ЕВРОПЕЙСКИ СЪЮЗ

ЕВРОПЕЙСКИ ПАРЛАМЕНТ **СЪВЕТ**

Брюксел, 19 декември 2024 г.
(OR. en)

2023/0109(COD)
LEX 2422

PE-CONS 94/1/24
REV 1

CYBER 208
TELECOM 218
CADREFIN 109
FIN 595
BUDGET 47
IND 328
JAI 1084
MI 633
DATAPROTECT 247
RELEX 881
CODEC 1588

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, И ЗА ИЗМЕНЕНИЕ НА РЕГЛАМЕНТ (ЕС) 2021/694 (ЗАКОНОДАТЕЛЕН АКТ В ОБЛАСТТА НА КИБЕРСОЛИДАРНОСТТА)

РЕГЛАМЕНТ (ЕС) 2024/...
НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

от 19 декември 2024 година

за определяне на мерки за укрепване на солидарността и способностите на Съюза за откриване, подготовка и реагиране при киберзаплахи и инциденти, и за изменение на Регламент (ЕС) 2021/694
(Законодателен акт в областта на киберсолидарността)

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[4],

---

1 Становище от 18 април 2023 г. (все още непубликувано в Официален вестник).
2 ОВ C 349, 29.9.2023 г., стр. 167.
3 ОВ C, C/2024/1049, 9.2.2024 г., ELI: http://data.europa.eu/eli/C/2024/1049/oj.
4 Позиция на Европейския парламент от 24 април 2024 г. (все още непубликувана в Официален вестник) и решение на Съвета от 19 декември 2024 г.

като имат предвид, че:

(1) Всички сектори на икономиката и обществото използват и се осланят на информационните и комуникационните технологии като съществен компонент на дейността си, с оглед на все по-голямата взаимосвързаност и взаимозависимост на публичните администрации, предприятията и гражданите на държавите членки отвъд секторните и териториалните граници, като едновременно се откриват възможни уязвимости.

(2) Мащабът, честотата и въздействието на киберинцидентите, включително атаките по веригата на доставки с цел кибершпионаж, софтуер за изнудване или смущения, се увеличават на равнището на Съюза и на световно равнище. Те представляват съществена заплаха за функционирането на мрежовите и информационните системи. С оглед на бързо променящата се картина на заплахите, заплахата от възможни мащабни киберинциденти, причиняващи значителни смущения или вреди на критичните инфраструктури, изисква повишена готовност на рамката за киберсигурност на Съюза. Тази заплаха надхвърля рамките на агресивната война на Русия срещу Украйна и е вероятно да продължи да съществува, като се има предвид многообразието от участници, замесени в настоящото геополитическо напрежение. Такива инциденти могат да възпрепятстват предоставянето на обществени услуги, тъй като кибератаките често са насочени към местни, регионални или национални обществени услуги и инфраструктури, като местните органи са особено уязвими, включително поради ограничените си ресурси. Те също могат да засегнат осъществяването на икономически дейности, включително в сектори с висока степен на критичност или други критични сектори, да доведат до значителни финансови загуби, да нарушат доверието на потребителите, да нанесат сериозни вреди на икономиката и демократичните системи в Съюза и дори да имат застрашаващи здравето или живота последици. Освен това киберинцидентите са непредвидими, тъй като често възникват и се развиват бързо, не се ограничават в рамките на определен географски район и се случват едновременно или се разпространяват мигновено в много държави. Важно е да има координирано сътрудничество между публичния сектор, частния сектор, академичните среди, гражданското общество и медиите.

(3) Необходимо е да се укрепи конкурентната позиция на промишлеността и услугите в Съюза в рамките на цифровата 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. Необходимо е да се повиши устойчивостта на гражданите, предприятията, и по-специално микропредприятията, малките и средните предприятия, както и новосъздадените предприятия 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, както и изграждане на капацитет за развитие на умения за киберсигурност, които ще подпомогнат по-бързото откриване и по-бързото реагиране при киберзаплахи и инциденти. Освен това държавите членки се нуждаят от помощ, за да се подготвят и реагират по-добре на значителни киберинциденти и мащабни киберинциденти, както и от помощ за първоначално възстановяване в случай на такива киберинциденти. Надграждайки съществуващите структури и тясното сътрудничество с тях, Съюзът следва също така да увеличи способностите си в тези области, по-специално 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 рисковете, по-специално Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета[5], директиви 2013/40/ЕС[6] и (ЕС) 2022/2555[7] на Европейския парламент и на Съвета и Препоръка (ЕС) 2017/1584 на Комисията[8]. В допълнение в препоръката на Съвета от 8 декември 2022 г. относно координиран подход на равнището на Съюза за укрепване на устойчивостта на критичната инфраструктура държавите членки се приканват да предприемат мерки и да си сътрудничат помежду си, с Комисията и с други съответни публични органи, както и със съответните субекти, за да повишат устойчивостта на критичната инфраструктура, използвана за предоставяне на основни услуги на вътрешния пазар.

---

5 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).

6 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.).

7 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).

8 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).

(5) Нарастващите киберрискове и цялостната сложна картина на заплахите, с ясен риск от бързо разпространение на инциденти от една държава членка към други държави членки и от трета държава към Съюза, изискват да се засили солидарността на равнището на Съюза за по-добро откриване, подготовка, реагиране и възстановяване от киберзаплахи и инциденти, по-специално като се укрепи капацитета на съществуващите структури. Освен това в заключенията на Съвета от 23 май 2022 г. относно установяването на позицията на Европейския съюз в киберпространството Комисията беше приканена да представи предложение за нов фонд за реагиране при извънредни ситуации в областта на киберсигурността.

(6) В съвместното съобщение на Комисията и на върховния представител на Съюза по въпросите на външните работи и политиката на сигурност от 10 ноември 2022 г. до Европейския парламент и до Съвета относно политиката на ЕС за киберотбрана беше обявена инициатива на ЕС за киберсолидарност с цел 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 създаване на киберрезерв на равнището на ЕС с услуги от надеждни 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 предотвратяване и реагиране при значителни киберинциденти и мащабни киберинциденти. Поради това следва да бъде създадена общоевропейска мрежа от киберхъбове (наричана по-нататък „Европейска система за предупреждение в областта на киберсигурността“) за изграждане на координирани способности за откриване и ситуационна осведоменост, подсилване на способностите на Съюза за откриване на заплахи и споделяне на информация; следва да бъде създаден Механизъм за действие при извънредни ситуации в областта на киберсигурността, който при искане от тяхна страна да подпомага държавите членки при подготовката, реагирането, смекчаването на въздействието и първоначалното възстановяване след значителни киберинциденти и мащабни киберинциденти и да подпомага други ползватели при реагиране на значителни киберинциденти и равностойни на мащабни киберинциденти; и следва да бъде създаден Европейски механизъм за преглед на киберинциденти, чрез който да се разглеждат и оценяват конкретни значителни киберинциденти или мащабни киберинциденти. Действията, предприети съгласно настоящия регламент следва да се извършват при надлежно зачитане на компетенциите на държавите членки и следва да допълват, а не да дублират дейностите, извършвани от мрежата на ЕРИКС, Европейската мрежа на организациите за връзка при киберкризи (EU-CyCLONe) или групата за сътрудничество (наричана по-нататък „Групата за сътрудничество за МИС“), всичките създадени съгласно Директива (ЕС) 2022/2555. Тези действия не засягат членове 107 и 108 от Договора за функционирането на Европейския съюз (ДФЕС).

(8) За постигането на тези цели е необходимо да се измени Регламент (ЕС) 2021/694 на Европейския парламент и на Съвета[9] 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 Европейската система за предупреждение в областта на киберсигурността и Механизма за действие при извънредни ситуации в областта на киберсигурността в рамките на специфична цел 3 на 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 киберзаплахите, както и към засилване на трансграничното сътрудничество и координация в областта на киберсигурността. Европейската система за предупреждение в областта на киберсигурността би могла да играе важна роля в подпомагането на държавите членки при предвиждането на и защитата срещу киберзаплахи, а Резервът за киберсигурност на ЕС би могъл да има значима роля при подпомагането на държавите членки, институциите, органите, службите и агенциите на Съюза и асоциираните към програмата „Цифрова Европа“ трети държави при реагирането и смекчаването на последиците от значителни киберинциденти, мащабни киберинциденти и равностойни на мащабни киберинциденти. Тези последици биха могли да включват значителни материални или нематериални щети и сериозни рискове за обществената сигурност и безопасност. С оглед на специфичните роли, които биха могли да изпълняват Европейската система за предупреждение в областта на киберсигурността и Резервът за киберсигурност на ЕС, с настоящия регламент следва да се измени Регламент (ЕС) 2021/694 по отношение на участието на правни субекти, които са установени в Съюза, но се контролират от трети държави, когато съществува реален риск необходимите и достатъчни инструменти, инфраструктури и услуги или технологии, експертен опит и капацитет да не са налични в Съюза и ползите от включването на такива субекти да надхвърлят риска за сигурността. Следва да бъдат установени конкретните условия, при които може да бъде отпусната финансова подкрепа за действия за внедряване на Европейската система за предупреждение в областта на киберсигурността и Резерва за киберсигурност на ЕС, както и 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] 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).

(9) От жизненоважно значение е да се укрепи реакцията на Съюза на киберзаплахи и сътрудничеството при инциденти с международните организации, както и с надеждни единомислещи международни партньори. В този контекст под надеждни единомислещи международни партньори следва да се разбират държавите, които споделят принципите, вдъхновили създаването на Съюза, а именно демокрацията, върховенството на закона, универсалността и неделимостта на правата на човека и на основните свободи, зачитане на човешкото достойнство, принципите на равенство и солидарност и зачитане на принципите на Устава на Организацията на обединените нации и на международното право, и които не подкопават основните интереси на Съюза или на неговите държави членки в областта на сигурността. Това сътрудничество би могло да бъде от полза и по отношение на действията, предприети съгласно настоящия регламент, по-специално Европейската система за предупреждение в областта на киберсигурността и Резерва за киберсигурност на ЕС. В Регламент (ЕС) 2021/694, при определени условия за наличност и сигурност, следва да се предвиди участието в поръчки за Европейската система за предупреждение в областта на киберсигурността и Резерва за киберсигурност на ЕС да бъде отворено за правни субекти, контролирани от трети държави, при спазване на изискванията за сигурност. При оценката на риска за сигурността от отварянето на участието в поръчки по този начин е важно да се вземат предвид принципите и ценностите, които Съюзът споделя с единомислещи международни партньори, когато тези принципи и ценности са свързани с основни интереси на Съюза в областта на сигурността. Освен това, когато такива изисквания за сигурност се разглеждат съгласно Регламент (ЕС) 2021/694, могат да бъдат взети предвид няколко елемента, като например корпоративната структура и процеса на вземане на решения на даден субект, сигурността на данните и класифицираната или чувствителната информация и да се гарантира, че резултатите от действието не подлежат на контрол или ограничения от страна на трети държави, които не отговарят на условията за допустимост.

(10) 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“. Конкретни условия за участие по отношение на всяко действие трябва да бъдат предвидени в съответните работни програми в съответствие с Регламент (ЕС) 2021/694.

(11) Към настоящия регламент се прилагат хоризонталните финансови правила, приети от Европейския парламент и Съвета на основание член 322 от ДФЕС. Тези правила са установени в Регламент (ЕС, Евратом) 2024/2509 на Европейския парламент и на Съвета[10] 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].

---

[10] Регламент (ЕС, Евратом) 2024/2509 на Европейския парламент и на Съвета от 23 септември 2024 г. за финансовите правила, приложими за общия бюджет на Съюза (ОВ L, 2024/2509, 26.9.2024 г., ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

[11] Регламент (ЕС, Евратом) 2020/2092 на Европейския парламент и на Съвета от 16 декември 2020 г. относно общ режим на обвързаност с условия за защита на бюджета на Съюза (ОВ L 433 I, 22.12.2020 г., стр. 1, ELI: https://eur-lex.europa.eu/eli/reg/2020/2092/oj?locale=bg).

(12) Въпреки че мерките за предотвратяване и готовност са от съществено значение за повишаване на устойчивостта на Съюза при справянето със значителни киберинциденти, мащабни киберинциденти и равностойни на мащабни киберинциденти, настъпването, моментът и мащабът на такива инциденти по своята същност са непредвидими. Финансовите ресурси, необходими за осигуряване на адекватна реакция, могат да варират значително през различни години и следва да могат да бъдат предоставени незабавно. Ето защо съчетаването на бюджетния принцип на предвидимост с необходимостта от бързо реагиране при възникването на нови потребности изисква адаптиране на финансовото изпълнение на работните програми. Поради това е целесъобразно да се разреши пренасяне на неизползваните бюджетни кредити, но единствено до следващата година и единствено за Резерва за киберсигурност на ЕС и действията за подпомагане на взаимопомощта, в допълнение към пренасянето на бюджетни кредити, разрешени съгласно член 12, параграф 4 от Регламент (ЕС, Евратом) 2024/2509.

(13) С оглед на по-ефективната превенция, оценяване, реагиране и възстановяване от 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. Проактивният подход за идентифициране, смекчаване и предотвратяване на киберзаплахи включва повишен капацитет за по-добро откриване на киберзаплахи. Европейската система за предупреждение в областта на киберсигурността следва да се състои от няколко оперативно съвместими трансгранични киберхъба, всеки от които обединява три или повече национални киберхъба. Тази инфраструктура следва да обслужва националните интереси и нуждите на Съюза в областта на киберсигурността, като използва най-съвременни технологии за авангардно събиране на относими данни и информация, анонимизирани, когато е целесъобразно, и инструменти за анализ, да подобрява координираните способности за откриване на киберзаплахи и управление на киберинциденти и осигурява ситуационна осведоменост в реално време. Тази инфраструктура следва да служи за подобряване на състоянието на киберсигурността чрез увеличаване на откриването, обобщаването и анализа на данни и информация с цел предотвратяване на киберзаплахи и инциденти и по този начин да допълва и подпомага субектите и мрежите на Съюза, отговарящи за управлението на киберкризи в Съюза, по-специално EU-CyCLONe.

(14) Участието в Европейската система за предупреждение в областта на киберсигурността е доброволно за държавите членки. Всяка държава членка следва да определи единен субект на национално равнище, натоварен със задачата да координира дейностите по откриване на киберзаплахи в тази държава членка. Тези национални киберхъбове следва да действат като отправна точка и портал на национално равнище за участие в Европейската система за предупреждение в областта на киберсигурността 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. Националните киберхъбове биха могли да засилят сътрудничеството и споделянето на информация между публичните и частните субекти и също така да подкрепят обмена на съответни данни и информация със съответните секторни и междусекторни общности, включително съответните промишлени центрове за споделяне на информация и анализ (ISAC). Тясното и координирано сътрудничество между публичните и частните субекти е от основно значение за укрепването на киберустойчивостта. Такова сътрудничество е особено ценно в контекста на споделянето на разузнавателна информация за киберзаплахи с цел подобряване на активната киберзащита. Като част от това сътрудничество и споделяне на информация националните киберхъбове биха могли да искат и получават конкретна информация. Тези национални киберхъбове не са нито задължени, нито разполагат с правомощия по силата на настоящия регламент да налагат изпълнението на такива искания. Когато е целесъобразно и в съответствие с правото на Съюза и с националното право, исканата или получената информация може да включва телеметрични, сензорни и регистрационни данни от субекти, като например доставчици на управлявани услуги за сигурност, които извършват дейност в сектори с висока степен на критичност или в други сектори от критично значение в тази държава членка, за да се подобри бързото откриване на потенциални киберзаплахи и инциденти на по-ранен етап, като по този начин се подобри ситуационната осведоменост. Ако националният киберхъб не е компетентният орган, определен или създаден от съответната държава членка съгласно член 8, параграф 1 от Директива (ЕС) 2022/2555, от решаващо значение е той да се координира с този компетентен орган във връзка с искания за и получаване на такива данни.

