурност и доверие;

г) 482 347 000 евро за специфична цел 4 — Задълбочени цифрови умения“;

б) добавя се следният параграф 8:

„8. Чрез дерогация от член 12, параграф 4 от Регламент (ЕС, Евратом) 2018/1046 неизползваните бюджетни кредити за поети задължения и за плащания за действия, насочени към постигане на целите, посочени в член 6, параграф 1, буква ж) от настоящия регламент, се пренасят автоматично и за тях могат да се поемат задължения и да се извършват плащания до 31 декември на следващата финансова година.“;

[20] Регламент (ЕС) 2021/887 на Европейския парламент и на Съвета от 20 май 2021 г. за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове (ОВ L 202, 8.6.2021 г., стр. 1—31).

3) В член 14 параграф 2 се заменя със следното:

„2. Програмата може да предоставя финансиране под всяка една от формите, предвидени във Финансовия регламент, включително по-специално чрез поръчки, като основна форма, или чрез безвъзмездни средства и награди.

Когато постигането на целта на действието изисква поръчки за иновативни стоки и услуги, безвъзмездни средства могат да се отпускат единствено на бенефициери, които са възлагащи органи или възложители съгласно определението в директиви 2014/24/ЕС [27] и 2014/25/ЕС [28] на Европейския парламент и на Съвета.

Когато за постигането на целите на действието е необходимо предоставянето на иновативни стоки или услуги, които все още не са налични на широка търговска основа, възлагащият орган или възложителят може да разреши възлагането на множество договори в рамките на една и съща процедура за възлагане на поръчка.

По надлежно обосновани причини, свързани с обществената сигурност, възлагащият орган или възложителят може да изиска мястото на изпълнение на договора да бъде на територията на Съюза.

При изпълнението на процедурите за възлагане на обществени поръчки за резерва за киберсигурност на ЕС, създаден с член 12 от Регламент (ЕС) 2023/XX, Комисията и ENISA могат да действат като централен орган за покупки, за да възлагат обществени поръчки от името или за сметка на трети държави, асоциирани към програмата, в съответствие с член 10. Комисията и ENISA могат също така да действат като търговци на едро, като купуват, складират и препродават или даряват доставки и услуги, включително наеми, на тези трети държави. Чрез дерогация от член 169, параграф 3 от Регламент (ЕС). XXX/XXXX [преработен текст на финансовия регламент], искането от една-единствена трета държава е достатъчно, за да се упълномощи Комисията или ENISA да предприемат действия.

При изпълнението на процедурите за възлагане на обществени поръчки за резерва за киберсигурност на ЕС, създаден с член 12 от Регламент (ЕС) 2023/XX, Комисията и ENISA могат да действат като централен орган за покупки, за да възлагат обществени поръчки от името или за сметка на институциите, органите, службите и агенциите на Съюза. Комисията и ENISA могат също така да действат като търговци на едро, като купуват, складират и препродават или даряват доставки и услуги, включително наеми, на институциите, органите, службите и агенциите на Съюза. Чрез дерогация от член 169, параграф 3 от Регламент (ЕС) XXX/XXXX [преработен текст на финансовия регламент] искането от една-единствена институция, орган, служба или агенция на Съюза е достатъчно, за да се упълномощи Комисията или ENISA да предприемат действия.

Програмата може да предоставя също така финансиране под формата на финансови инструменти в рамките на операции за смесено финансиране.“

4) Добавя се следният член 16а:

„В случай на действия за изпълнение на европейския киберщит, установен с член 3 от Регламент (ЕС) 2023/XX, приложимите правила са посочените в членове 4 и 5 от Регламент (ЕС) 2023/XX. В случай на противоречие между разпоредбите на настоящия регламент и членове 4 и 5 от Регламент (ЕС) 2023/XX, последните имат предимство и се прилагат за тези специфични действия.“

5) Член 19 се заменя със следното:

„Безвъзмездните средства по Програмата се отпускат и управляват в съответствие с дял VIII от Финансовия регламент и могат да покриват до 100 % от допустимите разходи, без да се засяга принципът на съфинансиране, установен в член 190 от Финансовия регламент. Такива безвъзмездни средства се отпускат и управляват, както е посочено за всяка специфична цел.

Подкрепа под формата на безвъзмездни средства може да бъде отпускана пряко от ЕССС без покана за представяне на предложения на националните ЦОС, посочени в член 4 от Регламент XXXX, и на консорциума, осигуряващ хостинг, посочен в член 5 от Регламент XXXX, в съответствие с член 195, параграф 1, буква г) от Финансовия регламент.

Подкрепа под формата на безвъзмездни средства за Механизма за действие при извънредни ситуации в областта на киберсигурността, както е посочено в член 10 от Регламент XXXX, може да бъде отпускана пряко от ЕССС на държавите членки без покана за представяне на предложения в съответствие с член 195, параграф 1, буква г) от Финансовия регламент.

За действията, посочени в член 10, параграф 1, буква в) от Регламент 202X/XXXX, ЕССС информира Комисията и ENISA за исканията на държавите членки за отпускане на преки безвъзмездни средства без покана за представяне на предложения.

За подпомагане на взаимопомощта за реагиране на значителен или мащабен киберинцидент, както е определено в член 10, буква в) от Регламент XXXX, и в съответствие с член 193, параграф 2, втора алинея, буква а) от Финансовия регламент, в надлежно обосновани случаи разходите могат да се считат за допустими, дори ако са направени преди подаването на заявлението за безвъзмездни средства.“

6) Приложения I и II се изменят в съответствие с приложението към настоящия регламент.

