ИЗМЕНЕНИЯ 001-001
внесени от Комисията по промишленост, изследвания и енергетика

Доклад
Лина Галвес Муньос **A9-0426/2023**
Законодателен акт за киберсолидарност

Предложение за регламент (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Изменение 1

ИЗМЕНЕНИЯ, ВНЕСЕНИ ОТ ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ*

към предложението на Комисията

2023/0109 (COD)

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

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

* Изменения: нов или изменен текст се обозначава с получер курсив; заличаванията се посочват със символа ▌ .

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

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

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Сметната палата[1],

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

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

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

(1) Всички сектори на икономиката използват и се осланят на информационните и комуникационните технологии, които се превърнаха в съществен компонент, ***но същевременно доведоха до възможни уязвимости*** във всички сектори на икономическата дейност ***и демокрацията,*** тъй като нашите публични администрации, предприятия и граждани са повече от всякога тясно свързани и взаимозависими отвъд секторните и териториалните граници.

(2) Мащабът, честотата и въздействието на киберинцидентите се увеличават ***в целия Съюз и на световно равнище от гледна точка на техните методи и въздействие***, включително атаките по веригата на доставки, целящи кибершпионаж, софтуер за изнудване или смущения. Те представляват съществена заплаха за функционирането на мрежовите и информационните системи. С оглед на бързо променящата се картина на заплахите, заплахата от възможни мащабни инциденти, причиняващи значителни смущения или вреди ***за икономиките и демокрациите, както и*** за критичните инфраструктури ***в целия Съюз***, изисква повишена готовност на всички нива на рамката за киберсигурност на Съюза. Тази заплаха надхвърля рамките на военната агресия на Русия в Украйна и е вероятно да продължи да съществува, като се има предвид

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

многообразието от свързани с държави участници ***и*** престъпни ▌участници, замесени в настоящото геополитическо напрежение. Такива инциденти могат да възпрепятстват предоставянето на обществени услуги и осъществяването на икономически дейности, включително в критични или висококритични сектори, да доведат до значителни финансови загуби, да нарушат доверието на потребителите, да нанесат големи вреди на икономиката на Съюза и дори да имат застрашаващи здравето или живота последици. Освен това киберинцидентите са непредвидими, тъй като често възникват и се развиват за много кратък период от време, не се ограничават в рамките на определен географски район и се случват едновременно или се разпространяват мигновено в много държави. ***Ето защо е необходимо тясно и координирано сътрудничество между публичния сектор, частния сектор, академичните среди, гражданското общество и медиите. Освен това реакцията на Съюза трябва да бъде координирана с тази на международните институции, както и с тази на надеждни и единомислещи международни партньори. Надеждни и единомислещи международни партньори са държави, които споделят ценностите на Съюза за демокрация, ангажираност по отношение на правата на човека, ефективно многостранно сътрудничество и основан на правила ред, в съответствие с рамките и споразуменията за международно сътрудничество. За да се гарантира сътрудничество с надеждни и единомислещи международни партньори и защита срещу системни съперници, на субекти, установени в трети държави, които не са страни по Споразумението за държавните поръчки (СДП), не следва да се разрешава да участват в обществени поръчки съгласно настоящия регламент.***

(3) Необходимо е да се укрепи конкурентната позиция на промишлеността и сектора на услугите в Съюза в рамките на цифровизираната икономика, както и да се подкрепи тяхната цифрова трансформация, като се повиши нивото на киберсигурност на цифровия единен пазар. Както се препоръчва в три различни предложения на Конференцията за бъдещето на Европа[1], необходимо е да се повиши устойчивостта на гражданите, предприятията***, и по-специално микропредприятията, малките и средните предприятия (МСП),***

[1] https://futureu.europa.eu/bg/

включително новосъздадените предприятия и субектите, извършващи дейност в критични инфраструктури, ***включително местните и регионалните органи***, 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 развиване на умения за киберсигурност***, които ще подпомогнат по-бързото откриване и реагиране при киберзаплахи и инциденти, а държавите членки се нуждаят от помощ, за да се подготвят, както и да реагират по-добре в случай на значителни и мащабни киберинциденти. Съюзът следва също така да увеличи способностите си в тези области, особено по отношение на събирането и анализирането на данни за киберзаплахите и инцидентите.