(15) Като част от Европейската система за предупреждение в областта на киберсигурността следва да бъдат създадени трансгранични киберхъбове. Тези трансгранични киберхъбове следва да обединяват национални киберхъбове от поне три държави членки, за да гарантират, че могат да се постигнат всички ползи от трансграничното откриване на заплахи и от споделянето и управлението на информация. Общата цел на трансграничните киберхъбове 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 споделянето на относима информация, анонимизирана, когато е целесъобразно, в доверителна и сигурна среда, 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 и сигурна среда. Трансграничните киберхъбове следва да осигурят нов допълнителен капацитет, който да надгражда и допълва съществуващите ЦОС, ЕРИКС и други съответни участници, включително мрежата на ЕРИКС.

(16) Държава членка, избрана от Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността (ЕССС), създаден с Регламент (ЕС) 2021/887 на Европейския парламент и на Съвета[12], след покана за изразяване на интерес за създаване или повишаване на капацитета на национален киберхъб, следва да закупи съвместно с ЕССС съответните инструменти, инфраструктура или услуги. Такава държава членка следва да отговаря на условията за получаване на безвъзмездни средства за експлоатация на инструментите, инфраструктурата или услугите. Консорциум, осигуряващ хостинг, състоящ се от най-малко три държави членки, избрани от ЕССС, след покана за изразяване на интерес за създаване или повишаване на капацитета на трансграничен киберхъб. следва да закупи съответните инструменти, инфраструктури и услуги съвместно с ЕССС. Консорциумът, осигуряващ хостинг, следва да отговаря на условията за получаване на безвъзмездни средства за експлоатация на инструментите, инфраструктурата или услугите. Процедурата за възлагане на поръчки за закупуване на съответните инструменти, инфраструктура или услуги следва да се проведе съвместно от ЕССС и съответните възлагащи органи на държавите членки, избрани след тези покани за изразяване на интерес. Процедурата за възлагане следва да бъде в съответствие с член 168, параграф 2 от Регламент (ЕС, Евратом) 2024/2509 и финансовите правила на ЕССС. Поради това частните субекти не следва да отговарят на критериите за участие в поканите за изразяване на интерес за съвместно закупуване на инструменти, инфраструктура или услуги съвместно с ЕССС или за получаване на безвъзмездни средства за експлоатацията на тези инструменти, инфраструктура или услуги. Държавите членки обаче следва да могат да включват частни субекти в създаването, подобряването и функционирането на своите национални киберхъбове и трансграничен киберхъб по други начини, които считат за подходящи, в съответствие с правото на Съюза и националното право. Частните субекти също биха могли да отговарят на условията за получаване на финансиране от Съюза съгласно Регламент (ЕС) 2021/887 с цел предоставяне на подкрепа на националните киберхъбове.

---

12 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, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

(17) За да се подобри откриването на киберзаплахи и ситуационната осведоменост в Съюза, държава членка, която след покана за изразяване на интерес е избрана да създаде или повиши капацитета на национален киберхъб, следва да се ангажира да кандидатства за участие в трансграничен киберхъб. Ако държава членка не е участник в трансграничен киберхъб в срок от две години от датата, на която са придобити инструментите, инфраструктурата или услугите или на която е получила безвъзмездни средства, в зависимост от това кое от двете събития настъпи първо, тя не следва да отговаря на критериите за допълнително подпомагане от Съюза в рамките на Европейската система за предупреждение в областта на киберсигурността за повишаване на капацитета на своя национален киберхъб. В такива случаи субекти от държавите членки все още могат да участват в покани за изразяване на интерес по други теми в рамките на програмата „Цифрова Европа“ или други програми за финансиране на Съюза, включително покани за изразяване на интерес във връзка с капацитет за откриване на киберзаплахи и споделяне на информация, при условие че тези субекти отговарят на критериите за допустимост, установени в програмите.

(18) ЕРИКС обменят информация в рамките на мрежата на ЕРИКС в съответствие с Директива (ЕС) 2022/2555. Европейската система за предупреждение в областта на киберсигурността следва да представлява нов капацитет, който допълва мрежата на ЕРИКС, като допринася за изграждането на ситуационна осведоменост на Съюза и позволява укрепването на капацитета на мрежата на ЕРИКС. Трансграничните киберхъбове следва да се координират и да си сътрудничат тясно с мрежата на ЕРИКС. Те следва да действат чрез обединяване на данни и споделяне на относима информация, анонимизирана, когато е целесъобразно, относно киберзаплахите от публични и частни субекти, повишават стойността на тези данни и информация чрез експертен анализ и съвместно придобити инфраструктури и най-съвременни инструменти и принос за технологичния суверенитет на Съюза, неговата отворена стратегическа автономност, конкурентоспособност и устойчивост, както и за развитието на способностите на Съюза.

(19) Трансграничните киберхъбове следва да действат като централно звено, позволяващо широко обединяване на относимите данни и разузнавателната информация за киберзаплахите, и да дават възможност за разпространение на информация за заплахите сред голям и разнообразен набор от заинтересовани страни, като екипи за незабавно реагиране при компютърни инциденти (CERT), ЕРИКС, ISAC и оператори на критични инфраструктури. Членовете на консорциума, осигуряващ хостинг, следва да посочат в споразумението за консорциум съответната информация, която следва да се споделя между участниците в съответния трансграничен киберхъб. Информацията, която се обменя между участниците в трансграничен киберхъб, може да включва например данни от мрежи и сензори, разузнавателни сведения за заплахи, показатели за компрометиране на системите и контекстуална информация за инциденти, киберзаплахи, ситуации, близки до инциденти, уязвимости, техники и процедури, злонамерени тактики, специфична информация за участниците в заплахите, предупреждения в областта на киберсигурността и препоръки относно конфигурацията на инструментите за киберсигурност за откриване на кибератаки. Освен това трансграничните киберхъбове следва да сключват и споразумения за сътрудничество между тях. В тези споразумения за сътрудничество следва по-специално да се определят принципите за споделяне на информация и оперативна съвместимост. Техните клаузи относно оперативната съвместимост, по-конкретно форматите и протоколите за споделяне на информация, следва да се ръководят от и следователно да приемат за отправна точка насоките за оперативна съвместимост, издадени от Агенцията на Европейския съюз за киберсигурност, създадена с Регламент (ЕС) 2019/881 (ENISA). Тези насоки следва да бъдат издадени бързо, за да се гарантира, че трансграничните киберхъбове могат да ги вземат предвид на ранен етап. Те следва да се ръководят от международните стандарти и най-добрите практики и функционирането на всички установени трансгранични киберхъбове.

(20) Трансграничните киберхъбове и мрежата на ЕРИКС следва да си сътрудничат тясно, за да осигурят полезни взаимодействия и допълване на дейности. За тази цел те следва да постигнат съгласие по процедурни договорености за сътрудничество и споделяне на съответната информация. Това би могло да включва споделяне на важна информация относно киберзаплахи и значителни киберинциденти и гарантиране, че опитът с най-съвременните инструменти, по-специално изкуствения интелект и технологиите за анализ на данни, използвани в рамките на трансграничните киберхъбове, се споделя с мрежата на ЕРИКС.

(21) Споделената ситуационна осведоменост между съответните органи е необходима предпоставка за готовността и координацията в целия Съюз по отношение на значителни киберинциденти и мащабни киберинциденти. С Директива (ЕС) 2022/2555 се създаде 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. С Директивата (ЕС) 2022/2555 също така се създаде мрежата на ЕРИКС за насърчаване на бързо и ефективно оперативно сътрудничество между държавите членки. За да се гарантира ситуационна осведоменост и да се засили солидарността, в случаите, когато трансграничните киберхъбове получават информация, свързана с потенциален или текущ мащабен киберинцидент, те следва да предоставят съответната информация на мрежата на ЕРИКС и да отправят ранно предупреждение до EU-CyCLONe. 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 внимание на принципа „необходимост да се знае“ и на потенциално чувствителния характер на споделяната информация. В Директива (ЕС) 2022/2555 се изтъкват отново 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[13], както и отговорностите за предоставянето на аналитични доклади за договореностите за интегрирана реакция на ЕС при политическа криза („договорености за ИРПК“) съгласно Решение за изпълнение (ЕС) 2018/1993 на Съвета[14].

---

13 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, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).

14 Решение за изпълнение (ЕС) 2018/1993 на Съвета от 11 декември 2018 г. относно договорености за интегрирана реакция на ЕС при политическа криза (ОВ L 320, 17.12.2018 г., стр. 28, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

Когато трансграничните киберхъбове споделят с EU-CyCLONe и мрежата на ЕРИКС относима информация и ранни предупреждения, свързани с потенциален или текущ мащабен киберинцидент, е наложително тази информация да се споделя чрез тези мрежи с органите на държавите членки, както и с Комисията. В това отношение Директива (ЕС) 2022/2555 предвижда EU-CyCLONe да има за цел да подпомага координираното управление на мащабни киберинциденти и кризи, свързани с киберсигурността, на оперативно равнище и да осигурява редовния обмен на съответната информация сред държавите членки и институциите, органите, службите и агенциите на Съюза. Задачите на EU-CyCLONe включват разработване на споделена ситуационна осведоменост за такива инциденти и кризи. От първостепенно значение е EU-CyCLONe да гарантира, в съответствие с тази цел и с неговите задачи, че такава информация се предоставя незабавно на съответните представители на държавите членки и на Комисията. За тази цел е от решаващо значение процедурният правилник на EU-CyCLONe да включва съответни разпоредби.

(22) Субектите, участващи в Европейската система за предупреждение в областта на киберсигурността, 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. Те следва също да гарантират 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 причините за открити киберзаплахи и киберрискове следва да отчита текущата извършена работа по уведомяването за инциденти в контекста на прилагането на Директива (ЕС) 2022/2555.

(23) За да се даде възможност за широкомащабен обмен на относими данни и информация за киберзаплахите от различни източници в доверителна и сигурна среда, субектите, участващи в Европейската система за предупреждение в областта на киберсигурността, следва да разполагат с най-съвременни инструменти, оборудване и инфраструктури с високо ниво на сигурност, както и с квалифициран персонал. 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.

(24) Чрез събирането, анализирането, споделянето и обмена на относими данни и информация Европейската система за предупреждение в областта на киберсигурността следва да повиши технологичния суверенитет и отворената стратегическа автономност в областта на киберсигурността, конкурентоспособността и издръжливостта на Съюза. Обединяването на висококачествени подбрани данни би могло да допринесе и за разработването на авангардни технологии за изкуствен интелект и анализ на данни. Извършваният от човек надзор и за тази цел квалифицираната работна сила продължават да бъдат от съществено значение за ефективното обединяване на висококачествени данни.

(25) Въпреки че Европейската система за предупреждение в областта на киберсигурността 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.

(26) Споделянето на информация между участниците в Европейската система за предупреждение в областта на киберсигурността 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 субекта, който предоставя данните, че данните са унищожени.

(27) Запазването на поверителността и информационната сигурност е от първостепенно значение и за трите стълба на настоящия регламент, независимо дали за насърчаване на споделянето или обмена на информация в контекста на Европейската система за предупреждение в областта на киберсигурността, за защита на интересите на субектите, кандидатстващи за подкрепа по линия на Механизма за действие при извънредни ситуации в областта на киберсигурността, или за гарантиране, че в докладите по Европейския механизъм за преглед на киберинциденти могат да бъдат извлечени полезни поуки, без да бъде оказвано отрицателно въздействие върху субектите, засегнати от инцидентите. Участието на държавите членки и субектите в тези механизми зависи от изграденото доверие между техните компоненти. Когато информацията е поверителна съгласно правилата на Съюза или националните правила, нейното споделяне или обмен според настоящия регламент следва да бъде ограничен до това, което е важно и пропорционално на целта на споделянето или обмена. Това споделяне или обмен следва също така да се извършва при зачитане на поверителността на информацията, включително при защита на сигурността и търговските интереси на засегнатите субекти. Споделянето или обменът на информация съгласно настоящия регламент може да се осъществява посредством споразумения за поверителност или насоки относно разпространението на информация, като например протокола „светофар“ с цветен код за поверителност (TLP). Протоколът светофар“ с цветен код за поверителност следва да се разглежда като средство за предоставяне на информация за всякакви ограничения по отношение на по-нататъшното разпространение на информацията. Той се използва в почти всички ЕРИКС и в някои ISAC. В допълнение към тези общи изисквания, когато става въпрос за Европейската система за предупреждение в областта на киберсигурността, в споразуменията на консорциумите за хостинг следва да се определят специални правила относно условията за споделяне на информация в рамките на съответния трансграничен киберхъб. По-конкретно, в споразуменията може да се изисква информацията да се споделя единствено в съответствие с правото на Съюза и националното законодателство.

(28) По отношение на разгръщането на Резерва за киберсигурност на ЕС са необходими специални правила за поверителност. Подкрепата ще се иска, оценява и предоставя в контекст на криза и по отношение на субекти, извършващи дейност в чувствителни сектори. За да функционира ефективно резервът за киберсигурност на ЕС, от съществено значение е ползвателите и субектите да могат да споделят и да предоставят незабавен достъп до цялата информация, необходима на всеки субект, за да изпълнява ролята си в оценката на исканията и разгръщането на подкрепата. Съответно в настоящия регламент следва да се предвиди, че цялата такава информация се използва или споделя само когато това е необходимо за функционирането на резерва, и че информацията, която е поверителна или класифицирана съгласно правото на Съюза и националното право, се използва и споделя само съгласно това право. Освен това ползвателите следва да могат, когато е целесъобразно, да използват протоколи за споделяне на информация, например протокол „светофар“ с цветен код за поверителност, за допълнително уточняване на ограниченията. Въпреки че потребителите разполагат с възможност за преценка в това отношение, важно е при прилагането на тези ограничения те да вземат предвид възможните последици, по-специално по отношение на забавената оценка или предоставяне на исканите услуги. За да бъде ефективен Резервът за киберсигурност на ЕС, е важно възлагащият орган да изясни тези последици на потребителя, преди да подаде искане. Тези предпазни мерки са ограничени до искането и предоставянето на услуги от Резерва за киберсигурност на ЕС и не засягат обмена на информация в друг контекст, например при възлагането на поръчки за Резерва за киберсигурност на ЕС.