Член 20

Оценка

До [четири години след датата на прилагането настоящия регламент] Комисията представя на Европейския парламент и на Съвета доклад относно оценката и прегледа на настоящия регламент.

Член 21

Процедура на комитет

1. Комисията се подпомага от координационния комитет на програмата „Цифрова Европа“, създаден с Регламент (ЕС) 2021/694. Този комитет е комитет по смисъла на Регламент (ЕС) 182/2011.
2. При позоваване на настоящия параграф се прилага член 5 от Регламент (ЕС) 182/2011.

Член 22

Влизане в сила

Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Страсбург на […] година.

За Европейския парламент
Председател

За Съвета
Председател

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1. Наименование на предложението/инициативата

1.2. Съответни области на политиката

1.3. Предложението/инициативата е във връзка с:

1.4. Цели

1.4.1. Общи цели

1.4.2. Специфични цели

1.4.3. Очаквани резултати и въздействие

1.4.4. Показатели за изпълнението

1.5. Мотиви за предложението/инициативата

1.5.1. Изисквания, които трябва да бъдат изпълнени в краткосрочна или дългосрочна перспектива, включително подробен график за изпълнението на инициативата

1.5.2. Добавена стойност от участието на Съюза (може да е в резултат от различни фактори, например ползи по отношение на координацията, правна сигурност, по-добра ефективност или взаимно допълване). За целите на тази точка „добавена стойност от участието на Съюза“ е стойността, която е резултат от намесата на ЕС и е допълнителна спрямо стойността, която би била създадена само от отделните държави членки.

1.5.3. Изводи от подобен опит в миналото

1.5.4. Съвместимост с многогодишната финансова рамка и евентуални полезни взаимодействия с други подходящи инструменти

1.5.5. Оценка на различните налични варианти за финансиране, включително възможностите за преразпределяне на средства

1.6. Продължителност и финансово отражение на предложението/инициативата

1.7. Планирани методи на изпълнение на бюджета

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

2.2. Системи за управление и контрол

2.2.1. Обосновка на предложените начини за управление, механизми за финансиране на изпълнението, начини за плащане и стратегия за контрол

2.2.2. Информация относно установените рискове и системите за вътрешен контрол, създадени с цел намаляването им

2.2.3. Оценка и обосновка на разходната ефективност на проверките (съотношение „разходи за контрол ÷ стойност на съответните управлявани фондове“) и оценка на очакваната степен на риска от грешки (при плащане и при приключване)

2.3. Мерки за предотвратяване на измами и нередности

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

3.1. Съответни функции от многогодишната финансова рамка и разходни бюджетни редове

3.2. Очаквано финансово отражение на предложението върху бюджетните кредити

3.2.1. Обобщение на очакваното отражение върху бюджетните кредити за оперативни разходи

3.2.2. Очакван резултат, финансиран с бюджетни кредити за оперативни разходи

3.2.3. Обобщение на очакваното отражение върху бюджетните кредити за административни разходи

3.2.3.1. Очаквани нужди от човешки ресурси

3.2.4. Съвместимост с настоящата многогодишна финансова рамка

3.2.5. Финансов принос от трети страни

3.3. Очаквано отражение върху приходите

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1. Наименование на предложението/инициативата

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

1.2. Съответни области на политиката

Европа, подготвена за цифровата ера

Европейски стратегически инвестиции

Дейност: стратегия в областта на цифровите технологии.

1.3. Предложението/инициативата е във връзка с:

☒ **ново действие**

☐ **ново действие след пилотен проект/подготвително действие**[33]

☐ **продължаване на съществуващо действие**

☐ **сливане или пренасочване на едно или няколко действия към друго/ново действие**

1.4. Цели

1.4.1. Общи цели

Законодателният акт за киберсолидарност ще засили солидарността на равнището на Съюза, за да може по-ефективно да се откриват киберзаплахите и да се подобри подготовката и реагирането при киберинциденти. Той има за цел:

а) укрепване на общите способности на ЕС за откриване и ситуационна осведоменост за киберзаплахи и инциденти;

б) повишаване на готовността на критичните субекти в целия ЕС и укрепване на солидарността чрез изграждане на общи способности за реагиране при значителни или мащабни киберинциденти, включително чрез предоставяне на подкрепа за реагиране при инциденти на трети държави, асоциирани към програмата „Цифрова Европа“;

в) повишаване на устойчивостта на Съюза и допринасяне за ефективно реагиране чрез преглед и оценка на значителни или мащабни киберинциденти, включително извличане на поуки и, когато е уместно, препоръки.

[33] Съгласно член 58, параграф 2, буква а) или б) от Финансовия регламент.

1.4.2. Специфични цели

Законодателният акт за киберсолидарност ще постигне набора от цели чрез:

а) разгръщането на общоевропейска инфраструктура от центрове за операции по сигурността („европейски киберщит“) за изграждане и подобряване на общите способности за откриване и ситуационна осведоменост;

б) създаването на Механизъм за действие при извънредни ситуации в областта на киберсигурността, който да подпомага държавите членки при подготовката, реагирането и незабавното възстановяване след значителни и мащабни киберинциденти. Подкрепа за реагиране при инциденти се предоставя и на институциите, органите, службите и агенциите на ЕС (EUIBA).

Тези действия ще бъдат подкрепени с финансиране от програмата „Цифрова Европа“, която ще бъде изменена с настоящия законодателен инструмент, за да се установят горепосочените действия, да се осигури финансова подкрепа за тяхното разработване и да се пояснят условията за възползване от финансовата подкрепа;

в) създаването на европейски Механизъм за преглед на киберинциденти, който да разглежда и оценява значителни или мащабни киберинциденти.