(3а) Кибератаките често са насочени към местни, регионални или национални обществени услуги и инфраструктури. Местните органи са сред най-уязвимите мишени за кибератаки поради липсата на финансови и човешки ресурси. Ето защо е особено важно лицата, отговарящи за вземането на решения на местно равнище, да бъдат запознати с необходимостта от повишаване на цифровата устойчивост, от увеличаване на техния капацитет за намаляване на въздействието на кибератаките и от използване на предвидените в настоящия регламент възможности.

(4) Съюзът вече е предприел редица мерки за намаляване на уязвимостта и повишаване на устойчивостта на критичните инфраструктури и субектите срещу киберрисковете, по-специално Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета[1], Препоръка (ЕС) 2017/1584 на Комисията[2], Директива 2013/40/ЕС на Европейския парламент и на Съвета[3] и

---

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

2 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).

3 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.)*.

Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета[1]. В допълнение в препоръката на Съвета относно координиран подход на равнището на Съюза за укрепване на устойчивостта на инфраструктурата от критично значение държавите членки се приканват да предприемат спешни и ефективни мерки и да си сътрудничат лоялно, ефикасно, солидарно и координирано помежду си, с Комисията и с други съответни публични органи, както и със съответните субекти, за да повишат устойчивостта на инфраструктурата от критично значение, използвана за предоставяне на основни услуги на вътрешния пазар.

(5) Нарастващите киберрискове и цялостната сложна картина на заплахите, с ясен риск от бързо разпространение на киберинциденти от една държава членка към други държави членки и от трета държава към Съюза, изискват засилена солидарност на равнището на Съюза за по-добро откриване, подготовка ▌, реагиране ***и възстановяване от*** киберзаплахи и инциденти. В заключенията на Съвета относно установяването на позицията на Европейския съюз в киберпространството държавите членки също приканиха Комисията да представи предложение за нов фонд за реагиране при извънредни ситуации в областта на киберсигурността[2].

(6) В съвместното съобщение „Политика на ЕС за киберотбрана“[3], прието на 10 ноември 2022 г., беше обявена инициатива на ЕС за киберсолидарност със следните цели: укрепване на общите способности на ЕС за откриване, ситуационна осведоменост и реагиране чрез насърчаване на разгръщането на ***мрежа*** на ЕС от центрове за операции по сигурността (ЦОС), подпомагане на постепенното изграждане на резерв за киберсигурност на равнището на ЕС от услуги от доверителни частни доставчици и изпитване на критични субекти за потенциални уязвимости въз основа на оценки на риска на ЕС.

---

1 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).

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

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

(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 и мащабни киберинциденти. Поради това следва да бъде разгърната общоевропейска ***мрежа от*** ЦОС (европейски киберщит) за изграждане и подобряване на общите способности за откриване и ситуационна осведоменост***, подсилване на способностите на Съюза за откриване на заплахи и обмен на информация***; следва да бъде създаден Механизъм за действие при извънредни ситуации в областта на киберсигурността, който да подпомага държавите членки при подготовката, реагирането и незабавното възстановяване след значителни и мащабни киберинциденти; следва да бъде създаден европейски Механизъм за преглед на киберинциденти, чрез който да се разглеждат и оценяват конкретни значителни или мащабни киберинциденти. Тези действия не засягат членове 107 и 108 от Договора за функционирането на Европейския съюз („ДФЕС“).

(8) За постигането на тези цели е необходимо също така да се измени Регламент (ЕС) 2021/694 на Европейския парламент и на Съвета[1] в някои области. По-специално с настоящия регламент следва да се измени Регламент (ЕС) 2021/694 по отношение на добавянето на нови оперативни цели, свързани с европейския киберщит и Механизма за действие при извънредни ситуации в областта на ***киберсигурността*** в рамките на специфична цел 3 на програмата „Цифрова Европа“, която е насочена към гарантиране на устойчивостта, целостта и надеждността на цифровия единен пазар, към укрепване на способностите за наблюдение и реагиране на кибератаките и заплахите, както и към засилване на трансграничното сътрудничество в областта на киберсигурността. Това ще бъде допълнено от конкретните условия, при които може да бъде отпусната финансова подкрепа за тези действия, и следва да бъдат определени механизмите за управление и координация, необходими за постигане на планираните цели. Други изменения на Регламент (ЕС) 2021/694 следва да включват описания на предложените действия в рамките на новите оперативни

[1] 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).