(29) С оглед на нарастващите рискове и броя на инцидентите, които засягат държавите членки, е необходимо да се създаде инструмент за подкрепа при кризи, а именно Механизма за действие при извънредни ситуации в областта на киберсигурността, за да се подобри устойчивостта на Съюза на значителни киберинциденти, мащабни киберинциденти и равностойни на мащабни киберинциденти и да се допълнят действията на държавите членки чрез спешна финансова подкрепа за готовност, реагиране при инциденти и първоначално възстановяване на основни услуги. Тъй като пълното възстановяване от инцидент е всеобхватен процес на възстановяване на функционирането на субекта, засегнат от инцидента, до състоянието отпреди инцидента и може да бъде дълъг процес, който води до значителни разходи, подкрепата от Резерва за киберсигурност на ЕС следва да бъде ограничена до началния етап на процеса на възстановяване, което да доведе до възстановяване на основните функции на системите. Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да дава възможност за бързо и ефективно 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).

(30) 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 първоначално възстановяване след значителни киберинциденти и мащабни киберинциденти, като например услугите, предоставяни от ENISA в съответствие с нейния мандат, координираното реагиране и помощта от мрежата на ЕРИКС, подкрепата за смекчаване на последиците от EU-CyCLONe, както и взаимопомощта между държавите членки, включително в контекста на член 42, параграф 7 от ДЕС и екипите за бързо реагиране в областта на киберсигурността на постоянното структурирано сътрудничество (ПСС), създадени съгласно Решение (ОВППС) 2017/2315 на Съвета[15]. Следва да се разгледа необходимостта да се гарантира наличието на специализирани средства за подпомагане на готовността, реагирането и възстановяването при такива инциденти в целия Съюз и в асоциираните към програмата „Цифрова Европа“ трети държави.

[15] 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 (ОВ L 331, 14.12.2017 г., стр. 57, ELI: http://data.europa.eu/eli/dec/2017/2315/2023-05-23).

(31) Настоящият регламент не засяга процедурите и рамките за координиране на реагирането при кризи на равнището на Съюза, по-специално Директива (ЕС) 2022/2555, Механизма за гражданска защита на Съюза, създаден с Решение № 1313/2013/ЕС на Европейския парламент и на Съвета[16], договореностите за ИРПК и Препоръка (ЕС) 2017/1584 на Комисията[17]. Подкрепата, предоставена 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, като се отчита гражданският характер на Механизма за действие при извънредни ситуации в областта на киберсигурността. Подкрепата, предоставяна по линия на Механизма за действие при извънредни ситуации в областта на киберсигурността, може да допълва действията, изпълнявани в контекста на член 42, параграф 7 от ДЕС, включително помощта, предоставена от една държава членка на друга, или да бъде част от съвместния отговор между Съюза и държавите членки или в ситуациите, посочени в член 222 от ДФЕС. Прилагането на настоящия регламент следва също така да бъде координирано с прилагането на мерките от инструментариума за кибердипломация, когато това е уместно.

---

16 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).

17 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).

(32) 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, ENISA, държавите членки, и ЕССС, когато е целесъобразно. 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.

(33) 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 за реагиране при инциденти с цел смекчаване на въздействието на значителни киберинциденти и мащабни киберинциденти, подпомагане на първоначалното възстановяване или възстановяване на основните функции на услугите, предоставяни от субекти, които извършват дейност в сектори с висока степен на критичност или субекти, които извършват дейност в други критични сектори.

(34) 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 изпитване и оценка на киберсигурността на субектите, извършващи дейност в сектори с висока степен на критичност, определени съгласно Директива (ЕС) 2022/2555, включително чрез учения и обучение. За тази цел Комисията, след консултации с ENISA, групата за сътрудничество за МИС и EU-CyCLONe, следва редовно да определя съответните сектори или подсектори, които следва да отговарят на условията за получаване на финансова подкрепа за координирано изпитване на готовността на равнището на Съюза. Секторите или подсекторите следва да бъдат избрани от секторите с висока степен на критичност, изброени в приложение I към Директива (ЕС) 2022/2555.

Координираното изпитване на готовността следва да се основава 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, извършвани от Комисията, върховния представител на Съюза по въпросите на външните работи и политиката на сигурност (наричан по-нататък „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, създаден с Регламент (ЕС) 2018/1971 на Европейския парламент и на Съвета[18], координираните на равнището на Съюза оценки на риска за сигурността на критичните вериги на доставки, 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[19]. 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.

---

[18] Регламент (ЕС) 2018/1971 на Европейския парламент и на Съвета от 11 декември 2018 г. за създаване на Орган на европейските регулатори в областта на електронните съобщения (ОЕРЕС) и на Агенция за подкрепа на ОЕРЕС (Службата на ОЕРЕС), за изменение на Регламент (ЕС) 2015/2120 и за отмяна на Регламент (ЕО) № 1211/2009 (ОВ L 321, 17.12.2018 г., стр. 1).

[19] 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 (ОВ L 333, 27.12.2022 г., стр. 1).

(35) Освен това Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да предоставя подкрепа за други действия за готовност и да подпомага готовността в други сектори, които не са обхванати от координираното изпитване на готовността на субектите, извършващи дейност в сектори с висока степен на критичност или субектите, извършващи дейност в други критични сектори. Тези действия може да включват различни видове дейности за готовност на национално равнище.

(36) Когато държавите членки получават безвъзмездни средства в подкрепа на действия за готовност, субекти в сектори с висока степен на критичност могат да участват в тези действия доброволно. Добра практика е след такива действия участващите субекти да изготвят корективен план, за да изпълнят всички произтичащи от тях препоръки за конкретни мерки и да се възползват в максимална степен от действието за готовност. Въпреки че е важно държавите членки да изискват като част от действията участващите субекти да изготвят и изпълняват такива корективни планове, държавите членки не са задължени или оправомощени по силата на настоящия регламент да изпълняват такива искания. Тези искания не засягат изискванията за субектите и надзорните правомощия на компетентните органи в съответствие с Директива (ЕС) 2022/2555.

(37) Механизмът за действие при извънредни ситуации в областта на киберсигурността следва също така да предоставя подкрепа за действия за реагиране при инциденти с цел смекчаване на въздействието на значителни киберинциденти, мащабни киберинциденти, и равностойни на мащабни киберинциденти, подпомагане на първоначалното 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 инцидентите върху гражданите.

(38) Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да подпомага техническата помощ, предоставяна от една държава членка на друга държава членка, която е засегната от значителен или мащабен киберинцидент, включително от ЕРИКС, както е посочено в член 11, параграф 3, буква е) от Директива (ЕС) 2022/2555. На държавите членки, които предоставят такава 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.

(39) Като се има предвид съществената роля, която частните предприятия играят за откриването, готовността и реагирането на мащабни киберинциденти или равностойни на мащабни киберинциденти, е важно да се признае значението на доброволното *pro bono* сътрудничество с такива предприятия, при което те предлагат услуги без възнаграждение в случай на мащабни киберинциденти и кризи, както и равностойни на мащабни киберинциденти и кризи. ENISA, в сътрудничество с EU-CyCLONe, би могла да наблюдава развитието на тези *pro bono* инициативи и да насърчава тяхното съответствие с критериите, приложими за доверителните доставчици на управлявани услуги за сигурност съгласно настоящия регламент, включително по отношение на надеждността на частните предприятия, техния опит, както и способността им да боравят с чувствителна информация по сигурен начин.

(40) Като част от Механизма за действие при извънредни ситуации в областта на киберсигурността постепенно следва да бъде създаден резерв за киберсигурност на ЕС, състоящ се от услуги от доверителни доставчици на управлявани услуги за сигурност, който да подпомага действията за реагиране и първоначално възстановяване в случай на значителни киберинциденти, мащабни киберинциденти или равностойни на мащабни киберинциденти, засягащи държави членки, институции, органи, служби или агенции на Съюза или асоциирани към програма „Цифрова Европа“ трети държави. Резервът за киберсигурност на ЕС следва да гарантира наличността и готовността на услугите. Поради това той следва да включва услуги, за които са предварително поети ангажименти, включително например способности, които са в готовност и могат да бъдат разгърнати в кратък срок. Услугите от Резерва за киберсигурност на ЕС следва да подпомагат националните органи при предоставянето на помощ на засегнатите субекти, извършващи дейност в сектори с висока степен на критичност или на засегнатите субекти, извършващи дейност в други критични сектори, като допълнение към собствените им действия на национално равнище. Услугите от Резерва за киберсигурност на ЕС следва да могат да служат и за подкрепа на институциите, органите, службите и агенциите на Съюза при сходни условия. Резервът за киберсигурност на ЕС би могъл също така да допринесе за укрепване на конкурентната позиция на промишлеността и на услугите в Съюза в цялата цифрова икономика, включително микропредприятията и малките и средните предприятия, както и стартиращите предприятия, включително чрез стимулиране на инвестициите в научни изследвания и иновации. При възлагането на поръчки за услуги за Резерва за киберсигурност на ЕС, важно е да се вземе предвид Европейската рамка за умения в областта на киберсигурността (ECSF) на ENISA. Когато искат подкрепа от Резерва за киберсигурност на ЕС, ползвателите следва да включват в искането си подходяща информация относно засегнатия субект и потенциалните въздействия, информация за исканата услуга от Резерва за киберсигурност на ЕС и подкрепата, предоставена на засегнатия субект на национално равнище, която следва да бъде взета предвид при оценката на искането от заявителя. За да се гарантира допълняемост с други форми на подкрепа, които са на разположение на засегнатия субект, искането следва да включва също, при наличност, информация относно съществуващи договорни споразумения за реагиране при инциденти и услуги за първоначално възстановяване, както и застрахователни договори, които потенциално покриват такъв тип инциденти.

(41) За да се гарантира ефективното използване на финансирането от Съюза, услугите, за които са поети задължения по Резерва за киберсигурност на ЕС, следва да бъдат преобразувани, съгласно съответния договор, в услуги за готовност, свързани с предотвратяването и реагирането при инциденти, в случай че тези услуги, за които са поети задължения, не се използват за реагиране при инциденти през периода, за който задълженията са били поети предварително. Тези услуги следва да бъдат допълващи се и следва да не дублират действията за готовност, които се управляват от ЕССС.

(42) Исканията за подкрепа от Резерва за киберсигурност на ЕС от органите за управление на киберкризи и ЕРИКС на държавите членки или CERT-EU, от името на институции, органи, служби и агенции на Съюза, следва да бъдат оценявани от възлагащия орган. Когато на ENISA е възложено управлението и функционирането на Резерва за киберсигурност на ЕС, този възлагащ орган е ENISA. Исканията за подкрепа от асоциирани към програма „Цифрова Европа“ трети държави следва да бъдат оценявани от Комисията. За да се улеснят подаването и оценяването на исканията за подкрепа, ENISA би могла да създаде сигурна платформа.

(43) Когато са получени множество паралелни искания, те следва да бъдат приоритизирани в съответствие с критериите, определени в настоящия регламент. С оглед на общите цели на настоящия регламент тези критерии следва да включват мащаба и сериозността на инцидента, вида на засегнатия субект, потенциалното въздействие на инцидента върху засегнатите държави членки и ползватели, потенциалния трансграничен характер и риска от разпространение на ефектите, както и вече предприетите от ползвателя мерки за подпомагане на реакцията и първоначалното възстановяване. С оглед на тези цели и като се има предвид, че исканията на ползвателите от държавите членки са предназначени изключително за подкрепа в целия Съюз на субекти, извършващи дейност в сектори с висока степен на критичност или на субекти, извършващи дейност в други критични сектори, е целесъобразно да се даде по-висок приоритет на исканията на ползвателите от държавите членки, когато тези критерии водят до оценка на две или повече искания като равнопоставени. Това не засяга задълженията, които държавите членки могат да имат, съгласно съответните споразумения за хостинг, да предприемат мерки за защита и подпомагане на институциите, органите, службите и агенциите на Съюза.

(44) Комисията следва да носи цялостна отговорност за изпълнението на Резерва за киберсигурност на ЕС. Като се има предвид значителния опит, натрупан от ENISA във връзка с действието за подкрепа на киберсигурността, тя е най-подходящата агенция за изпълнение на Резерва за киберсигурност на ЕС. Поради това Комисията следва да възложи на ENISA частично или, когато счете за целесъобразно, изцяло функционирането и управлението на Резерва за киберсигурност на ЕС. Възлагането следва да се извършва в съответствие с приложимите правила съгласно Регламент (ЕС, Евратом) 2024/2509, и по-специално при условие че са изпълнени съответните условия за подписване на споразумение за финансов принос. Всички аспекти на функционирането и управлението на Резерва за киберсигурност на ЕС, които не са възложени на ENISA, следва да подлежат на пряко управление от Комисията, включително преди подписването на споразумението за финансов принос.

(45) Държавите членки следва да играят ключова роля в създаването, разгръщането и последващото разгръщане на Резерва за киберсигурност на ЕС. Тъй като Регламент (ЕС) 2021/694 е съответният основен акт за действия за изпълнение на резерва за киберсигурност на ЕС, действията в рамките на Резерва за киберсигурност на ЕС следва да бъдат предвидени в работните програми, посочени в член 24 от Регламент (ЕС) 2021/694. Съгласно параграф 6 от посочения член тези работни програми се приемат от Комисията чрез актове за изпълнение в съответствие с процедурата по разглеждане. Освен това Комисията, в координация с групата за сътрудничество за МИС, следва да определи приоритетите и развитието на Резерва за киберсигурност на ЕС.

(46) Договорите, сключени в рамките на Резерва за киберсигурност на ЕС, не следва да засягат отношенията между стопански субекти и съществуващите задължения между засегнатия субект или ползватели и доставчика на услуги.

(47) 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 и изисквания, които следва да бъдат включени в поканата за участие в поръчки за подбор на тези доставчици, за да се гарантира, че са удовлетворени нуждите на органите на държавите членки, субектите, извършващи дейност в сектори с висока степен на критичност или субектите, извършващи дейност в други критични сектори. За да се отговори на специфичните нужди на държавите членки, при възлагането на поръчки за услуги за Резерва за киберсигурност на ЕС възлагащият орган следва, когато е целесъобразно, да разработи критерии за подбор и изисквания в допълнение към определените в настоящия регламент. Важно е да се насърчава участието на по-малки доставчици, действащи на регионално и местно равнище.

(48) При избора на доставчици, които да бъдат включени в Резерва за киберсигурност на ЕС, възлагащият орган следва да се стреми да гарантира, че Резервът за киберсигурност на ЕС, като цяло, съдържа доставчици, които са в състояние да отговорят на езиковите изисквания на ползвателите. За тази цел възлагащият орган, преди да изготви тръжните спецификации проверява дали потенциалните ползватели на Резерва за киберсигурност на ЕС имат специфични езикови изисквания, така че услугите за поддръжка на Резерва за киберсигурност на ЕС да могат да се предоставят на език измежду официалните езици на институциите на Съюза или на държавите членки, който е вероятно да бъдат разбран от ползвателя или засегнатия субект. В случай че ползвателят изисква повече от един език за предоставянето на услуги за подкрепа от Резерва за киберсигурност на ЕС и тези услуги са възложени на тези езици за този ползвател, ползвателят следва да може да посочи в искането за подкрепа от Резерва за киберсигурност на ЕС на кой от тези езици следва да се предоставят услугите във връзка с конкретния инцидент, довел до искането.