1.4.3. Очаквани резултати и въздействие

Да се посочи въздействието, което предложението/инициативата следва да окаже по отношение на бенефициерите/целевите групи.

Предложението би донесло значителни ползи за различните заинтересовани страни. Европейският киберщит ще подобри способностите на държавите членки за откриване на киберзаплахи. Механизмът за действие при извънредни ситуации в областта на киберсигурността ще допълва действията на държавите членки чрез спешна подкрепа за готовност, реагиране и незабавно възстановяване/възстановяване на функционирането на основните услуги.

Тези действия ще укрепят конкурентната позиция на промишлеността и предприятията в Европа в рамките на цифровизираната икономика, както и тяхната цифрова трансформация, като се повиши нивото на киберсигурността на цифровия единен пазар. По-специално целта е да се повиши устойчивостта на гражданите, предприятията и субектите, извършващи дейност в критични или висококритични сектори, срещу нарастващите киберзаплахи, които могат да имат опустошително въздействие върху обществото и икономиката. Това ще се осъществи чрез инвестиране в инструменти, които ще подпомогнат по-бързото откриване и реагиране при киберзаплахи и инциденти, както и чрез подкрепа за държавите членки с цел подобряване на тяхната подготовка и

реагиране при значителни и мащабни киберинциденти. По този начин следва да се подпомогнат и осигурят по-силни способности на Европа в тези области, особено по отношение на събирането и анализирането на данни за киберзаплахите и инцидентите.

1.4.4. Показатели за изпълнението

Да се посочат показателите за проследяване на напредъка и на постиженията.

За да се насърчи солидарността на равнището на Съюза, могат да се вземат предвид няколко показателя:

(1) Брой на съвместно придобитите инфраструктури или инструменти за киберсигурност, или и двете

(2) Брой на действията в подкрепа на готовността и реагирането при киберинциденти в рамките на Механизма за действие при извънредни ситуации в областта на киберсигурността.

1.5. Мотиви за предложението/инициативата

1.5.1. Изисквания, които трябва да бъдат изпълнени в краткосрочна или дългосрочна перспектива, включително подробен график за изпълнението на инициативата

Регламентът следва да бъде напълно приложим скоро след приемането му, т.е. на двадесетия ден след публикуването му в Официален вестник на Европейския съюз.

1.5.2. Добавена стойност от участието на Съюза (може да е в резултат от различни фактори, например ползи по отношение на координацията, правна сигурност, по-добра ефективност или взаимно допълване). За целите на тази точка „добавена стойност от участието на Съюза“ е стойността, която е резултат от намесата на ЕС и е допълнителна спрямо стойността, която би била създадена само от отделните държави членки.

Силно изразеният трансграничен характер на киберзаплахите като цяло и нарастващият брой на рисковете и инцидентите, които се разпространяват към други държави, сектори и продукти, означават, че целите на настоящата намеса не могат да бъдат постигнати ефективно само от държавите членки и изискват общи действия и солидарност на равнището на Съюза. Опитът от противодействието на киберзаплахите, произтичащи от войната срещу Украйна, както и поуките, извлечени от ученията в областта на киберсигурността, проведено по време на френското председателство (EU-CyCLES), показаха, че за постигане на солидарност на равнището на ЕС следва да се разработят конкретни механизми за взаимна подкрепа, по-специално сътрудничество с частния сектор. В този контекст в заключенията на Съвета от 23 май 2022 г. относно установяването на позицията на Европейския съюз в киберпространството Комисията се призовава да представи предложение за нов фонд за реагиране при извънредни ситуации в областта на киберсигурността. Подкрепата и действията на равнището на Съюза за по-добро откриване на

киберзаплахите и за повишаване на готовността и способността за реагиране осигуряват добавена стойност, тъй като така се избягва дублиране на усилията в Съюза и държавите членки. Това би довело до по-добро използване на съществуващите активи и до по-добра координация и обмен на информация относно извлечените поуки.

1.5.3. Изводи от подобен опит в миналото

По отношение на ситуационната осведоменост и откриването в рамките на европейския киберщит, като част от работната програма за киберсигурност на програмата „Цифрово десетилетие“ за периода 2021—2022 г. бяха отправени покана за заявяване на интерес за съвместна обществена поръчка за инструменти и инфраструктура с цел създаване на трансгранични ЦОС и покана за предоставяне на безвъзмездни средства, за да се даде възможност за изграждане на капацитет на ЦОС, обслужващи публични и частни организации.

По отношение на готовността и реагирането при инциденти Комисията създаде краткосрочна програма за подпомагане на държавите членки чрез допълнително финансиране, отпуснато на ENISA, с цел незабавно укрепване на готовността и способностите за реагиране при големи киберинциденти. Обхванатите услуги включват действия за готовност, като например изпитването на проникване за критични субекти с цел установяване на уязвимости. С програмата също така се засилват възможностите за подпомагане на държавите членки в случай на сериозен инцидент, засягащ критични субекти. Изпълнението на тази краткосрочна програма от страна на ENISA е в ход и вече са получени относими ценни сведения, които са взети предвид при съставянето на настоящия регламент.

1.5.4. Съвместимост с многогодишната финансова рамка и евентуални полезни взаимодействия с други подходящи инструменти

Законодателният акт за киберсолидарност ще се основава на действията, които понастоящем се подкрепят от Съюза и държавите членки, за подобряване на ситуационната осведоменост и откриването на киберзаплахи, както и за реагиране на мащабни и трансгранични киберинциденти. Освен това инструментът е в съответствие с други рамки за управление на кризи, включително ИРПК, общата политика за сигурност и отбрана, включително екипите за бързо реагиране в областта на киберсигурността, и помощта, предоставяна от една държава членка на друга държава членка в контекста на член 42, параграф 7 от Договора за Европейския съюз. Новото предложение също така ще допълни и подкрепи структурите, разработени в рамките на други инструменти в областта на киберсигурността, като например Директива (ЕС) 2022/2555 (Директива МИС 2) или Регламент (ЕС) 2019/881 (Акт за киберсигурността).