цели, както и измерими показатели за наблюдение на изпълнението на новите оперативни цели.

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

(9а) С оглед на геополитическите събития и средата на нарастващи киберзаплахи и с цел да се гарантира приемственост и доразвиване на мерките, предвидени в настоящия регламент след 2027 г., по-специално във връзка с европейския киберщит и Механизма за действие при извънредни ситуации в областта на киберсигурността, в многогодишната финансова рамка за периода 2028 – 2034 г. трябва да се осигури специален бюджетен ред. Държавите членки следва да се стремят да поемат ангажимент за подкрепа на всички необходими мерки за намаляване на киберзаплахите и инцидентите в целия Съюз и за увеличаване на солидарността.

(10) Към настоящия регламент се прилагат хоризонталните финансови правила, приети от Европейския парламент и Съвета на основание член 322 от ДФЕС. Тези правила са установени в Регламент ***(ЕС, Евратом) № 2018/1046 на Европейския парламент и на Съвета***[1] 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,

---

1 ***Регламент (ЕС, Евратом) 2018/1046 на Европейския парламент и на Съвета от 18 юли 2018 г. за финансовите правила, приложими за общия бюджет на Съюза, за изменение на регламенти (ЕС) № 1296/2013, (ЕС) № 1301/2013, (ЕС) № 1303/2013, (ЕС) № 1304/2013, (ЕС) № 1309/2013, (ЕС) № 1316/2013, (ЕС) № 223/2014 и (ЕС) № 283/2014 и на Решение № 541/2014/ЕС и за отмяна на Регламент (ЕС, Евратом) № 966/2012 (ОВ L 193, 30.7.2018 г., стр. 1, ELI: https://eur-lex.europa.eu/eli/reg/2018/1046/oj?locale=bg).***

установен в Регламент (ЕС, Евратом) 2020/2092 на Европейския парламент и на Съвета[1].

(11) За целите на доброто финансово управление следва да се определят специални правила за пренасяне на неизползваните бюджетни кредити за поети задължения и за плащания. При спазване на принципа, че бюджетът на Съюза се определя ежегодно, в настоящия регламент следва, предвид непредвидимия, извънреден и специфичен характер на положението в областта на киберсигурността, да се предвидят възможности за пренасяне на неизползвани средства извън определените в ***Регламент (ЕС, Евратом) 2018/1046***, като по този начин се увеличи максимално капацитетът на Механизма за действие при извънредни ситуации в областта на киберсигурността за подпомагане на държавите членки в ефективното противодействие на киберзаплахите.

(11а) Механизмът за действие при извънредни ситуации в областта на киберсигурността и резервът за киберсигурност на ЕС, създаден с настоящия регламент, са нови инициативи и не бяха предвидени при създаването на многогодишната финансова рамка за периода 2021 – 2027 г., а финансирането за тези инициативи цели да ограничи възможно най-много намаляването на финансирането за други приоритети на програмата „Цифрова Европа“. Поради това размерът на финансовите средства, предназначени за резерва за киберсигурност на ЕС, следва да бъде намален и да бъде осигурен основно от неразпределените маржове под таваните на многогодишната финансова рамка или да бъде мобилизиран чрез нетематичните специални инструменти на многогодишната финансова рамка. Всяко заделяне или преразпределяне на средства от съществуващите програми следва да бъде сведено до абсолютния минимум, за да могат съществуващите програми, и по-специално „Еразъм+“, да се предпазят от неблагоприятно въздействие и да се гарантира, че тези програми ще могат да постигнат поставените им цели.

---

[1] ***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) 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 потенциални киберзаплахи включва повишен капацитет за по-добро откриване на киберзаплахи, което е необходимо за спирането на комплексни трайни заплахи. Разузнавателната информация за заплахите представлява информация, която се събира, анализира и тълкува, за да се разберат потенциалните заплахи и рискове. Чрез анализ и съпоставяне на големи обеми от данни, тя разкрива модели, тенденции и показатели за компрометиране на системите, които могат да разкрият злонамерени действия или уязвимости.*** Следва да бъде разгърната ***мрежа*** от ЦОС („европейски киберщит“), състояща се от няколко оперативно съвместими трансгранични платформи, всяка от които обединява няколко национални ЦОС. Тази инфраструктура следва да обслужва националните интереси и нуждите на Съюза в областта на киберсигурността, като използва най-съвременни технологии за авангардно събиране на данни и инструменти за анализ, подобрява способностите за откриване и управление на кибератаки и осигурява ситуационна осведоменост в реално време. ***Националният ЦОС е централизиран капацитет, който отговаря за непрекъснатото събиране на разузнавателна информация за заплахи и за подобряването на състоянието на киберсигурността на субектите под национална юрисдикция чрез предотвратяване, откриване и анализиране на заплахи за киберсигурността.*** Тази инфраструктура следва да служи за по-добро откриване на киберзаплахи и инциденти и по този начин да допълва и подпомага субектите и мрежите на Съюза, отговарящи за управлението на кризи в Съюза, по-специално мрежата за връзка на организациите при кибернетични кризи („EU-CyCLONe“), както е определена в Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета[1].