(49) За да подкрепи създаването на Резерва за киберсигурност на ЕС, важно е Комисията да поиска от ENISA да изготви схема за сертифициране на кандидати във връзка с киберсигурността на управлявани услуги за сигурност съгласно Регламент (ЕС) 2019/881в областите, обхванати от Механизма за действие при извънредни ситуации в областта на киберсигурността.

(50) 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 киберинциденти и мащабни киберинциденти, Комисията или EU-CyCLONe, с подкрепата на мрежата на ЕРИКС и с одобрението на засегнатите държави членки, следва да могат да поискат от ENISA да направи преглед и оценка на киберзаплахите, вече известните използваеми уязвимости и действията за смекчаване на последиците по отношение на конкретен значителен киберинцидент или мащабен киберинцидент. След приключване на прегледа и оценката на даден инцидент ENISA следва да изготви доклад за преглед на инцидента в сътрудничество със засегнатата държава членка, съответните заинтересовани страни, включително представители на частния сектор, Комисията и други съответни институции, органи, служби и агенции на Съюза. Въз основа на сътрудничеството със заинтересованите страни, включително от 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 на EU-CyCLONe, мрежата на ЕРИКС и Комисията и следва да бъде използван за информиране за тяхната работа, както и на работата на ENISA. Когато инцидентът се отнася до асоциирана към програма „Цифрова Европа“ трета държава, Комисията следва да предостави доклада също и на върховния представител.

(51) Като се има предвид непредвидимият характер на кибератаките 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 киберинциденти и равностойни на мащабни киберинциденти допринася за защитата на Съюза, и по-специално неговия вътрешен пазар и промишленост, като цяло. Тези дейности биха могли допълнително да допринесат за кибердипломацията на Съюза. Поради това асоциираните към програма „Цифрова Европа“ трети държави следва да могат да поискат подкрепа от Резерва за киберсигурност на ЕС на цялата им територия или на част от нея, когато това е предвидено в споразумението, чрез което третата държава е асоциирана към програмата „Цифрова Европа“. Финансирането на асоциираните към програма „Цифрова Европа“ 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 първоначалното възстановяване след значителни киберинциденти или равностойни на мащабни киберинциденти.

(52) Условията, определени за Резерва за киберсигурност на ЕС и доверителните доставчици на управлявани услуги за сигурност в настоящия регламент, следва да се прилагат при предоставянето на подкрепа на трети държави, асоциирани към програма „Цифрова Европа“. Асоциираните към програма „Цифрова Европа“ трети държави следва да могат да поискат подкрепа от Резерва за киберсигурност на ЕС, когато целевите субекти, за които искат подкрепа от Резерва за киберсигурност на ЕС, са субекти, извършващи дейност в сектори с висока степен на критичност или субекти, извършващи дейност в други критични сектори, и когато откритите инциденти водят до значителни оперативни смущения или могат да имат допълнителни последици за Съюза. Асоциираните към програма „Цифрова Европа“ трети държави следва да отговарят на условията за получаване на подкрепа само когато споразумението, чрез което те са асоциирани към програма „Цифрова Европа“, изрично предвижда такава подкрепа. Освен това тези трети държави следва да продължат да отговарят на условията, само ако са изпълнени три критерия. Първо, третата държава следва да спазва изцяло съответните условия на това споразумение. Второ, като се има предвид допълващият характер на Резерва за киберсигурност на ЕС, третата държава следва да е предприела подходящи мерки, за да се подготви за значителни киберинциденти или равностойни на мащабни киберинциденти. Трето, предоставянето на подкрепа от Резерва за киберсигурност на ЕС следва да бъде в съответствие с политиката на Съюза и цялостните отношения с тази държава, както и с други политики на Съюза в областта на сигурността. В контекста на своята оценка на спазването на този трети критерий Комисията следва да се консултира с върховния представител за привеждането на предоставянето на такава подкрепа в съответствие с общата външна политика на сигурност.

(53) Предоставянето на подкрепа на асоциирани към програма „Цифрова Европа“ трети държави може да засегне отношенията с трети държави и политиката на сигурност на Съюза, включително в контекста на общата външна политика и политика на сигурност и общата политика за сигурност и отбрана. Поради това е целесъобразно на Съвета да бъдат предоставени изпълнителни правомощия за разрешаване и уточняване на срока, през който може да се предоставя такава подкрепа. Съветът следва да действа въз основа на предложение на Комисията, като надлежно отчита оценката на Комисията на трите критерия. Същото следва да се приложи и за подновяванията и за предложенията за изменение или отмяна на такива актове. Когато, при изключителни обстоятелства, Съветът счита, че е настъпила значителна промяна в обстоятелствата по отношение на третия критерий, Съветът следва да може да действа по собствена инициатива за да измени или отмени акт за изпълнение, без да чака предложение на Комисията. Такива значителни промени вероятно ще изискват спешни действия, ще имат особено важни последици за отношенията с трети държави и няма да изискват предварителна подробна оценка от страна на Комисията. Освен това Комисията следва да си сътрудничи с върховния представител по отношение на искания за подкрепа на асоциирани към програма „Цифрова Европа“ трети държави и на изпълнението на подкрепата, предоставена на тези трети държави. Комисията следва също така да вземе предвид всички становища, предоставени от ENISA по отношение на такива искания и подкрепа. Комисията следва да информира Съвета за резултата от оценката на исканията, включително съответните съображения, направени в това отношение, и за услугите, които се използват.

(54) В съобщението на Комисията 18 април 2023 г. относно Академията на ЕС за киберумения се признава недостигът на квалифицирани специалисти. Такива умения са необходими за постигане на целите на настоящия регламент. Съюзът спешно се нуждае от специалисти с умения и компетентности, за да предотвратява, открива и възпира кибератаки и да защитава Съюза, включително най-критичните му инфраструктури, от такива атаки и да гарантира неговата устойчивост. За тази цел е важно да се насърчава сътрудничеството между заинтересованите страни, включително от частния сектор, академичните среди и публичния сектор. Също толкова важно е да се създадат полезни взаимодействия на всички територии на Съюза за инвестициите в образование и обучение, за да се насърчи създаването на предпазни мерки за избягване на изтичането на мозъци, както или увеличаването на разликата в уменията повече в някои региони, отколкото в други. Спешно трябва да се преодолее недостигът на умения в областта на киберсигурността, като се обърне специално внимание на намаляването на неравнопоставеността между половете по отношение на работната сила в областта на киберсигурността, за да се насърчи присъствието и участието на жените в проектирането на цифровото управление.

(55) За да се стимулират иновациите в цифровия единен пазар, е важно да се засилят научните изследвания и иновациите в областта на киберсигурността с цел да се допринесе за повишаване на устойчивостта на държавите членки и на отворената стратегическа автономност на Съюза, като и двете са цели на настоящия регламент. Полезните взаимодействия са от съществено значение за засилване на сътрудничеството и координацията между различните заинтересовани страни, включително от частния сектор, гражданското общество и академичните среди.

(56) Настоящият регламент следва да отчита ангажимента, определен в съвместната декларация от 26 януари 2022 г. на Европейския парламент, Съвета и Комисията, озаглавена „Европейската декларация относно цифровите права и принципи за цифровото десетилетие“ за защита на интересите на демокрациите, хората, предприятията и публичните институции на Съюза срещу свързаните с киберсигурността рискове и киберпрестъпността, включително срещу нарушения на сигурността на данните и кражба или манипулиране на самоличността.

(57) С цел допълване на някои несъществени елементи от настоящия регламент, на Комисията следва да бъде делегирано правомощието да приема актове в съответствие с член 290 от ДФЕС за уточняване на видовете и броя на услугите за реагиране, необходими за Резерва за киберсигурност на ЕС. От особена важност е по време на подготвителната си работа Комисията да проведе подходящи консултации, включително на експертно равнище, и тези консултации да бъдат проведени в съответствие с принципите, заложени в Междуинституционалното споразумение от 13 април 2016 г. за по-добро законотворчество[20]. По-специално, с цел осигуряване на равностойно участие при подготовката на делегираните актове, Европейският парламент и Съветът получават всички документи едновременно с експертите от държавите членки, като техните експерти получават систематично достъп до заседанията на експертните групи на Комисията, занимаващи се с подготовката на делегираните актове.

[20] ОВ L 123, 12.5.2016 г., стр. 1, ELI: https://eur-lex.europa.eu/eli/agree_interinstit/2016/512/oj?locale=bg.

(58) За да се гарантират еднакви условия за изпълнение на настоящия регламент, на Комисията следва да бъдат предоставени изпълнителни правомощия за допълнително определяне на подробните процедурни условия 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[21].

(59) Без да се засягат правилата, свързани с годишния бюджет на Съюза съгласно Договорите, Комисията следва да взема предвид задълженията, произтичащи от настоящия регламент, когато оценява бюджета и нуждите от персонал на ENISA.

(60) Комисията следва редовно да извършва оценка на мерките, предвидени в настоящия регламент. Първата такава оценка следва да се извърши през първите две години след датата на влизане в сила на настоящия регламент и най-малко на всеки четири години след това, като се взема предвид графикът за преразглеждане на многогодишната финансова рамка, установена съгласно член 312 на ДФЕС. Комисията следва да представи доклад за постигнатите резултати на Европейския парламент и на Съвета. За да оцени различните необходими елементи, включително обхвата на информацията, споделяна в рамките на Европейската система за предупреждение в областта на киберсигурността, Комисията следва да се позовава изключително на информация, която е леснодостъпна или доброволно предоставена. Като се вземат предвид геополитическите развития и с цел гарантиране на непрекъснатост и по-нататъшно развитие на установените в настоящия регламент мерки след 2027 г., важно е Комисията да направи оценка на необходимостта за разпределяне на подходящ бюджет в многогодишната финансова рамка за периода 2028—2034 г.

---

[21] Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета от 16 февруари 2011 г. за установяване на общите правила и принципи относно реда и условията за контрол от страна на държавите членки върху упражняването на изпълнителните правомощия от страна на Комисията (ОВ L 55, 28.2.2011 г., стр. 13), ELI: https://eur-lex.europa.eu/eli/reg/2011/182/oj?locale=bg).

(61) Доколкото целите на настоящия регламент, а именно да се укрепи конкурентната позиция на промишлеността и услугите в Съюза в рамките на цифровата икономика и да се допринесе за технологичния суверенитет и отворената стратегическа автономност на Съюза в областта на киберсигурността, не могат да бъдат постигнати в достатъчна степен от държавите членки, а поради обхватът или последиците от действието могат да бъдат по-добре постигнати на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от ДЕС В съответствие с принципа на пропорционалност, уреден в същия член, настоящият регламент не надхвърля необходимото за постигане на тези цели,

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

Глава I

Общи разпоредби

Член 1

Предмет и цели

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

   а) общоевропейска мрежа от киберхъбове (наричана по-нататък „Европейска система за предупреждение в областта на киберсигурността“) за изграждане и подобряване на координирани способности за откриване и обща ситуационна осведоменост;

   б) Механизъм за действие при извънредни ситуации в областта на киберсигурността, който да подпомага държавите членки при подготовката, реагирането, смекчаването на въздействието и първоначалното възстановяване след значителни киберинциденти и мащабни киберинциденти и да подпомага други ползватели при реагиране на значителни киберинциденти и равностойни на мащабни киберинциденти;

   в) Европейски механизъм за преглед на киберинциденти, който да разглежда и оценява значителни киберинциденти или мащабни киберинциденти.

2. Настоящия регламент преследва общите цели за укрепване на конкурентната позиция на промишлеността и на услугите в Съюза в цялата цифрова икономика, включително микропредприятията и малките и средните предприятия, както и стартиращите предприятия, и за допринасяне за технологичния суверенитет и отворената стратегическа автономност на Съюза в областта на киберсигурността, включително чрез стимулиране на иновациите в цифровия единен пазар. Той преследва тези цели чрез укрепване на солидарността на равнището на Съюза, укрепване на екосистемата за киберсигурност, повишаване на киберустойчивостта на държавите членки и развиване на уменията, ноу-хау, способностите и компетентностите на работната сила във връзка с киберсигурността.

3. Постигането на общите цели, посочени в параграф 2, се преследва посредством следните специфични цели:

а) укрепване на общите координирани способности на Съюза за откриване и обща ситуационна осведоменост за киберзаплахи и инциденти;

б) повишаване на готовността на субектите, извършващи дейност в сектори с висока степен на критичност или субектите, извършващи дейност в други критични сектори в целия Съюз, и укрепване на солидарността чрез развиване на координирано изпитване на готовността и засилени способности за реагиране и възстановяване за справяне със значителни киберинциденти, мащабни киберинциденти или равностойни на мащабни киберинциденти, включително възможността за предоставяне на подкрепа от Съюза за реагиране при киберинциденти на асоциирани към програма „Цифрова Европа“ трети държави;

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

4. Действията съгласно настоящия регламент се извършват при надлежно зачитане на компетенциите на държавите членки и допълват дейностите, извършвани от мрежата на ЕРИКС, EU-CyCLONe и групата за сътрудничество за МИС.

5. Настоящият регламент не засяга съществените функции на държавите членки, включително осигуряването на териториална цялост на държавата, поддържането на обществения ред и опазването на националната сигурност. По-специално, националната сигурност остава единствено в рамките на отговорността на всяка държава членка.

6. Съгласно настоящия регламент споделянето или обменът на информация, която е поверителна съгласно правилата на Съюза или националните правила, е ограничено до информацията, която има значение за целите на това споделяне или обмен и която е пропорционална на тези цели. Това споделяне и обмен на информация се извършва при зачитане на нейната поверителност и на сигурността и търговските интереси на засегнатите субекти. Това не включва предоставянето на информация, чието разкриване би противоречило на основните интереси на държавите членки по отношение на националната сигурност, обществената сигурност или отбраната.