1.5.5. Оценка на различните налични варианти за финансиране, включително възможностите за преразпределяне на средства

Управлението на областите на действие, възложени на ENISA, съответства на нейния съществуващ мандат и общи задачи. Тези области на действие може да

изискват специфични профили или нови задачи, но те могат да бъдат поети от съществуващите ресурси на ENISA чрез преразпределение или свързване на различни задачи. Понастоящем ENISA изпълнява краткосрочна програма, която беше създадена през 2022 г. от Комисията с цел незабавно укрепване на готовността и способностите за реагиране при големи киберинциденти. Обхванатите услуги включват възможности за оказване на помощ на държавите членки в случай на голям инцидент, засягащ критични субекти. Изпълнението на тази краткосрочна програма от страна на ENISA е в ход и вече са получени относими ценни сведения, които са взети предвид при съставянето на настоящия регламент. Ресурсите, отпуснати за краткосрочната програма, могат да бъдат използвани и в контекста на настоящия регламент.

1.6. Продължителност и финансово отражение на предложението/инициативата

☒ **ограничен срок на действие**

– ☒ в сила от датата на приемане на предложението за Регламент на Европейския парламент и на Съвета за укрепване на солидарността и способностите на Съюза за откриване, подготовка и реагиране при киберзаплахи и инциденти („законодателен акт за киберсолидарност“)

– ☒ финансово отражение от 2023 г. до 2027 г. за бюджетни кредити за поети задължения и от 2023 г. до 2031 г. за бюджетни кредити за плащания[34].

☐ **неограничен срок на действие**

– Изпълнение с период на започване на дейност от ГГГГ до ГГГГ,

– последван от функциониране с пълен капацитет.

1.7. Планирани методи на изпълнение на бюджета[35]

☒ **Пряко управление** от Комисията

– ☒ от нейните служби, включително от нейния персонал в делегациите на Съюза;

– ☐ от изпълнителните агенции.

☐ **Споделено управление** с държавите членки

☒ **Непряко управление** чрез възлагане на задачи по изпълнението на бюджета на:

– ☐ трети държави или на органите, определени от тях;

– ☐ международни организации и техните агенции (да се уточни);

– ☐ ЕИБ и Европейския инвестиционен фонд;

– ☒ органите, посочени в членове 70 и 71 от Финансовия регламент;

– ☐ публичноправни органи;

– ☐ частноправни органи със задължение за обществена услуга, доколкото предоставят подходящи финансови гаранции;

---

34 Действията в законодателния акт следва да бъдат подкрепени от следващата многогодишна финансова рамка.

35 Подробности във връзка с методите на изпълнение на бюджета и позоваванията на Финансовия регламент могат да бъдат намерени на уебсайта BUDGpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx

– ☐ органи, уредени в частното право на държава членка, на които е възложено осъществяването на публично-частно партньорство и които предоставят подходящи финансови гаранции;

– ☐ органи или лица, на които е възложено изпълнението на специфични дейности в областта на ОВППС съгласно дял V от ДЕС и които са посочени в съответния основен акт.

– *Ако е посочен повече от един метод на управление, да се поясни в частта „Забележки“.*

Забележки

Действията, свързани с европейския киберщит, ще бъдат изпълнявани от ЕССС. Докато Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността изгради капацитет за изпълнение на собствения си бюджет, Европейската комисия ще изпълнява действията в рамките на прякото управление от името на ЕССС. ЕССС може да избере субекти въз основа на покани за заявяване на интерес за участие в съвместна обществена поръчка за инструменти. ЕССС може да отпуска безвъзмездни средства за функционирането на тези инструменти. Освен това ЕССС може да отпуска безвъзмездни средства за действия за готовност в рамките на Механизма за действие при извънредни ситуации в областта на киберсигурността. Комисията носи цялостна отговорност за изпълнението на резерва за киберсигурност на ЕС. Комисията може да възложи функционирането и управлението на резерва за киберсигурност на ЕС, изцяло или частично, на ENISA посредством споразумения за финансов принос. Дейностите, възложени на ENISA с настоящия регламент, са в съответствие със съществуващия ѝ мандат. Тези дейности включват: i) подпомагане на групата за сътрудничество за МИС при разработването на действия за готовност в съответствие с оценките на риска; ii) подпомагане на Комисията при създаването и надзора на изпълнението на резерва за киберсигурност на ЕС, включително получаване и обработване на исканията за подкрепа; iii) разработване на образци за улесняване на подаването на искания за подкрепа и на специални споразумения, които да бъдат сключени между доставчика на услуги и потребителя, на когото се предоставя подкрепа в рамките на резерва за киберсигурност на ЕС; iv) преглед и оценка на заплахите, уязвимостите и действията за смекчаване на последиците по отношение на конкретен значителен или мащабен киберинцидент и изготвяне на доклади за него. Всички тези задачи се оценяват на около 7 ЕПРВ от съществуващите ресурси на ENISA, като се основават на експертния опит и подготвителната работа, която понастоящем се извършва от ENISA в рамките на пилотния проект за спешна подкрепа за готовност и реагиране при инциденти.

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

Да се посочат честотата и условията.