[1] 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

(13) ***За да участва в киберщита, всяка*** държава членка следва да определи публичен орган на национално равнище, натоварен със задачата да координира дейностите по откриване на киберзаплахи в тази държава членка. ***Държавите членки се насърчават да включат националния капацитет на ЦОС в своята вече съществуваща киберструктура и управление, за да се избегне създаването на допълнителни нива на управление и настоящият регламент да се приведе в съответствие с вече съществуващия законодателен акт, включително и Директива (ЕС) 2022/2555.*** Тези национални ЦОС следва да действат като отправна точка и портал на национално равнище за участие ***на частни и публични субекти, и по-специално техните национални ЦОС***, в европейския киберщит и следва да гарантират, че информацията за киберзаплахите от публични и частни субекти се споделя и събира на национално равнище по ефективен и рационализиран начин. ***Националните ЦОС следва да засилят сътрудничеството и обмена на информация между публичните и частните субекти, за да се премахнат съществуващите понастоящем отделни комуникационни канали. По този начин те могат да подкрепят създаването на модели за обмен на данни и следва да улесняват и насърчават споделянето на информация в доверителна и сигурна среда. Тясното и координирано сътрудничество между публичните и частните субекти е от основно значение за укрепването на устойчивостта на Съюза в областта на киберсигурността.***

(14) Като част от европейския киберщит следва да бъдат създадени редица трансгранични центрове за операции по сигурността („трансгранични ЦОС“). Те следва да обединяват национални ЦОС от поне три държави членки, за да могат да се постигнат всички ползи от трансграничното откриване на заплахи и от обмена и управлението на информация. Общата цел на трансграничните ЦОС следва да бъде укрепване на способностите за анализ, превенция и откриване на киберзаплахи и подпомагане на изготвянето на висококачествена разузнавателна информация за киберзаплахите, ***включително събиране и споделяне на данни и информация за възможно злонамерено хакване, новоразработени***

на Директива (ЕС) 2016/1148 (Директива МИС 2) (ОВ L 333, 27.12.2022 г., стр. 80).

злонамерени заплахи и зловредни кодове, които все още не са внедрени в киберинциденти, и усилия за анализ, по-специално чрез обмен на данни от различни източници, публични или частни, както и чрез споделяне и съвместно използване на най-съвременни инструменти и съвместно развитие на способности за откриване, анализ и превенция в доверителна ***и сигурна*** среда ***с подкрепата на ENISA, по въпроси, свързани с оперативното сътрудничество между държавите членки. Трансграничните ЦОС следва да улесняват и да насърчават споделянето на информация в доверителна и сигурна среда*** и следва да осигурят нов допълнителен капацитет, който да надгражда и допълва съществуващите ЦОС и екипите за реагиране при инциденти с компютърната сигурност („ЕРИКС“), както и други съответни участници.

(15) На национално равнище наблюдението, откриването и анализът на киберзаплахите обикновено се осигуряват от ЦОС от публични и частни субекти в комбинация с ЕРИКС. Освен това ЕРИКС обменят информация в контекста на мрежата на ЕРИКС в съответствие с Директива (ЕС) 2022/2555. Трансграничните ЦОС следва да представляват нов ***капацитет, който да бъде включен в съществуващата инфраструктура за киберсигурност, и по-специално в*** мрежата на ЕРИКС, като обединяват и обменят данни за киберзаплахите от публични и частни субекти, ***по-конкретно от техните ЦОС***, повишават стойността на тези данни чрез експертен анализ и съвместно придобити инфраструктури и най-съвременни инструменти и допринасят за ***технологичния суверенитет на Съюза, за неговата отворена стратегическа автономност, конкурентоспособност и устойчивост, както и за развитието на значителна екосистема за киберсигурност, включително в сътрудничество с надеждни и единомислещи международни партньори.*** .