Член 2

Определения

За целите на настоящия регламент се прилагат следните определения:

1) „трансграничен киберхъб“ означава многонационална платформа, създадена с писмено споразумение за консорциум, която обединява в координирана мрежова структура национални киберхъбове от най-малко три държави членки и която е предназначена да засили мониторинга, откриването и анализа на киберзаплахи, да предотвратява инциденти и да подпомага изготвянето на разузнавателна информация за киберзаплахите, по-специално чрез обмен на относими данни и информация, анонимизирани, когато е целесъобразно, както и чрез споделяне на най-съвременни инструменти и съвместното развитие на способности за откриване на киберзаплахи, анализ, превенция и защита в доверителна среда;

2) „консорциум, осигуряващ хостинг“ означава консорциум, съставен от участващи държави членки, които са се споразумели да създадат и допринесат за придобиването на инструменти, инфраструктури или услуги за трансграничен киберхъб и за неговото функциониране;

3) „ЕРИКС“ означава ЕРИКС, определен или създаден съгласно член 10 от Директива (ЕС) 2022/2555;

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

5) „субекти, извършващи дейност в сектори с висока степен на критичност“ означава видовете субекти, изброени в приложение I към Директива (ЕС) 2022/2555;

6) „субекти, извършващи дейност в други критични сектори“ означава видовете субекти, изброени в приложения II към Директива (ЕС) 2022/2555;

7) „риск“ означава риск съгласно определението в член 6, точка 9 от Директива (ЕС) 2022/2555;

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

9) „инцидент“ означава инцидент съгласно определението в член 6, точка 6 от Директива (ЕС) 2022/2555;

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

11) „съществен инцидент“ означава съществен инцидент съгласно определението в член 3, точка 8 от Регламент (ЕС, Евратом) 2023/2841 на Европейския парламент и на Съвета[22];

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

[22] Регламент (ЕС, Евратом) 2023/2841 на Европейския парламент и на Съвета от 13 декември 2023 г. за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза (ОВ L, 2023/2841, 18.12.2023 г., ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

13) „равностоен на мащабен киберинцидент“ означава, в случай на институции, органи, служби и агенции на Съюза, сериозен инцидент, а в случай на асоциирани трети държави — инцидент, който причинява степен на смущение, надвишаваща способността на съответната асоциирана към програма „Цифрова Европа“ трета държава да реагира на него;

(14) „асоциирана към програма „Цифрова Европа“ трета държава“ означава трета държава, която е страна по споразумение със Съюза, позволяващо нейното участие в програмата „Цифрова Европа“ съгласно член 10 от Регламент (ЕС) 2021/694;

(15) „възлагащ орган“ означава Комисията или, доколкото функционирането и управлението на Резерва за киберсигурност на ЕС са възложени на ENISA съгласно член 14, параграф 5 — ENISA;

(16) „доставчик на управлявани услуги за сигурност“ означава доставчик на управлявани услуги за сигурност съгласно определението в член 6, точка 40 от Директива (ЕС) 2022/2555;

(17) „доверителни доставчици на управлявани услуги за сигурност“ означава доставчици на управлявани услуги за сигурност, избрани да бъдат включени в Резерва за киберсигурност на ЕС в съответствие с член 17.

Глава II
Европейската система за предупреждение в областта на киберсигурността

Член 3

Създаване на Европейската система за предупреждение в областта на киберсигурността

1. Създава се общоевропейска мрежа от инфраструктура, която се състои от национални киберхъбове и трансгранични киберхъбове, присъединяващи се на доброволна основа към Европейската система за предупреждение в областта на киберсигурността, за да се подпомогне развитието на усъвършенствани способности на Съюза за подобряване на способностите за откриване, анализ и обработка на данни във връзка с киберзаплахи и предотвратяването на инциденти в Съюза.

2. Европейската система за предупреждение в областта на киберсигурността

   а) допринася за по-добрата защита и реагиране на киберзаплахи, като подкрепя и си сътрудничи със съответните субекти, по-специално ЕРИКС, мрежата на ЕРИКС, EU-CyCLONe и компетентните органи, определени или създадени съгласно член 8, параграф 1 от Директива (ЕС) 2022/2555, и укрепва техните способности;

   б) обединява съответните данни и информация за киберзаплахи и инциденти от различни източници в рамките на трансграничните киберхъбове и споделя анализирана или обобщена информация чрез трансгранични киберхъбове, когато е целесъобразно, с мрежата на ЕРИКС;

в) събира и подпомага изготвянето на висококачествена, приложима информация и разузнавателни сведения за киберзаплахите чрез използване на най-съвременни инструменти и авангардни технологии и споделя тази информация и разузнавателни сведения за киберзаплахи;

г) допринася за подобряване на координираното откриване на киберзаплахи и общата ситуационна осведоменост в целия Съюз, както и за подаването на сигнали, включително, когато е целесъобразно, чрез предоставяне на конкретни препоръки на субектите;

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

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

Член 4

Национални киберхъбове

1. Когато държава членка реши да участва в Европейската система за предупреждение за киберсигурност, тя определя или, когато е приложимо, създава национален киберхъб за целите на настоящия регламент.

2. Националният киберхъб е единен субект, действащ под ръководството на държава членка. Това може да бъде ЕРИКС или, когато е приложимо, национален орган за управление на киберкризи или друг компетентен орган, определен или създаден съгласно член 8, параграф 1 от Директива (ЕС) 2022/2555, или друг субект. Националният киберхъб:

   а) 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 киберхъб съгласно посоченото в член 5; както и

   б) е в състояние да открива, обобщава и анализира данни и информация, свързани с киберзаплахи и инциденти, като например разузнавателни данни за киберзаплахи, чрез използване по-специално на най-съвременни технологии и с цел предотвратяване на инциденти.

3. Като част от функциите, посочени в параграф 2 от настоящия член, националните киберхъбове могат да си сътрудничат със субекти от частния сектор за обмен на съответни данни и информация за целите на откриването и предотвратяването на киберзаплахи и инциденти, включително със секторни и междусекторни общности от съществени и значими субекти, както е посочено в член 3 от Директива (ЕС) 2022/2555. Когато е целесъобразно и в съответствие с правото на Съюза и националното право, информацията, поискана или получена от националните киберхъбове, може да включва телеметрични, сензорни и регистрационни данни.

4. Държава членка, избрана съгласно член 9, параграф 1, се ангажира да подаде заявление за участие на нейния национален киберхъб в трансграничен киберхъб.

Член 5

Трансгранични киберхъбове

1. Когато най-малко три държави членки са поели ангажимент да гарантират, че техните национални киберхъбове работят заедно, за да координират своите дейности по откриване и наблюдение на киберзаплахи, тези държави членки могат да създадат консорциум, осигуряващ хостинг, за целите на настоящия регламент.

2. Консорциум, осигуряващ хостинг, е съставен от поне три участващи държави, които са се споразумели да създадат и допринесат за придобиването на инструменти, инфраструктура или услуги за трансграничен киберхъб и за неговото функциониране в съответствие с параграф 4.

3. Когато се избира консорциум, осигуряващ хостинг, в съответствие с член 9, параграф 3, неговите членове сключват писмено споразумение за консорциум, в което:

   а) в което се посочват вътрешните договорености за изпълнение на споразумението за хостинг и използване, посочено в член 9, параграф 3;

   б) се създава трансграничен киберхъб на консорциума, осигуряващ хостинг; както и

   в) се включват специфичните клаузи, изисквани съгласно член 6, параграфи 1 и 2.

4. Трансграничният киберхъб е многонационална платформа, създадена с писмено споразумение за консорциум, както е посочено в параграф 3. Той обединява в координирана мрежова структура националните киберхъбове на държавите членки на консорциума, осигуряващ хостинг. Той е проектиран така, че да се засилват мониторингът, откриването и анализът на киберзаплахи, да се предотвратяват инциденти и да се оказва подкрепа на изготвянето на разузнавателна информация за киберзаплахи, по-специално чрез обмена на относими данни и информация, анонимизирани, когато е целесъобразно, както и чрез споделянето на най-съвременни инструменти и съвместното развитие на способности за откриване на киберзаплахи, анализ, превенция и защита в доверителна среда.

5. Трансграничният киберхъб се представлява за правни цели от член на съответния консорциум, осигуряващ хостинг, действащ като координатор, или от консорциума, осигуряващ хостинг, ако той е юридическо лице. Отговорността за съответствието на трансграничния киберхъб с настоящия регламент и споразумението за хостинг и използване се разпределя в писменото споразумение за консорциум, посочено в параграф 3.

6. Държава членка може да се присъедини към съществуващ консорциум, осигуряващ хостинг, със съгласието на членовете на консорциума, осигуряващ хостинг. Писменото споразумение за консорциум, посочено в параграф 3, и споразумението за хостинг и използване се изменят съответно. Това не засяга правата на собственост на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността (ECCC) върху инструментите, инфраструктурите и услугите, които вече са възложени съвместно с този консорциум за хостинг.

Член 6

Сътрудничество и споделяне на информация

в рамките на трансграничните киберхъбове и между тях

1. Членовете на консорциума, осигуряващ хостинг, гарантират, че техните национални киберхъбове споделят, в съответствие с писменото споразумение за консорциум, посочено в член 5, параграф 3, относима информация, анонимизирана, когато е целесъобразно, като 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, помежду си в рамките на трансграничния киберхъб, когато това споделяне на информация:

   а) насърчава и подобрява откриването на киберзаплахи и укрепва способностите на мрежата на ЕРИКС за предотвратяване и реагиране на инциденти или смекчаване на тяхното въздействие;

   б) подобрява нивото на киберсигурност, например 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, 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 споделяне между членовете на консорциума, осигуряващ хостинг, на информация съгласно посоченото в параграф 1, и условията, при които ще се извършва споделянето на информация;

б) рамка за управление, която изяснява и стимулира споделянето на относимата информация, анонимизирана, когато е целесъобразно, съгласно посоченото в параграф 1;

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

В споразумението за консорциум може да се уточни, че информацията, посочена в параграф 1, се споделя в съответствие с правото на Съюза и националното законодателство.

3. Трансграничните киберхъбове сключват споразумения за сътрудничество помежду си, в които се посочват принципите за оперативна съвместимост и споделяне на информация между трансграничните киберхъбове. Трансграничните киберхъбове информират Комисията за сключените споразумения за сътрудничество.

4. Споделянето на информация, посочено в параграф 1, между трансграничните киберхъбове се гарантира чрез високо ниво на оперативна съвместимост. За да се подпомогне такава оперативна съвместимост, ENISA, в тясно сътрудничество с Комисията, без ненужно забавяне и при всички случаи до ... [12 месеца след датата на влизане в сила на настоящия регламент], издава насоки за оперативна съвместимост, в които се уточняват по-специално форматите и протоколите за споделяне на информация, като се вземат предвид международните стандарти и най-добри практики, както и функционирането на всички установени трансгранични киберхъбове. Изискванията за оперативна съвместимост, предвидени в споразуменията за сътрудничество в областта на трансграничните киберхъбове се основават на насоките, издадени от ENISA.

Член 7

Сътрудничество и обмен на информация с мрежи на равнището на Съюза

1. Трансграничните киберхъбове и мрежата на ЕРИКС си сътрудничат тясно, по-специално за целите на споделянето на информация. За тази цел те постигат съгласие относно процедурните договорености за сътрудничество и споделяне на съответната информация и без да се засяга параграф 2, видовете информация, които трябва да се споделят.

2. Когато трансграничните киберхъбове получат информация, свързана с потенциален или текущ мащабен киберинцидент, те незабавно гарантират, за целите на общата ситуационна осведоменост, че относимата информация, както и ранните предупреждения биват предоставени на органите на държавите членки и на Комисията чрез EU-CyCLONe и мрежата на ЕРИКС.

Член 8

Сигурност

1. Държавите членки, участващи в Европейската система за предупреждение в областта на киберсигурността, осигуряват високо ниво на киберсигурност, включително поверителност и сигурност на данните, както и физическа сигурност на Европейската система за предупреждение в областта на киберсигурността и гарантират, че мрежата 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 и информацията и данните, споделяни чрез мрежата.

2. Държавите членки, участващи в Европейската система за предупреждение в областта на киберсигурността, гарантират, че споделянето на информацията, посочена в член 6, параграф 1, в рамките на Европейската система за предупреждение в областта на киберсигурността със субект, различен от публичен орган или структура на държава членка, не засяга отрицателно интересите на Съюза или на държавите членки в областта на сигурността.

Член 9

Финансиране на Европейската система

за предупреждение в областта на киберсигурността

1. След покана за изразяване на интерес от страна на държавите членки, които възнамеряват да участват в Европейската система за предупреждение в областта на киберсигурността, ЕССС избира държави членки, които да участват, заедно с ЕССС, в съвместното възлагане на поръчки за инструменти, инфраструктури или услуги, за да се създадат или да се подобрят способностите на национални киберхъбове, определени или създадени съгласно член 4, параграф 1. ЕССС може да отпуска на избраните държави членки безвъзмездни средства за финансиране на функционирането на тези инструменти, инфраструктура или услуги. Финансовото участие на Съюза покрива до 50 % от разходите за придобиване на инструментите, инфраструктурите или услугите до 50 % от оперативните разходи. Избраните държави членки поемат останалите разходи. Преди да започнат процедурата за придобиване на инструментите, инфраструктурите или услугите, ЕССС и избраните държави членки сключват споразумение за хостинг и използване, което урежда използването на инструментите, инфраструктурите или услугите.

2. Ако националният киберхъб на държава членка не е участник в трансграничен киберхъб в срок от две години от датата, на която са придобити инструментите, инфраструктурите или услугите или на която е получил безвъзмездни средства, в зависимост от това кое от двете събития настъпи по-рано, държавата членка не отговаря на условията за допълнително подпомагане от Съюза по настоящата глава, докато не се присъедини към трансграничен киберхъб.

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

4. ЕССС изготвя най-малко на всеки две години картографиране на инструментите, инфраструктурите и услугите, необходими и с подходящо качество за създаване или подобряване на способностите на националните киберхъбове и трансграничните киберхъбове, и тяхната наличност, включително от правни субекти, установени или считани за установени в държави членки и контролирани от държавите членки или от граждани на държавите членки. При изготвянето на картографирането ЕССС се консултира с мрежата на ЕРИКС, всички съществуващи трансгранични киберхъбове, ENISA и Комисията.

Глава III

Механизъм за действие при извънредни ситуации в областта на киберсигурността

Член 10

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 окаже подкрепа за подобряването на устойчивостта на Съюза на киберзаплахи и подготвянето и смекчаването, в дух на солидарност, на краткосрочното въздействие на значителни киберинциденти, мащабни киберинциденти и равностойни на мащабни киберинциденти.

2. В случая на държавите членки действията в рамките на Механизма за действие при извънредни ситуации в областта на киберсигурността се предоставят при поискване и допълват усилията и действията на държавите членки за подготовка, реагиране и възстановяване от инциденти.

3. 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, по-специално със специфична цел 3 от него.

4. Действията в рамките на Механизма за действие при извънредни ситуации в областта на киберсигурността се изпълняват предимно по линия на ЕССС в съответствие с Регламент (ЕС) 2021/887 Действията за изпълнение на Резерва за киберсигурност на ЕС, посочени в член 11, буква б) от настоящия регламент, се изпълняват обаче от Комисията и ENISA.

Член 11

Видове дейности

Механизмът за действие при извънредни ситуации в областта на киберсигурността подпомага следните видове действия:

а) действия за готовност, а именно:

i) координираното изпитване на готовността на субектите, извършващи дейност в сектори с висока степен на критичност в целия Съюз, както е посочено в член 12;

ii) други действия за готовност за субекти, извършващи дейност в сектори с висока степен на критичност, или субекти, извършващи дейност в други сектори от критично значение, както е посочено в член 13;

б) действия, подпомагащи реагирането и първоначалното възстановяване след значителни киберинциденти, мащабни киберинциденти и равностойни на мащабни киберинциденти, които да се предоставят от доверителни доставчици на управлявани услуги за сигурност, участващи в Резерва за киберсигурност на ЕС, създаден съгласно член 14;

в) действия за подпомагане на взаимопомощта, както е посочено в член 18.

Член 12

Координирано изпитване на готовността на субектите

1. Механизмът за действие при извънредни ситуации в областта на киберсигурността подкрепя доброволното координирано изпитване на готовността на субектите, извършващи дейност в сектори с висока степен на критичност.

2. Координираното изпитване на готовността може да се състои от дейности за готовност, като например тестване за проникване и оценка на заплахите.