Комисията ще наблюдава изпълнението, прилагането и спазването на тези нови разпоредби, за да оцени тяхната ефективност. До четири години след датата на прилагането настоящия регламент Комисията представя на Европейския парламент и на Съвета доклад относно оценката и прегледа на настоящия регламент.

2.2. Системи за управление и контрол

2.2.1. Обосновка на предложените начини за управление, механизми за финансиране на изпълнението, начини за плащане и стратегия за контрол

С регламента се въвежда рамка за изпълнение на финансирането от ЕС с цел повишаване на киберустойчивостта чрез действия, подобряващи способностите за откриване, реагиране и възстановяване в случай на значителни и мащабни киберинциденти. Отделите в ГД „Съобщителни мрежи, съдържание и технологии“, отговарящи за областта на политиката, ще ръководят прилагането на директивата.

За да се отговори на новите задачи, е необходимо да се осигурят достатъчно ресурси за службите на Комисията. Изчислено е, че за прилагането на новия регламент ще са необходими 6 ЕПРВ (3 администратори (AD) и 3 договорно наети служители (CA), за да се обхванат следните задачи:

- Определяне на действия за готовност в съответствие с оценките на риска;
- Осигуряване на оперативна съвместимост между трансграничните платформи на ЦОС;
- Разработване на потенциални актове за изпълнение (два за ЦОС и два за Механизма за действие при извънредни ситуации в областта на киберсигурността);
- Управление на споразуменията за хостинг и използване на ЦОС;
- Създаване и управление на резерва за киберсигурност на ЕС, пряко или чрез споразумение за финансов принос към ENISA. В случай на споразумение за финансов принос към ENISA — разработване и надзор на изпълнението на споразумението за финансов принос по отношение на задачите, възложени на ENISA;
- Участие в консултативните групи, свикани от ENISA за преглед и оценка на значителни и мащабни киберинциденти, и изготвяне на доклади.

2.2.2. Информация относно установените рискове и системите за вътрешен контрол, създадени с цел намаляването им

Рискът, установен за европейския киберщит, е, че държавите членки не обменят достатъчно количество относима информация за киберзаплахи нито в рамките на трансграничните платформи за ЦОС, нито между трансграничните платформи и други съответни субекти на равнището на ЕС. За да се намалят тези рискове, финансирането ще се разпределя след покана за заявяване на интерес, при която държавите членки ще поемат ангажимент да споделят определен обем информация с равнището на ЕС. След това този ангажимент ще бъде формализиран в споразумение за хостинг и използване, което ще даде на ЕССС правомощия да извършва одити, за да се гарантира, че съвместно закупените инструменти и инфраструктура се използват в съответствие със споразумението. Ангажиментите за високо ниво на обмен на информация в рамките на трансграничните ЦОС ще бъдат формализирани в споразумение за консорциум.

Установено е, че за Механизма за действие при извънредни ситуации в областта на киберсигурността съществува риск ползвателите, участващи в механизма, да не предприемат достатъчно мерки, за да осигурят готовност в случай на кибератаки. Поради тази причина, за да могат да получат подкрепа от резерва за киберсигурност на ЕС, ползвателите са задължени да предприемат такива мерки за готовност. При подаване на искания за подкрепа до резерва за киберсигурност на ЕС ползвателите трябва да обяснят какви мерки вече са предприети за реагиране на инцидента, които ще бъдат взети предвид при оценката на исканията до резерва за киберсигурност на ЕС.

2.2.3. Оценка и обосновка на разходната ефективност на проверките (съотношение „разходи за контрол ÷ стойност на съответните управлявани фондове“) и оценка на очакваната степен на риска от грешки (при плащане и при приключване)

Тъй като правилата за участие в програмата „Цифрова Европа“, приложими за подкрепата в рамките на законодателния акт за киберсолидарност са сходни с тези, които Комисията ще използва в работните си програми, а групата на бенефициерите е със сходен рисков профил като тези на програмите под пряко управление, може да се очаква, че интервалът на грешката ще бъде подобен на предвидения от Комисията за програмата „Цифрова Европа“, т.е. че могат да се дадат разумни гаранции, че на годишна основа рискът от грешка в рамките на многогодишния разходен период е в диапазона 2—5 %, като крайната цел е да се постигне остатъчен процент на грешка, възможно най-близък до 2 % при приключването на многогодишните програми, след като се вземе предвид финансовото въздействие на всички одити и на мерките за корекции и възстановяване.

2.3. Мерки за предотвратяване на измами и нередности

Да се посочат съществуващите или планираните мерки за превенция и защита, например от стратегията за борба с измамите.

В случая с европейския киберщит ЕССС ще има правомощието да извършва одит, въз основа на достъп до информация и проверки на място, на съвместно закупените инструменти и инфраструктури в съответствие със споразумението за хостинг и използване, което ще бъде подписано между консорциума, осигуряващ хостинг, и ЕССС.

Съществуващите мерки за превенция на измами, приложими за институциите, органите, службите и агенциите на ЕС, ще покрият допълнителните бюджетни кредити, необходими за настоящия регламент.

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

3.1. Съответни функции от многогодишната финансова рамка и разходни бюджетни редове

- Съществуващи бюджетни редове

По реда на функциите от многогодишната финансова рамка и на бюджетните редове.