(16) Трансграничните ЦОС следва да действат като централно звено, позволяващо широко обединяване на относимите данни и разузнавателната информация за киберзаплахите, да дават възможност за разпространение на информация за заплахите сред голям и разнообразен набор от участници (напр. екипи за незабавно реагиране при компютърни инциденти („CERT“), ЕРИКС, центрове за обмен на информация и анализ („ISAC“), оператори на критични инфраструктури), ***с оглед улесняване на премахването на съществуващите***

понастоящем отделни комуникационни канали. По този начин трансграничните ЦОС биха могли също така да подкрепят създаването на модели за обмен на данни в целия Съюз. Информацията, която се обменя между участниците в трансграничен ЦОС, може да включва данни от мрежи и сензори, разузнавателни сведения за заплахи, показатели за компрометиране на системите и контекстуална информация за инциденти, заплахи и уязвимости, ***включително събиране и споделяне на данни и информация за евентуални злонамерени хакерски атаки, новоразработени злонамерени заплахи и зловредни кодове, които все още не са внедрени в киберинциденти, както и усилия за анализ.*** Освен това трансграничните ЦОС следва да сключват и споразумения за сътрудничество с други трансгранични ЦОС.

(17) Споделената ситуационна осведоменост между съответните органи е необходима предпоставка за готовността и координацията в целия Съюз по отношение на значителни и мащабни киберинциденти. С Директива (ЕС) 2022/2555 се създава EU-CyCLONe с цел подпомагане на координираното управление на мащабни киберинциденти и кризи на оперативно равнище и осигуряване на редовния обмен на относимата информация сред държавите членки и институциите, органите, службите и агенциите на Съюза. В Препоръка (ЕС) 2017/1584 относно координирана реакция на мащабни киберинциденти и кризи се разглежда ролята на всички съответни участници. В Директива (ЕС) 2022/2555 се припомнят и отговорностите на Комисията в рамките на Механизма за гражданска защита на Съюза („МГЗС“), създаден с Решение 1313/2013/ЕС на Европейския парламент и на Съвета[1], както и тези за предоставянето на аналитични доклади за механизма за интегрирана реакция при политическа криза („ИРПК“) съгласно Решение за изпълнение (ЕС) 2018/1993 ***на Съвета***[2]. Следователно в ситуации, когато трансграничните ЦОС получат информация, свързана с потенциален или текущ мащабен киберинцидент, те следва да предоставят относимата информация на

---

1 ***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:*** https://eur-lex.europa.eu/eli/dec/2013/1313/oj?locale=bg***).***

2 ***Решение за изпълнение (ЕС) 2018/1993 на Съвета от 11 декември 2018 г. относно договореностите за интегрирана реакция на ЕС на политическо равнище в кризисни ситуации (ОВ L 320, 17.12.2018 г., стр. 28, ELI: https://eur-lex.europa.eu/eli/dec_impl/2018/1993/oj?locale=bg).***

EU-CyCLONe, мрежата на ЕРИКС и Комисията, в ***съответствие с Директива (ЕС) 2022/2555***. По-специално в зависимост от ситуацията, информацията, която трябва да бъде споделена, може да включва техническа информация, информация за естеството и мотивите на нападателя или потенциалния нападател, както и нетехническа информация от по-високо ниво за потенциален или текущ мащабен киберинцидент. В този контекст следва да се обърне надлежно внимание на принципа „необходимост да се знае“ и на потенциално чувствителния характер на споделяната информация.

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

(19) За да се даде възможност за широкомащабен обмен на данни за киберзаплахите от различни източници в доверителна ***и сигурна*** среда, субектите, участващи в европейския киберщит, следва да разполагат с най-съвременни инструменти, оборудване и инфраструктури с високо ниво на сигурност***, както и 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.