3. Подкрепата за действия за готовност съгласно настоящия член се предоставя на държавите членки предимно под формата на безвъзмездни средства и при спазване на условията, предвидени в съответните работни програми, посочени в член 24 от Регламент (ЕС) 2021/694.

4. С цел подпомагане на координираното изпитване на готовността на субектите, посочени в член 11, буква а), точка (i) от настоящия регламент в целия Съюз, Комисията, след консултация с групата за сътрудничество за МИС, EU-CyCLONe и ENISA, определя съответните сектори или подсектори от секторите с висока степен на критичност, изброени в приложение I към Директива (ЕС) 2022/2555, за които може да се публикуват покани за представяне на предложения за отпускане на безвъзмездни средства. Участието на държавите членки в тези покани за представяне на предложения е доброволно.

5. При определянето на секторите или подсекторите, посочени в параграф 4 Комисията взема предвид координираните оценки на риска и изпитването на устойчивостта на равнището на Съюза, както и резултатите от тях.

6. Групата за сътрудничество за МИС, в сътрудничество с Комисията, върховния представител на Съюза по въпросите на външните работи и политиката на сигурност (наричан по-нататък „върховният представител“) и ENISA и, в рамките на своя мандат, EU-CyCLONe, разработва общи сценарии за риска и методологии за координираното изпитване на готовността, посочено в член 11, буква а), точка i), и когато е целесъобразно, за други действия за готовност, посочени в буква а), точка ii) от посочения член.

7. Когато субект, извършващ дейност в сектор с висока степен на критичност, участва доброволно в координирано изпитване на готовността и то води до препоръки за конкретни мерки, които участващият субект може да интегрира в корективен план, органът на държавата членка, отговарящ за координираното изпитване на готовността, преразглежда, когато е целесъобразно, последващите действия във връзка с тези мерки от страна на участващите субекти с цел повишаване на готовността.

Член 13

Други действия за готовност

1. Механизмът за действие при извънредни ситуации в областта на киберсигурността подкрепя действия за готовност, които не са обхванати от член 12. Тези действия включват действия за готовност за субекти в сектори, които не са определени за координирано изпитване на готовността съгласно член 12. Тези действия могат да подпомогнат мониторинга на уязвимостта, мониторинга на риска, упражненията и обученията.

2. Подкрепата за действия за готовност съгласно настоящия член се предоставя на държавите членки при поискване и предимно под формата на безвъзмездни средства и при условията, определени в съответните работни програми, посочени в член 24 от Регламент (ЕС) 2021/694.

Член 14

Създаване на Резерв за киберсигурност на ЕС

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

2. Резервът за киберсигурност на ЕС се състои от услуги за реагиране, предоставяни от доверителни доставчици на управлявани услуги за сигурност, избрани в съответствие с критериите, посочени в член 17, параграф 2. Резервът за киберсигурност на ЕС може да включва предварително заявени услуги. В случаите, когато тези услуги не се използват за реагиране при инциденти през времето, за което тези услуги са предварително заявени, услугите на доверителен доставчик на управлявани услуги за сигурност могат да бъдат превърнати в услуги за готовност, свързани с предотвратяването и реагирането при инциденти. Резервът за киберсигурност на ЕС може да се използва при поискване във всички държави членки, институции, органи, служби и агенции на Съюза и в асоциираните към програма „Цифрова Европа“ трети държави, посочени в член 19, параграф 1.

3. Ползвателите на услугите, предоставени от Резерва за киберсигурност на ЕС включват следното:

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) CERT-EU, в съответствие с член 13 от Регламент (ЕС, Евратом) 2023/2841;

в) компетентни органи като екипите за реагиране при инциденти с компютърната сигурност и органите за управление на киберкризи на асоциирани към програма „Цифрова Европа“ трети държави в съответствие с член 19, параграф 8.

4. Комисията носи цялостна отговорност за изпълнението на Резерва за киберсигурност на ЕС. Комисията определя приоритетите и развитието на Резерва за киберсигурност на ЕС в координация с групата за сътрудничество за МИС и в съответствие с изискванията на ползвателите, посочени в параграф 3, упражнява надзор върху неговото изпълнение и 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. Тези приоритети се преразглеждат и, ако е целесъобразно, се ревизират на всеки две години. Комисията уведомява Европейския парламент и Съвета за тези приоритети и всички техни преразглеждания.

5. Без да се засяга цялостната отговорност на Комисията за изпълнението на Резерва за киберсигурност на ЕС, посочен в параграф 4 от настоящия член, и при условие че е налице споразумение за финансов принос, както е определено в член 2, точка 19 от Регламент (ЕС, Евратом) 2024/2509, Комисията възлага функционирането и управлението на Резерва за киберсигурност на ЕС, изцяло или частично, на ENISA. Аспектите, които не са възложени на ENISA, остават под пряко управление на Комисията.

6. ENISA изготвя най-малко на всеки две години картографиране на услугите, необходими на ползвателите, посочени в параграф 3, букви а) и б) от настоящия член. Картографирането включва също така наличието на такива услуги, включително от правни субекти, установени или считани за установени в държавите членки и контролирани от държавите членки или от граждани на държавите членки. При картографирането на това наличие ENISA оценява уменията и капацитета на работната сила на Съюза в областта на киберсигурността, които имат отношение към целите на Резерва за киберсигурност на ЕС. Когато изготвя картографирането, ENISA се консултира с групата за сътрудничество за МИС, EU-CyCLONe, Комисията и когато е приложимо, Междуинституционалния съвет по киберсигурност, създаден съгласно член 10 от Регламент (ЕС, Евратом) 2023/2841 (МСК). При картографирането на наличието на услуги ENISA се консултира и със съответните заинтересовани страни от сектора на киберсигурността, включително с доставчиците на управлявани услуги за сигурност. ENISA изготвя подобно картографиране, след като информира Съвета и се консултира с EU-CyCLONe, Комисията и когато е приложимо, с върховния представител, за да определи нуждите на ползвателите, посочени в параграф 3, буква в) от настоящия член.

7. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 23 с цел допълване на настоящия регламент чрез определяне на видовете и броя на услугите за реагиране, необходими за Резерва за киберсигурност на ЕС. При изготвянето на тези делегирани актове Комисията взема предвид картографирането, посочено в параграф 6 от настоящия член, и може да обменя съвети и да си сътрудничи с групата за сътрудничество за МИС и ENISA.

Член 15

Искания за подкрепа от Резерва за киберсигурност на ЕС

1. Ползвателите, посочени в член 14, параграф 3, могат да поискат услуги от Резерва за киберсигурност на ЕС, за да подпомогнат реагирането и да започнат възстановяване след значителни киберинциденти, мащабни киберинциденти или равностойни на мащабни киберинциденти.

2. За да получат подкрепа от Резерва за киберсигурност на ЕС, ползвателите, посочени в член 14, параграф 3, трябва да предприемат всички подходящи мерки за смекчаване на последиците от инцидента, във връзка с който е поискана подкрепата, включително, когато е целесъобразно, предоставяне на пряка техническа помощ и други ресурси за подпомагане на реагирането на инцидента и на усилията за възстановяване.

3. Исканията за подкрепа се предават на възлагащия орган както следва:

   а) в случай на ползватели, посочени в член 14, параграф 3, буква а) от настоящия регламент, чрез единното звено за контакт, определено или създадено съгласно член 8, параграф 3 от Директива (ЕС) 2022/2555;

б) в случай на ползвателя, посочен в член 14, параграф 3, буква б), от този ползвател;

в) в случай на ползвателите, посочени в член 14, параграф 3, буква в) чрез единното звено за контакт, посочено в член 19, параграф 9.

4. В случай на искания от ползвателите, посочени в член 4, параграф 3, буква а), държавите членки информират мрежата на ЕРИКС и когато е целесъобразно, EU-CyCLONe за исканията на ползвателите за подкрепа за реагиране при инциденти и първоначално възстановяване съгласно настоящия член.

5. Исканията за подкрепа за реагиране при инциденти и първоначално възстановяване включват:

а) подходяща информация относно засегнатия субект и потенциалното въздействие на инцидента върху:

i) засегнатите държави членки и ползватели, включително риска от разпространение в друга държава членка, в случай на ползватели, посочени в член 14, параграф 3, буква а);

ii) засегнатите институции, органи, служби или агенции на Съюза, в случай на ползвател, посочен в член 14, параграф 3, буква б);

iii) засегнатите държави, асоциирани към програма „Цифрова Европа“, в случай на ползватели, посочени в член 14, параграф 3, буква в);

б) информация относно исканата подкрепа, заедно с планираното използване на исканата подкрепа, включително посочване на предвижданите нужди;

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

г) когато е целесъобразно, налична информация за други форми на подкрепа, които са на разположение на засегнатия субект.

6. ENISA, в сътрудничество с Комисията и EU-CyCLONe, 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 процедурни условия за начина, по който трябва да се подават искания за услуги за подкрепа от Резерва за киберсигурност на ЕС и начина, по който трябва да се отговаря на тези искания съгласно настоящия член, член 16, параграф 1 и член 19, параграф 10, включително разпоредби за подаване на такива искания и предоставяне на отговорите и образци за докладите, посочени в член 16, параграф 9. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 24, параграф 2.

Член 16

Изпълнение на подкрепата от Резерва за киберсигурност на ЕС

1. В случай на искания от ползватели, посочени в член 14, параграф 3, букви а) и б), исканията за подкрепа от Резерва за киберсигурност на ЕС се оценяват от възлагащия орган. На ползвателите, посочени в член 14, параграф 3, букви а) и б), се изпраща отговор незабавно и при всички случаи не по-късно от 48 часа от подаването на искането, за да се гарантира ефективност на подкрепата. Възлагащият орган уведомява Съвета и Комисията за резултатите от процеса.

2. По отношение на информацията, споделяна в хода на искането и предоставянето на услугите на Резерва за киберсигурност на ЕС, всички страни, участващи в прилагането на настоящия регламент:

   а) ограничават използването и споделянето на тази информация до необходимото за изпълнението на техните задължения или функции съгласно настоящия регламент;

   б) използват и споделят информация, която е поверителна или класифицирана съгласно правото на Съюза и националното право, само в съответствие с това право; както и

   в) осигуряват ефективен, ефикасен и сигурен обмен на информация, по целесъобразност чрез използване и спазване на съответните протоколи за споделяне на информация, включително протокола „светофар“ с цветен код за поверителност.

3. При оценката на индивидуалните искания по член 16, параграф 1 и член 19, параграф 10 възлагащият орган или Комисията, според случая, първо преценява дали са изпълнени критериите, посочени в член 15, параграфи 1 и 2. Ако случаят е такъв, те оценяват продължителността и естеството на подходящата подкрепа, като вземат предвид целта, посочена в член 1, параграф 3, буква б), и следните критерии, когато е приложимо:

а) мащаба и сериозността на инцидента;

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

в) потенциалното въздействие на инцидента върху засегнатите държави членки, институции, органи, служби или агенции на Съюза или асоциираните към програма „Цифрова Европа“ трети държави;

г) потенциалния трансграничен характер на инцидента и риска от разпространението му към други държави членки, институции, органи, служби или агенции на Съюза или асоциирани към програма „Цифрова Европа“ трети държави;

д) мерките, предприети от ползвателя за подпомагане на реагирането и усилията за първоначално възстановяване, както е посочено в член 15, параграф 2.

4. За да се даде приоритет на исканията, в случай на едновременни искания от ползватели, посочени в член 14, параграф 3, критериите, посочени в параграф 3 от настоящия член, се вземат предвид, по целесъобразност, без да се засяга принципът на лоялно сътрудничество между държавите членки и институциите, органите, службите и агенциите на Съюза. Когато две или повече искания се оценяват като еднакви съгласно тези критерии се дава по-висок приоритет на исканията на ползвателите от държавите членки. Когато функционирането и управлението на Резерва за киберсигурност на ЕС са поверени изцяло или частично на ENISA съгласно член 14, параграф 5, ENISA и Комисията си сътрудничат тясно за приоритизиране на исканията в съответствие с настоящия параграф.

5. Услугите в рамките на Резерва за киберсигурност на ЕС се предоставят в съответствие със специални споразумения между доверителния доставчик на управлявани услуги за сигурност и ползвателя, на когото се предоставя подкрепата в рамките на Резерва за киберсигурност на ЕС. Тези услуги могат да бъдат предоставяни в съответствие със специални споразумения между доверителния доставчик на управлявани услуги за сигурност, ползвателя и засегнатия субект. Всички споразумения, посочени в настоящия параграф, включват, наред с останалото, условия за отговорност.

6. Споразуменията, посочени в параграф 3, се основават на образци, изготвени от ENISA след консултации с държавите членки и по целесъобразност, с други ползватели на Резерва за киберсигурност на ЕС.

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

8. Ползвателите могат да използват услугите от Резерва за киберсигурност на ЕС, предоставяни в отговор на искане съгласно член 15, параграф 1, само за да подпомогнат реагирането и да започнат възстановяване от значителни киберинциденти, мащабни киберинциденти или равностойни на мащабни киберинциденти. Те могат да използват тези услуги само по отношение на:

   а) субекти, извършващи дейност в сектори с висока степен на критичност или субекти, извършващи дейност в други критични сектори, в случай на ползватели, посочени в член 14, параграф 3, буква а), и равностойни субекти в случай на ползватели, посочени в член 14, параграф 3, буква в); както и

   б) институции, органи, служби и агенции на Съюза, в случай на ползвател, посочен в член 14, параграф 3, буква б).

9. В срок от два месеца от края на дадена подкрепа ползвателите, които са получили подкрепа, предоставят обобщен доклад за предоставената услуга, постигнатите резултати и извлечените поуки на:

   а) Комисията, ENISA, мрежата на ЕРИКС и EU-CyCLONe, в случай на ползвателите, посочени в член 14, параграф 3, буква а);

   б) Комисията, ENISA и МСК, в случай на ползвателите, посочени в член 14, параграф 3, буква б);

в) Комисията, в случай на ползвател, посочен в член 14, параграф 3, буква в).

Съгласно буква в) от настоящия параграф Комисията предава всеки обобщен доклад, получен от ползвателите, посочени в член 14, параграф 3, на Съвета и върховния представител.

10. Когато функционирането и управлението на Резерва за киберсигурност на ЕС са поверени изцяло или частично на ENISA съгласно член 14, параграф 5 от настоящия регламент, ENISA докладва на Комисията и редовно се консултира с нея във връзка с това. В този контекст ENISA незабавно изпраща на Комисията всички искания, които получава от ползвателите, посочени в член 14, параграф 3, буква в) от настоящия регламент, а когато това се изисква за целите на приоритизирането съгласно настоящия член, всички искания, които е получила от ползвателите, посочени в член 14, параграф 3, буква а) или б) от настоящия регламент. Задълженията по настоящия параграф не засягат член 14 от Регламент (ЕС) 2019/881.

11. В случай на ползватели, посочени в член 14, параграф 3, букви а) и б), възлагащият орган докладва редовно и най-малко два пъти годишно на групата за сътрудничество за МИС за използването и резултатите от подкрепата.

12. В случай на ползватели, посочени в член 14, параграф 3, буква в), Комисията докладва на Съвета и информира върховния представител редовно и най-малко два пъти годишно за използването и резултатите от подкрепата.