Функция от многогодишната финансова рамка	Бюджетен ред	Вид разход	Финансов принос			
	Номер	Многогод./ едногод.[36]	от държави от ЕАСТ [37]	от държави кандидатки и и потенциални кандидати [38]	от други трети държави	други целеви приходи
1	02 04 01 10 — програма „Цифрова Европа“ — Киберсигурност	Многогод.	ДА	ДА	НЕ	НЕ
1	02 04 01 11 — програма „Цифрова Европа“ — Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността	Многогод.	ДА	ДА	НЕ	НЕ
1	02 04 03 — програма „Цифрова Европа“ — Изкуствен интелект	Многогод.	ДА	ДА	НЕ	НЕ
1	02 04 04 — програма „Цифрова Европа“ — Умения	Многогод.	ДА	ДА	НЕ	НЕ
1	02 01 30 — Разходи за подкрепа на програмата „Цифрова Европа“	Едногод.	ДА	ДА	НЕ	НЕ

[36] Многогод. = многогодишни бюджетни кредити / Едногод. = едногодишни бюджетни кредити.
[37] ЕАСТ: Европейска асоциация за свободна търговия.
[38] Държави кандидатки и, ако е приложимо, потенциални кандидатки.

3.2. Очаквано финансово отражение на предложението върху бюджетните кредити

3.2.1. Обобщение на очакваното отражение върху бюджетните кредити за оперативни разходи

– ☐ Предложението/инициативата не налага използване на бюджетни кредити за оперативни разходи

– ☒ Предложението/инициативата налага използване на бюджетни кредити за оперативни разходи съгласно обяснението по-долу:

млн. евро (до 3-тия знак след десетичната запетая)

Функция от многогодишната финансова рамка	Номер	1 **Единен пазар, иновации и цифрова сфера**

Предложението няма да увеличи общия размер на поетите задължения по програмата „Цифрова Европа“. Всъщност приносът на настоящата инициатива е преразпределение на задълженията, произтичащи от СЦ 2 и СЦ 4, за да се подсили бюджетът на СЦ 3 и ЕССС. Всяко увеличение на поетите задължения по програмата „Цифрова Европа“, произтичащо от преразглеждането на МФР, би могло да се използва за целите на тази инициатива.

ГД „Съобщителни мрежи, съдържание и технологии“			Година **2025**	Година **2026**	Година **2027**	Година **2028+**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)			**ОБЩО**
○ Бюджетни кредити за оперативни разходи										
Бюджетен ред[39] 02.040110 (преразпределение от 02.0403 и 02.0404)	Поети задължения	(1a)	15 000	15 000	6000	p.m. — символичен запис				**36 000**
	Плащания	(2a)	15 000	15 000	6000					**36 000**
Бюджетен ред 02.040111.02	Поети	(1б)	13 000	23 000	28 000	p.m. —				**64 000**

[39] Съгласно официалната бюджетна номенклатура.

(преразпределение от 02.0403 и 02.0404)	задължения					символ ичен запис				
	Плащания	(2б)	8450	18 200	25 250	12 100				**64 000**
Бюджетни кредити за административни разходи, финансирани от пакета за определени програми[40]										
Бюджетен ред 02.0130		(3)	0,150	0,150	0,150	p.m. — символ ичен запис				0,450
ОБЩО бюджетни кредити за ГД „Съобщителни мрежи, съдържание и технологии“	Поети задължения	=1а+1б +3	**28 150**	**38 150**	**34 150**	**p.m. — символ ичен запис**				**100 450**
	Плащания	=2а+2б +3	**23 600**	**33 350**	**31 400**	**12 100**				**100 450**

○ ОБЩО бюджетни кредити за оперативни разходи	Поети задължения	(4)	28 000	38 000	34 000	p.m. — символ ичен запис				**100 000**
	Плащания	(5)	23 450	33 200	31 250	12 100				**100 000**
○ ОБЩО бюджетни кредити за административни разходи, финансирани от пакета за определени програми		(6)	0,150	0,150	0,150	p.m. — символ ичен запис				**0,450**
ОБЩО бюджетни кредити	Поети	=4+6	**28 150**	**38 150**	**34 150**	**p.m. — симво**				**100 450**

[40] Техническа и/или административна помощ и разходи в подкрепа на изпълнението на програми и/или дейности на ЕС (предишни редове ВА), непреки научни изследвания, преки научни изследвания.

за ФУНКЦИЯ 1 от многогодишната финансова рамка	задължения					**личен запис**				
	Плащания	=5+6	**23 600**	**33 350**	**31 400**	**12 100**				**100 450**

Ако предложението/инициативата има отражение върху повече от една оперативна функция, повторете частта по-горе:

○ ОБЩО бюджетни кредити за оперативни разходи (всички оперативни функции)	Поети задължения	(4)	28 000	38 000	34 000	p.m. — символичен запис				**100 000**
	Плащания	(5)	23 450	33 200	31 250	12 100				**100 000**
ОБЩО бюджетни кредити за административни разходи, финансирани от пакета за определени програми (всички оперативни функции)		(6)	0,150	0,150	0,150					**0,450**
ОБЩО бюджетни кредити за ФУНКЦИИ 1—6 от многогодишната финансова рамка (Референтна стойност)	Поети задължения	=4+6	**28 150**	**38 150**	**34 150**	**p.m. — символичен запис**				**100 450**
	Плащания	=5+6	**23 600**	**33 350**	**31 400**	**12 100**				**100 450**

Функция от многогодишната финансова рамка	**7**	„Административни разходи“

Тази част следва да бъде попълнена, като се използва таблицата за бюджетни данни от административно естество,които първо се въвеждат в приложението към законодателната финансова обосновка (приложение 5 към Решението на Комисията относно вътрешните правила за изпълнението на раздела за Комисията от общия бюджет на Европейския съюз), което се качва в DECIDE за провеждането на вътрешни консултации между службите.

млн. евро (до 3-тия знак след десетичната запетая)

		Година **2025**	Година **2026**	Година **2027**	Година **2028+**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)			**ОБЩО**
ГД: „Съобщителни мрежи, съдържание и технологии“									
○ Човешки ресурси		0,786	0,786	0,786	p.m. — символичен запис				**2,358**
○ Други административни разходи		0,035	0,035	0,035	p.m. — символичен запис				**0,105**
ОБЩО ГД „Съобщителни мрежи, съдържание и технологии“	Бюджетни кредити	**0,821**	**0,821**	**0,821**					**2,463**

ОБЩО бюджетни кредити по ФУНКЦИЯ 7 от многогодишната финансова рамка	(Общо поети задължения = Общо плащания)	**0,821**	**0,821**	**0,821**					**2,463**

млн. евро (до 3-тия знак след десетичната запетая)

		Година **2025**	Година **2026**	Година **2027**	Година **2028+**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)			**ОБЩО**
ОБЩО бюджетни кредити за ФУНКЦИИ 1—7 от многогодишната финансова рамка	Поети задължения	**28 971**	**38 971**	**34 971**	**p.m. — символичен запис**				**102 913**
	Плащания	**24 421**	**34 171**	**32 221**	**12 100**				**102 913**

3.2.2. Очакван резултат, финансиран с бюджетни кредити за оперативни разходи

Бюджетни кредити за поети задължения, в млн. евро (до 3-тия знак след десетичната запетая)

Да се посочат целите и резултатите			Година **N**		Година **N+1**		Година **N+2**		Година **N+3**		Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)						**ОБЩО**	
	РЕЗУЛТАТИ																	
⇩	Вид[41]	Среден разход	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Общо бр.	Общо разходи
СПЕЦИФИЧНА ЦЕЛ № 1[42]…																		
— Резултат																		
— Резултат																		
— Резултат																		

41 Резултатите са продуктите и услугите, които ще бъдат доставени (напр.: брой финансирани студентски обмени, брой километри изградени пътища и др.).

42 Описана в точка 1.4.2. „Специфични цели...“

Междинен сбор за специфична цел № 1																
СПЕЦИФИЧНА ЦЕЛ № 2...																
— Резултат																
Междинен сбор за специфична цел № 2																
ОБЩО																

3.2.3. Обобщение на очакваното отражение върху бюджетните кредити за административни разходи

– ☐ Предложението/инициативата не налага използване на бюджетни кредити за административни разходи

– ☒ Предложението/инициативата налага използване на бюджетни кредити за административни разходи съгласно обяснението по-долу:

млн. евро (до 3-тия знак след десетичната запетая)

	Година 2025	Година 2026	Година 2027	Година N+3	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)			**ОБЩО**
ФУНКЦИЯ 7 от многогодишната финансова рамка								
Човешки ресурси	0,786	0,786	0,786					**2,358**
Други административни разходи	0,035	0,035	0,035					**0,105**
Междинен сбор за ФУНКЦИЯ 7 от многогодишната финансова рамка	**0,821**	**0,821**	**0,821**					**2,463**

Извън ФУНКЦИЯ 7[43] от многогодишната финансова рамка								
Човешки ресурси								
Други разходи с административен характер	0,150	0,150	0,150					**0,450**
Междинен сбор извън ФУНКЦИЯ 7 от многогодишната финансова рамка	**0,150**	**0,150**	**0,150**					**0,450**

ОБЩО	**0,971**	**0,971**	**0,971**					**2,913**

Бюджетните кредити, необходими за човешки ресурси и други разходи с административен характер, ще бъдат покрити от бюджетни кредити на ГД, които вече са определени за управлението на действието и/или които са преразпределени в рамките на ГД, при необходимост заедно с допълнително отпуснати ресурси, които могат да

[43] Техническа и/или административна помощ и разходи в подкрепа на изпълнението на програми и/или дейности на ЕС (предишни редове ВА), непреки научни изследвания, преки научни изследвания.

бъдат предоставени на управляващата ГД в рамките на годишната процедура за отпускане на средства и като се имат предвид бюджетните ограничения.

3.2.3.1. Очаквани нужди от човешки ресурси

– ☐ Предложението/инициативата не налага използване на човешки ресурси

– ☒ Предложението/инициативата налага използване на човешки ресурси съгласно обяснението по-долу:

Оценката се посочва в еквиваленти на пълно работно време

		Година **2025**	Година **2026**	Година 2027	Година **N+3**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)		
○ Длъжности по щатното разписание (длъжностни лица и срочно наети служители)								
20 01 02 01 (Централа и представителства на Комисията)		3	3	3				
20 01 02 03 (Делегации)								
01 01 01 01 (Непреки научни изследвания)								
01 01 01 11 (Преки научни изследвания)								
Други бюджетни редове (да се посочат)								
○ Външен персонал (в еквивалент на пълно работно време: ЕПРВ)[44]								
20 02 01 (ДНП, КНЕ, ПНА от „общия финансов пакет“)		3	3	3				
20 02 03 (ДНП, МП, КНЕ, ПНА и МЕД в делегациите)								
XX 01 xx **yy zz** [45]	— в централата							
	— в делегациите							
01 01 01 02 (ДНП, КНЕ, ПНА — Непреки научни изследвания)								
01 01 01 12 (ДНП, КНЕ, ПНА — Преки научни изследвания)								
Други бюджетни редове (да се посочат)								
ОБЩО		**6**	**6**	**6**				

XX е съответната област на политиката или бюджетен дял.