Член 17

Доверителни доставчици на управлявани услуги за сигурност

1. При процедурите за възлагане на поръчки за целите на създаването на Резерва за киберсигурност на ЕС възлагащият орган действа в съответствие с принципите, установени в Регламент (ЕС, Евратом) 2024/2509, и в съответствие със следните принципи:

   а) гарантиране, че услугите, включени в Резерва за киберсигурност на ЕС, взети като цяло, са такива, 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 за езици, 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 Съюза, 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 Съюза.

2. При възлагане на поръчки за услуги за Резерва за киберсигурност на ЕС възлагащият орган включва в документацията за поръчката следните критерии и изисквания:

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 и непрекъснатост на експертния опит, както и необходимите технически ресурси;

б) доставчикът и всички съответни дъщерни дружества и подизпълнители спазват приложимите правила за защита на класифицираната информация и разполагат с подходящи мерки, включително, когато е приложимо, споразумения помежду си за защита на поверителната информация, свързана с услугата, и по-специално на доказателствата, констатациите и докладите;

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, когато това се изисква от държава членка;

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

е) доставчикът разполага с хардуера и софтуера, необходими за поддържане на търсената услуга, които не съдържат вече известни и използваеми уязвимости, включват последните актуализации на сигурността и при всички случаи са в съответствие с всяка приложима разпоредба на Регламент (ЕС) 2024/... на Европейския парламент и на Съвета[23+];

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

з) доставчикът е в състояние да достави услугата в кратък срок в държавите членки, в които може да я предоставя;

и) доставчикът е в състояние да достави услугата на един или повече официални езици на институциите на Съюза или на държава членка, както се изисква, ако има такива, от държавите членки или ползвателите, посочени в член 14, параграф 3, букви б) и в), в които доставчикът може да я предоставя;

й) след като бъде въведена европейска схема за сертифициране на киберсигурността на управлявани услуги за сигурност съгласно Регламент (ЕС) 2019/881, в срок от две години, от датата на прилагане на схемата, доставчикът се сертифицира в съответствие с тази схема;

---

[23] Регламент (ЕС) 2024/... на Европейския парламент и на Съвета от ... относно ... (ОВ L, …, ELI: …).

[+] ОВ: моля, впишете в текста номера на регламента, съдържащ се в документ PE-CONS 100/23 (2022/0272(COD)), и въведете номера, датата, заглавието, данните за публикуването в ОВ и референтния ELI на посочения в бележката под линия регламент.

к) доставчикът включва в поканата за участие в поръчки условията за преобразуване за всяка неизползвана услуга за реагиране при инциденти, която би могла да бъде преобразувана в услуги за готовност, тясно свързани с реагирането при инциденти, като учения или обучения.

3. За целите на възлагането на поръчки за услуги за Резерва за киберсигурност на ЕС възлагащият орган може, по целесъобразност, да разработи критерии и изисквания в допълнение към посочените в параграф 2, в тясно сътрудничество с държавите членки.

Член 18

Действия за подпомагане на взаимопомощ

1. Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да предоставя подкрепа за техническата помощ от една държава членка на друга държава членка, засегната от значителен киберинцидент или мащабен киберинцидент, включително в случаи, посочени в член 11, параграф 3, буква е) от Директива (ЕС) 2022/2555.

2. Подкрепата за техническата взаимопомощ по параграф 1 от настоящия член се предоставя под формата на безвъзмездни средства и при условията, определени в съответните работни програми, посочени в член 24 от Регламент (ЕС) 2021/694.

Член 19

Подкрепа за асоциирани към програма „Цифрова Европа“ трети държави

1. Асоциирана към програма „Цифрова Европа“ трета държава може да поиска подкрепа от Резерва за киберсигурност на ЕС, когато в споразумението, чрез което тя е асоциирана към програмата „Цифрова Европа“, се предвижда участие в Резерва за киберсигурност на ЕС. Тези споразумения включват разпоредби, изискващи от съответната трета държава, асоциирана към програма „Цифрова Европа“, да спазва задълженията, посочени в параграфи 2 и 9 от настоящия член. За целите на участието на трета държава в Резерва за киберсигурност на ЕС частичното асоцииране на трета държава към програма „Цифрова Европа“ може да включва асоцииране, ограничено до оперативната цел, посочена в член 6, параграф 1, буква ж) от Регламент (ЕС) 2021/694.

2. В срок от три месеца от сключването на споразумението, посочено в параграф 1, и при всички случаи преди да получи каквато и да е подкрепа от Резерва за киберсигурност на ЕС, асоциираната към програма „Цифрова Европа“ трета държава предоставя на Комисията информация за способностите си за киберустойчивост и управление на риска, включително най-малко информация за предприетите национални мерки за подготовка за значителни киберинциденти, мащабни киберинциденти или равностойни на мащабни киберинциденти, както и информация за отговорните национални субекти, включително ЕРИКС или равностойни субекти, техните способности и предоставените им ресурси. Третата държава, асоциирана към програма „Цифрова Европа“, предоставя актуализации на тази информация редовно и поне веднъж годишно. Комисията предоставя тази информация на върховния представител и ENISA с цел улесняване на прилагането на параграф 11.

3. Комисията оценява редовно и поне веднъж годишно следните критерии по отношение на всяка трета държава, асоциирана към програма „Цифрова Европа“, посочена в параграф 1:

а) дали тази държава спазва условията на споразумението, посочено в параграф 1, доколкото тези условия се отнасят до участие в Резерва за киберсигурност на ЕС;

б) дали тази държава е предприела подходящи стъпки за подготовка за значителни киберинциденти или равностойни на мащабни киберинциденти въз основа на информацията, посочена в параграф 2; както и

в) дали предоставянето на подкрепа е в съответствие с политиката на Съюза и цялостните отношения с тази държава, и дали то е в съответствие с други политики на Съюза в областта на сигурността.

При извършването на оценката, посочена в първа алинея, Комисията се консултира с върховния представител по отношение на критерия, посочен в буква в) от посочената алинея.

Когато Комисията стигне до заключението, че асоциирана към програма „Цифрова Европа“ трета държава отговаря на всички условия, посочени в първа алинея, Комисията представя на Съвета предложение за приемане на акт за изпълнение в съответствие с параграф 4, с който се разрешава предоставянето на подкрепа от Резерва за киберсигурност на ЕС на тази държава.

4. Съветът може да приема актовете за изпълнение, посочени в параграф 1б. Тези актове за изпълнение се прилагат най-много за срок от една година. Те могат да бъдат подновявани. Те могат да включват лимит от не по-малко от 75 дни, за броя на дните, за които може да се предостави подкрепа в отговор на едно-единствено искане.

За целите на настоящия член Съветът действа без забавяне и по правило приема актовете за изпълнение, посочени в настоящия параграф, в срок от осем седмици от приемането на съответното предложение на Комисията съгласно параграф 3, трета алинея.

5. По предложение на Комисията Съветът може по всяко време да изменя или отменя акт за изпълнение, приет съгласно параграф 4.

Когато Съветът прецени, че е настъпила значителна промяна по отношение на критерия, посочен в параграф 3, първа алинея, буква в), Съветът може да измени или отмени акт за изпълнение, приет съгласно параграф 4, като действа по надлежно мотивирана инициатива на една или повече държави членки.

6. При упражняването на изпълнителните си правомощия съгласно настоящия член Съветът прилага критериите, посочени в параграф 3, първа алинея, и обяснява своята оценка на тези критерии. По-специално, когато действа по собствена инициатива съгласно параграф 5, втора алинея, Съветът обяснява значителната промяна, посочена в същата алинея.

7. Подкрепата от Резерва за киберсигурност на ЕС за асоциирана към програма „Цифрова Европа“ трета държава е съобразена с всички специфични условия, предвидени в споразумението, посочено в параграф 1.

8. Ползвателите от асоциирани към програма „Цифрова Европа“ трети държави, които имат право да получават услуги от Резерва за киберсигурност на ЕС, включват компетентни органи, като например екипите за реагиране при инциденти с компютърната сигурност или равностойни субекти и органи за управление на киберкризи.

9. Всяка асоциирана към програма „Цифрова Европа“ 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.

10. Исканията за подкрепа от Резерва за киберсигурност на ЕС по настоящия член се оценяват от Комисията. Възлагащият орган може да предоставя подкрепа на трета държава само когато и докато е в сила акт за изпълнение на Съвета, с който се разрешава такава подкрепа по отношение на тази държава, приет съгласно параграф 4 от настоящия член. На ползвателите, посочени в член 14, параграф 3, буква в), се предава отговор без ненужно забавяне.

11. При получаване на искане за подкрепа по настоящия член Комисията незабавно информира Съвета. Комисията информира редовно Съвета за оценката на искането. Комисията също така си сътрудничи с върховния представител във връзка с получените искания и изпълнението на подкрепата, предоставена на асоциирани към програма „Цифрова Европа“ трети държави от Резерва за киберсигурност на ЕС. Освен това Комисията също така взема предвид всякакви становища, предоставени от ENISA по отношение на тези искания.

Член 20

Координация с механизмите за управление на кризи на Съюза

1. Когато значителен киберинцидент, мащабен киберинцидент или равностоен на мащабен киберинцидент произтича от или води до бедствие, както е определено в член 4, точка 1 от Решение № 1313/2013/ЕС, подкрепата, предоставяна по настоящия регламент за реагиране на такъв инцидент допълва действията по посоченото решение и не засяга неговите разпоредби.

2. В случай на мащабен киберинцидент или равностоен на мащабен трансграничен киберинцидент, при който са задействани договореностите за интегрирана реакция на ЕС при политическа криза съгласно Решение за изпълнение (ЕС) 2018/1993 (договорености за IPCR), подкрепата по настоящия регламент за реагиране на такъв инцидент се осъществява съгласно съответните протоколи и процедури по договореностите за IPCR.

Глава IV

Европейски механизъм за преглед на киберинциденти

Член 21

Европейски механизъм за преглед на киберинциденти

1. По искане на Комисията или EU-CyCLONe ENISA, с подкрепата на мрежата на ЕРИКС и с одобрението на засегнатите държави членки, извършва преглед и оценка на киберзаплахите, известните и използваеми уязвимости и действията за смекчаване на последиците по отношение на конкретен значителен киберинцидент или мащабен киберинцидент. След приключване на прегледа и оценката на даден инцидент и с цел извличане на поуки за избягване или смекчаване на бъдещи инциденти ENISA предоставя доклад за прегледа на инцидента на EU-CyCLONe, мрежата на ЕРИКС, засегнатите държави членки и Комисията, за да ги подкрепи при изпълнението на техните задачи, по-специално на посочените задачи в членове 15 и 16 от Директива (ЕС) 2022/2555. Когато даден инцидент оказва въздействие върху трета държава, асоциирана към програма „Цифрова Европа“, ENISA предоставя доклада на Съвета. В такива случаи Комисията предоставя доклада на върховния представител.

2. За изготвянето на доклада за преглед на инцидент, посочен в параграф 1 от настоящия член, ENISA си сътрудничи със и събира обратна информация от всички съответни заинтересовани страни, включително представители на държавите членки, Комисията, други съответни институции, органи, служби и агенции на Съюза, на сектора, включително доставчиците на управлявани услуги за сигурност, и ползвателите на услуги за киберсигурност. Когато е целесъобразно, ENISA, в сътрудничество с ЕРИКС и когато е приложимо, компетентните органи, определени или създадени съгласно член 8, параграф 1 от Директива (ЕС) 2022/2555, си сътрудничи и със субекти, засегнати от значителни киберинциденти или мащабни киберинциденти. Консултираните представители оповестяват всеки потенциален конфликт на интереси.

3. Докладът за преглед на инцидент обхваща, посочен в параграф 1 от настоящия член, преглед и анализ на конкретния значителен киберинцидент или мащабен киберинцидент, включително основните причини, известните използваеми уязвимости и извлечените поуки. ENISA гарантира, че докладът е съобразен с правото на Съюза или националното законодателство относно защитата на чувствителна или класифицирана информация. Ако съответните държави членки или други ползватели, посочени в член 14, параграф 3, които са засегнати от инцидента, поискат това, данните и информацията, които докладът съдържа, се анонимизират. Той не включва подробности за активно използвани уязвимости, които остават некоригирани.

4. Когато е целесъобразно, докладът за преглед на инцидент съдържа препоръки за подобряване на състоянието на киберсигурността на Съюза и може да включва най-добри практики и поуки, извлечени от съответните заинтересовани страни.

5. ENISA може да издаде публично достъпна версия на доклада за преглед на инцидент. Тази версия на доклада включва само надеждна публична информация или друга надеждна информация със съгласието на съответните държави членки, а по отношение на информацията, свързана с ползвател, както е посочено в член 14, параграф 3, буква б) или в) – със съгласието на този ползвател.

Глава V

Заключителни разпоредби

Член 22

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:

i) вмъква се следната буква:

„аа) подкрепяне на разработването на Европейска система за предупреждение в областта на киберсигурността, създадена с член 3 от Регламент (ЕС) …/… на Европейския парламент и на Съвета*[+] (наричана по-нататък „системата за предупреждение в областта на киберсигурността“), включително разработването, разгръщането и функционирането на национални киберхъбове и трансгранични киберхъбове, които допринасят за ситуационната осведоменост в Съюза и за повишаване на способностите на Съюза за разузнаване на киберзаплахи;

---

* Регламент (ЕС) .../... на Европейския парламент и на Съвета от ... за определяне на мерки за укрепване на солидарността и способностите на Съюза за откриване, подготовка и реагиране при киберзаплахи и инциденти, и за изменение на Регламент (ЕС) 2021/694 (Законодателен акт в областта на киберсолидарността) (ОВ L, …, ELI: …).“;

[+] ОВ: моля въведете в текста номера на регламента, който се съдържа в PE-CONS 94/24 (2023/0109(COD)) и въведете в бележката под линия номера, датата, данните за публикуването в ОВ и референтния ELI на посочения регламент.

ii) добавя се следната буква:

„ж) създаване и управление на Механизма за действие при извънредни ситуации в областта на киберсигурността, създаден с член 10 от Регламент (ЕС) …/…[+], включително Резерва за киберсигурност на ЕС, създаден с член 14 от посочения регламент (наричан по-нататък „Резервът за киберсигурност на ЕС“) в подкрепа на държавите членки при подготовката и реагирането на значителни киберинциденти и мащабни киберинциденти, който допълва националните ресурси и способности и други форми на подкрепа, налични на равнището на Съюза, и в подкрепа на други ползватели при реагирането на значителни киберинциденти и равностойни на мащабни киберинциденти;“;

б) 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[*]. Резервът за киберсигурност на ЕС се изпълнява обаче от Комисията и, в съответствие с член 14, параграф 6 от Регламент (ЕС) .../...[+], от ENISA.

---

* 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).“.

[+] ОВ: Моля въведете в текста номера на регламента, съдържащ се в документ PE-CONS 94/24 (2023/0109(COD)).