Нуждите от човешки ресурси ще бъдат покрити от персонала на ГД, на който вече е възложено управлението на дейността и/или който е преразпределен в рамките на ГД, при необходимост заедно с всички допълнителни отпуснати ресурси, които могат да бъдат предоставени на управляващата ГД в рамките на годишната процедура за отпускане на средства и като се имат предвид бюджетните ограничения.

Описание на задачите, които трябва да се изпълнят:

Длъжностни лица и срочно наети служители	- Определяне на действия за готовност в съответствие с оценките на риска (член 11) - Разработване на потенциални актове за изпълнение (два за ЦОС и два за Механизма за действие при извънредни ситуации в областта на киберсигурността); - Управление на споразуменията за хостинг и използване на ЦОС;

44 ДНП = договорно нает персонал; МП = местен персонал; КНЕ = командирован национален експерт; ПНА = персонал, нает чрез агенции за временна заетост; МЕД = младши експерт в делегация.

45 Подтаван за външния персонал, покрит с бюджетните кредити за оперативни разходи (предишни редове ВА).

	- Създаване и управление на резерва за киберсигурност на ЕС, пряко или чрез споразумение за финансов принос към ENISA.
Външен персонал	Под надзора на длъжностно лице: - Определяне на действия за готовност в съответствие с оценките на риска (член 11) - Разработване на потенциални актове за изпълнение (два за ЦОС и два за Механизма за действие при извънредни ситуации в областта на киберсигурността); - Управление на споразуменията за хостинг и използване на ЦОС; - Създаване и управление на резерва за киберсигурност на ЕС, пряко или чрез споразумение за финансов принос към ENISA.

3.2.4. Съвместимост с настоящата многогодишна финансова рамка

Предложението/инициативата:

– ☒ може да се финансира изцяло чрез преразпределяне на средства в рамките на съответната функция от многогодишната финансова рамка (МФР).

Обяснете какво препрограмиране е необходимо, като посочите съответните бюджетни редове и суми. Моля, представете таблица в Excel, ако е необходимо голямо препрограмиране.

	2023	2024	2025	2026	2027	общо
СЦ 1	16 232 897	20 528 765	17 406 899	16 223 464	10 022 366	80 414 391
СЦ 2 — първоначално	226 316 819	295 067 000	195 649 000	221 809 000	246 608 000	1 185 449 819
За инициативата в областта на киберсигурността			18 000 000	28 000 000	19 000 000	65 000 000
НОВА СЦ 2	**226 316 819**	**295 067 000**	**177 649 000**	**193 809 000**	**227 608 000**	**1 120 449 819**
СЦ 3 DB 24	24 361 553	35 596 172	3 638 000	3 638 000	11 175 000	78 408 725
От СЦ 2—СЦ 4			15 000 000	15 000 000	6 000 000	36 000 000
Нова СЦ 3	**24 361 553**	**35 596 172**	**18 638 000**	**18 638 000**	**17 175 000**	**114 408 725**
ЕССС — първоначално	176 222 303	208 374 879	104 228 130	90 704 986	84 851 497	664 381 795
От СЦ 2—СЦ 4			13 000 000	23 000 000	28 000 000	64 000 000
ЕССС — Ново	**176 222 303**	**208 374 879**	**117 228 130**	**113 704 986**	**112 851 497**	**728 381 795**
СЦ 4 — първоначално	66 902 708	64 892 032	56 577 977	70 477 245	72 107 201	330 957 163
За инициативата в областта на киберсигурността			10 000 000	10 000 000	15 000 000	35 000 000
НОВА СЦ 4	**66 902 708**	**64 892 032**	**46 577 977**	**60 477 245**	**57 107 201**	**295 957 163**

– ☐ налага да се използват неразпределеният марж под съответната функция от МФР и/или специалните инструменти, предвидени в Регламента за МФР.

Обяснете какво е необходимо, като посочите съответните функции, бюджетни редове и суми и инструментите, които се предлага да бъдат използвани.

– ☐ налага преразглеждане на МФР.

Обяснете какво е необходимо, като посочите съответните функции, бюджетни редове и суми.

3.2.5. Финансов принос от трети страни

Предложението/инициативата:

– ☒ не предвижда съфинансиране от трети страни

– ☐ предвижда следното съфинансиране от трети страни, като оценките са дадени по-долу:

Бюджетни кредити в млн. евро (до третия знак след десетичната запетая)

	Година **N**[46]	Година **N+1**	Година **N+2**	Година **N+3**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)			Общо
Да се посочи съфинансиращият орган								
ОБЩО съфинансирани бюджетни кредити								

[46] Година N е годината, през която започва да се изпълнява предложението/инициативата. Моля, заменете буквата „N“ с очакваната първа година от изпълнението (например: 2021). Същото за следващите години.

3.3. Очаквано отражение върху приходите

– ☒ Предложението/инициативата няма финансово отражение върху приходите.

– ☐ Предложението/инициативата има следното финансово отражение:

  – ☐ върху собствените ресурси

  – ☐ върху другите приходи

  – моля, посочете дали приходите са записани по разходни бюджетни редове☐

млн. евро (до 3-тия знак след десетичната запетая)

Приходен бюджетен ред:	Налични бюджетни кредити за текущата финансова година	Отражение на предложението/инициативата[47]						
		Година **N**	Година **N+1**	Година **N+2**	Година **N+3**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)		
Статия …….								

За целевите приходи да се посочат съответните разходни бюджетни редове.

[…]

Други забележки (например метод/формула за изчисляване на отражението върху приходите или друга информация).

[…]

[47] Що се отнася до традиционните собствени ресурси (мита, налози върху захарта), посочените суми трябва да бъдат нетни, т.е. брутни суми, от които са приспаднати 20 % за разходи по събирането.