2) Член 9 се изменя, както следва:

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

„б) 1 760 806 000 евро за специфична цел 2 – Изкуствен интелект;

в) 1 372 020 000 евро за специфична цел 3 – Киберсигурност и доверие;

г) 482 640 000 евро за специфична цел 4 – Задълбочени цифрови умения“;

б) добавя се следният параграф:

„8. Чрез дерогация от член 12, параграф 1 от Финансовия регламент неизползваните бюджетни кредити за поети задължения и за плащания за действия в контекста на изпълнението на Резерва за киберсигурност на ЕС и действия за подпомагане на взаимопомощта съгласно Регламент …/…[+], 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.“; Европейският парламент и Съветът биват информирани за пренесените бюджетни кредити съгласно член 12, параграф 6 от Финансовия регламент.“;

[+] ОВ: Моля въведете в текста номера на регламента, съдържащ се в документ PE-CONS 94/24 (2023/0109(COD)).

3) Член 12 се изменя, както следва:

а) вмъкват се следните параграфи:

„5а. .Параграф 5 не се прилага, що се отнася до правни субекти, които са установени в Съюза, но се контролират от трети държави, за всяко действие за изпълнение на Европейската система за предупреждение в областта на киберсигурността, когато по отношение на съответното действие са изпълнени следните две условия:

а) налице е реален риск, като се вземат предвид резултатите от картографирането, извършено съгласно член 9, параграф 4 от Регламент (ЕС) .../...[+], че правните субекти, установени или считани за установени в държави членки и контролирани от държави членки или от граждани на държави членки, няма да разполагат с необходимите и достатъчни инструменти, инфраструктури и услуги, за да може това действие да допринесе по подходящ начин за постигането на целта на Европейската система за предупреждение в областта на киберсигурността;

б) рискът за сигурността, свързан с възлагането на поръчки на такива правни субекти в рамките на Европейската система за предупреждение за киберсигурност, е пропорционален на ползите и не подкопава основните интереси на Съюза и неговите държави членки в областта на сигурността.

[+] ОВ: Моля въведете в текста номера на регламента, съдържащ се в документ PE-CONS 94/24 (2023/0109(COD)).

5б. .Параграф 5 не се прилага, що се отнася до правни субекти, които са установени в Съюза, но се контролират от трети държави, за всяко действие за изпълнение на Резерва за киберсигурност на ЕС, когато по отношение на съответното действие са изпълнени следните две условия:

а) налице е реален риск, като се вземат предвид резултатите от картографирането, извършено съгласно член 14, параграф 6 от Регламент (ЕС) .../...[+], че правните субекти, установени или считани за установени в държави членки и контролирани от държави членки или от граждани на държави членки, няма да разполагат с необходимите и достатъчни технологии, експертен опит или капацитет, за да може Резервът за киберсигурност на ЕС да изпълнява по подходящ начин функциите си;

б) рискът за сигурността, свързан с включването на такива правни субекти в Резерва за киберсигурност на ЕС, е пропорционален на ползите и не подкопава основните интереси на Съюза и неговите държави членки в областта на сигурността.“;

[+] ОВ: Моля въведете в текста номера на регламента, съдържащ се в документ PE-CONS 94/24 (2023/0109(COD)).

б) параграф 6 се заменя със следното:

„6. Ако това е надлежно обосновано поради съображения за сигурност, в работната програма може също така да се предвижда правните субекти, установени в асоциирани държави, и правните субекти, установени в Съюза, но контролирани от трети държави, да могат да отговарят на изискванията за участие във всички или в някои от действията по специфични цели 1 и 2 само ако те отговарят на изискванията, които трябва да бъдат изпълнени от тези правни субекти, за да се гарантира защитата на съществените интереси на Съюза и на държавите членки, свързани със сигурността, и за да се гарантира защитата на информацията от класифицирани документи. Тези изисквания се определят в работната програма.

Първа алинея се прилага също, що се отнася до правни субекти, които са установени в Съюза, но се контролират от трети държави, за действия по специфична цел 3:

а) да прилагат Европейската система за предупреждение в областта на киберсигурността, когато се прилага параграф 5а; както и

б) да изпълняват Резерва за киберсигурност на ЕС, когато се прилага параграф 5б.“

4) 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* и 2014/25/ЕС** 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 поръчки за Резерва за киберсигурност на ЕС, Комисията и ENISA могат да действат като централен орган за покупки, за да възлагат поръчки от името или за сметка на трети държави, асоциирани към програмата, в съответствие с член 10 на настоящия регламент. 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 168, параграф 3 от Регламент (ЕС, Евратом) 2024/2509 на Европейския парламент и на Съвета[***], искането от единствена трета държава е достатъчно, за да се упълномощи Комисията или ENISA да предприемат действия.

При изпълнението на процедурите за възлагане на поръчки за Резерва за киберсигурност на ЕС, Комисията и ENISA могат да действат като централен орган за покупки, за да възлагат поръчки от името или за сметка на институциите, органите, службите или 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 или агенциите на Съюза. Чрез дерогация от член 168, параграф 3 от Регламент (ЕС, Евратом) 2024/2509 искането от 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.

---

* 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).

** Директива 2014/25/ЕС на Европейския парламент и на Съвета от 26 февруари 2014 г. относно възлагането на поръчки от възложители, извършващи дейност в секторите на водоснабдяването, енергетиката, транспорта и пощенските услуги и за отмяна на Директива 2004/17/ЕО (ОВ L 94, 28.3.2014 г., стр. 243).

*** Регламент (ЕС, Евратом) 2024/2509 на Европейския парламент и на Съвета от 23 септември 2024 г. за финансовите правила, приложими за общия бюджет на Съюза (ОВ L, 2024/2509, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).“;

5) Вмъква се следният член:

„*Член 16а*

Противоречие между правилата

В случай на действия за прилагане на Европейската система за предупреждение в областта на киберсигурността, приложимите правила са изложените в членове 4, 5 и 9 от Регламент (ЕС) …/…[+]. В случай на противоречие между разпоредбите на настоящия регламент и членове 4, 5 и 9 от Регламент (ЕС) .../...[+], последните имат предимство и се прилагат за тези специфични действия.

[+] ОВ: Моля въведете в текста номера на регламента, съдържащ се в документ PE-CONS 94/24 (2023/0109(COD)).

По отношение на Резерва за киберсигурност на ЕС в член 19 от Регламент (ЕС) .../...[+] са определени специални правила за участието на трети държави, асоциирани към програмата. В случай на противоречие между разпоредбите на настоящия регламент и член 19 от Регламент (ЕС) .../...[+], последните имат предимство и се прилагат за тези специфични действия.“;

6) Член 19 се заменя със следното:

„*Член 19*
Безвъзмездни средства

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 държави членки, избрани съгласно член 9 от Регламент (ЕС) .../...[+], и на консорциума, осигуряващ хостинг, посочен в член 5 от Регламент (ЕС) .../...[+], 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 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.

[+] ОВ: Моля въведете в текста номера на регламента, съдържащ се в документ PE-CONS 94/24 (2023/0109(COD)).

По отношение на действията за подпомагане на взаимопомощта, предвидена в член 18 от Регламент (ЕС) .../...[+], ЕССС информира Комисията и ENISA за исканията на държавите членки за отпускане на преки безвъзмездни средства без покана за представяне на предложения.

По отношение на действията за подпомагане на взаимопомощта, предвидена в член 18 от Регламент (ЕС) .../...[+], и в съответствие с член 193, параграф 2, втора алинея, буква а) от Финансовия регламент, разходите могат, в надлежно обосновани случаи, да се считат за допустими, дори ако са направени преди подаването на заявлението за безвъзмездни средства.“

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

Член 23

Упражняване на делегираните правомощия

1. Правомощието да приема делегирани актове се предоставя на Комисията при спазване на предвидените в настоящия член условия.

2. Правомощието да приема делегирани актове, посочено в член 14, параграф 7, се предоставя на Комисията за срок от 5 години, считано от ... [датата на влизане в сила на настоящия регламент]. Комисията изготвя доклад относно делегирането на правомощия не по-късно от девет месеца преди изтичането на петгодишния срок. Делегирането на правомощия се продължава мълчаливо за срокове с еднаква продължителност, освен ако Европейският парламент или Съветът не възразят срещу подобно продължаване не по-късно от три месеца преди изтичането на всеки срок.

[+] ОВ: Моля въведете в текста номера на регламента, съдържащ се в документ PE-CONS 94/24 (2023/0109(COD)).

3. Делегирането на правомощия, посочено в член 14, параграф 7, може да бъде оттеглено по всяко време от Европейския парламент или от Съвета. С решението за оттегляне се прекратява посоченото в него делегиране на правомощия. Оттеглянето поражда действие в деня след публикуването на решението в *Официален вестник на Европейския съюз* или на по-късна дата, посочена в решението. То не засяга действителността на делегираните актове, които вече са в сила.

4. Преди приемането на делегиран акт Комисията се консултира с експерти, определени от всяка държава членка в съответствие с принципите, залегнали в Междуинституционалното споразумение от 13 април 2016 г. за по-добро законотворчество.

5. Веднага след като приеме делегиран акт, Комисията нотифицира акта едновременно на Европейския парламент и на Съвета.

6. Делегиран акт, приет съгласно член 14, параграф 8, влиза в сила единствено ако нито Европейският парламент, нито Съветът не са представили възражения в срок от два месеца след нотифицирането на същия акт на Европейския парламент и Съвета или ако преди изтичането на този срок и Европейският парламент, и Съветът са уведомили Комисията, че няма да представят възражения. Посоченият срок се удължава с два месеца по инициатива на Европейския парламент или на Съвета.

Член 24

Процедура на комитет

1. Комисията се подпомага от координационния комитет на програмата „Цифрова Европа“, посочен в член 31, параграф 1 от 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 25

Оценка и преглед

1. До ... [две години от датата на влизане в сила на настоящия регламент] и най-малко на всеки четири години след това Комисията оценява функционирането на мерките, предвидени в настоящия регламент, и представя доклад на Европейския парламент и на Съвета.

2. Посочената в параграф 1 оценка включва, по-специално:

а) броя на създадените национални киберхъбове и трансгранични киберхъбове, обхвата на споделената информация, включително, ако е възможно, въздействието върху работата на мрежата на ЕРИКС и степента, до която те са допринесли за укрепването на общото откриване и ситуационна осведоменост на Съюза за киберзаплахи и инциденти и за разработването на най-съвременни технологии; използването на финансиране по програма „Цифрова Европа“ за съвместно възлагане на поръчки за инструменти, инфраструктури или услуги в областта на киберсигурността; а ако информацията е налична – равнището на сътрудничество между националните киберхъбове и секторните и междусекторните общности на съществените и значимите субекти, посочени в член 3 от Директива (ЕС) 2022/2555;

б) използването и ефективността на действията по линия на Механизма за действие при извънредни ситуации в областта на киберсигурността в подкрепа на готовността, включително обучения, реагиране и първоначално възстановяване от значителни киберинциденти, мащабни киберинциденти и равностойни на мащабни киберинциденти, включително използването на финансиране по програма „Цифрова Европа“ и извлечените поуки и препоръките от прилагането на Механизма за действие при извънредни ситуации в областта на киберсигурността;

в) използването и ефективността на Резерва за киберсигурност на ЕС по отношение на видовете ползватели, включително използването на финансиране по програма „Цифрова Европа“, използването на услуги, включително техния вид, средното време за отговор на исканията и за разполагане на Резерва за киберсигурност на ЕС, процента на услугите, преобразувани в услуги за готовност, свързани с предотвратяването и реагирането на инциденти, и извлечените поуки и препоръките от изпълнението на Резерва за киберсигурност на ЕС;

г) приноса на настоящия регламент за укрепване на конкурентната позиция на промишлеността и услугите в Съюза в цялата цифрова икономика, включително микропредприятията и малките и средните предприятия, както и стартиращите предприятия, и приноса към цялостната цел за повишаване на уменията и капацитета на работната сила във връзка с киберсигурността.

3. Въз основа на докладите, посочени в параграф 1, Комисията, ако е целесъобразно, представя на Европейския парламент и на Съвета законодателно предложение за изменение на настоящия регламент.

Член 26

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 Брюксел на

За Европейския парламент	*За Съвета*
Председател	*Председател*

ПРИЛОЖЕНИЕ

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

1) В приложение II разделът „Специфична цел 3 — Киберсигурност и доверие“ се заменя със следното:

„Специфична цел 3 — Киберсигурност и доверие

Програмата стимулира укрепването, изграждането и придобиването на съществен капацитет за обезпечаване на цифровата икономика, обществото и демокрацията на Съюза чрез укрепване на промишления потенциал и конкурентоспособността на Съюза в областта на киберсигурността, както и чрез подобряване на капацитета на частния и публичния сектор за защита на гражданите и предприятията от киберзаплахи, включително подкрепа за изпълнението на Директива (ЕС) 2016/1148.

Първоначалните и, когато е целесъобразно, последващите действия в рамките на тази цел включват:

1. Съвместно инвестиране с държавите членки в съвременно оборудване, инфраструктура и знания в областта на киберсигурността, които са от съществено значение за защитата на критичните инфраструктури и на цифровия единен пазар като цяло. Това съвместно инвестиране би могло да включва инвестиции в квантови съоръжения и ресурси от данни за киберсигурността, информираност за ситуацията в киберпространството, включително национални киберхъбове и трансгранични киберхъбове, формиращи Европейската система за предупреждение в областта на киберсигурността, както и други инструменти, които да бъдат предоставени на публичния и частния сектор в цяла Европа.

2. Увеличаване на съществуващия технологичен капацитет, свързване в мрежа на експертните центрове в държавите членки и гарантиране, че този капацитет отговоря на потребностите на публичния сектор и на промишлеността, включително чрез продукти и услуги, които допринасят за киберсигурността и доверието в рамките на цифровия единен пазар.

3. Широко внедряване на ефективни най-съвременни решения, свързани с киберсигурността и доверието, във всички държави членки. Това внедряване включва укрепване на сигурността и безопасността на продуктите — от проектирането до пазарната им реализация.

4. Подкрепа за преодоляване на недостига на умения в областта на киберсигурността, като се взема предвид балансът между половете, например чрез съгласуване на програмите за изграждане на умения в тази област с цел те да се адаптират към специфичните секторни нужди и да се улесни достъпът до целенасочено специализирано обучение.

5. Насърчаване на солидарността между държавите членки при подготовката и реагирането при значителни киберинциденти и мащабни киберинциденти чрез използване на трансгранични услуги в областта на киберсигурността, включително подпомагане на взаимопомощта между публичните органи и създаване на резерв от доверителни доставчици на управлявани услуги за сигурност на равнището на Съюза.“

2) В приложение II разделът „Специфична цел 3 — Киберсигурност и доверие“ се заменя със следното:

„Специфична цел 3 — Киберсигурност и доверие

3.1. Брой на съвместно придобитите инфраструктури или инструменти за киберсигурност, или и двете, включително в контекста на Европейската система за предупреждение в областта на киберсигурността

3.2. Брой на ползвателите и общностите от ползватели, получаващи достъп до европейски съоръжения за киберсигурност

3.3 Брой на действията в подкрепа на готовността и реагирането при киберинциденти в рамките на Механизма за действие при извънредни ситуации в областта на киберсигурността“.

Във връзка с този акт е направено изявление, което може да бъде намерено в [Службата на ОВ да предостави: ОВ C XXX, XX.XX.2024 г., стр. XX] и на следния линк: [Службата на ОВ: моля въведете линка към заявлението].