(20) Чрез събирането, споделянето и обмена на данни европейският киберщит следва да повиши технологичния суверенитет на Съюза***, неговата отворена стратегическа автономност, конкурентоспособност и устойчивост и развитието на значителна екосистема за киберсигурност на ЕС***. Обединяването на висококачествени подбрани данни следва да допринесе и за разработването на авангардни технологии за изкуствен интелект и анализ на

данни. ***Изкуственият интелект е най-ефективен, когато е съчетан с човешки анализ. Поради това квалифицираната работна сила продължава да бъде от съществено значение за обединяването на висококачествени данни.*** Това следва да бъде улеснено чрез свързването на европейския киберщит с общоевропейската инфраструктура за високопроизводителни изчислителни технологии, създадена с Регламент (ЕС) 2021/1173 на Съвета[1].

(21) Въпреки че европейският киберщит е граждански проект, общността за киберотбрана би могла да се възползва от по-силните граждански способности за откриване и ситуационна осведоменост, разработени за защита на критичната инфраструктура. Трансграничните ЦОС, с подкрепата на Комисията и Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността („ECCC“) и в сътрудничество с върховния представител на Съюза по въпросите на външните работи и политиката на сигурност („върховния представител“), следва постепенно да разработят специални протоколи и стандарти ***за условията за достъп и гаранциите,*** които да позволят сътрудничество с общността за киберотбрана, включително проверка и условия за сигурност***, като се зачита гражданският характер на институциите и предназначението на финансирането, като по този начин се използват средствата, с които разполага общността за отбрана***. Разработването на европейския киберщит следва да бъде придружено от обмисляне, позволяващо бъдещо сътрудничество с мрежите и платформите, отговарящи за обмена на информация в общността за киберотбрана, в тясно сътрудничество с върховния представител ***и при пълно зачитане на правата и свободите***.

(22) Обменът на информация между участниците в европейския киберщит следва да бъде в съответствие със съществуващите правни изисквания, и по-специално със законодателството на Съюза и националното законодателство за защита на данните, както и с правилата за конкуренция на ЕС, уреждащи обмена на информация. Получателят на информацията следва да приложи, доколкото е

[1] Регламент (ЕС) 2021/1173 на Съвета от 13 юли 2021 г. за създаване на Съвместно предприятие за европейски високопроизводителни изчислителни технологии и за отмяна на Регламент (ЕС) 2018/1488 (ОВ L 256, 19.7.2021 г., стр. 3), ***ELI: https://eur-lex.europa.eu/eli/reg/2021/1173/oj?locale=bg***).

необходимо обработването на лични данни, технически и организационни мерки, които гарантират правата и свободите на субектите на данни, и да унищожи данните веднага щом те вече не са необходими за посочената цел, и да информира органа, който предоставя данните, че данните са унищожени.

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

(24) С оглед на нарастващите рискове и броя на киберинцидентите, които засягат държавите членки, е необходимо да се създаде инструмент за подкрепа при кризи, за да се подобри устойчивостта на Съюза на значителни и мащабни киберинциденти и да се допълнят действията на държавите членки чрез спешна финансова подкрепа за готовност, реагиране и незабавно възстановяване на основни услуги. Този инструмент следва да дава възможност за бързо ***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).

(25) Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да предоставя подкрепа на държавите членки в допълнение към техните собствени мерки и ресурси, както и към други съществуващи възможности за подкрепа в случай на реагиране и незабавно възстановяване след значителни и мащабни киберинциденти, като например услугите, предоставяни от Агенцията на Европейския съюз за киберсигурност („ENISA“) в съответствие с нейния мандат, координираното реагиране и помощта от мрежата на ЕРИКС, подкрепата за смекчаване на последиците от EU-

CyCLONe, както и взаимната помощ между държавите членки, включително в контекста на член 42, параграф 7 от ДЕС, екипите за бързо реагиране в областта на киберсигурността на ПСС[1] и хибридните екипи за бързо реагиране. Следва да се разгледа необходимостта да се гарантира наличието на специализирани средства за подпомагане на готовността и реагирането при киберинциденти в целия Съюз и в трети държави.

(26) Настоящият инструмент не засяга процедурите и рамките за координиране на реагирането при кризи на равнището на Съюза, по-специално МГЗС[2], ИРПК[3], и Директива (ЕС) 2022/2555. Той може да подкрепи или да допълни действията, осъществявани в контекста на член 42, параграф 7 от ДЕС или в ситуации, определени в член 222 от ДФЕС. Използването на този инструмент следва също така да бъде координирано с прилагането на мерките от инструментариума за кибердипломация, когато това е уместно.

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

(28) Директива (ЕС) 2022/2555 изисква от държавите членки да определят или създадат един или повече органи за управление на киберкризи и да гарантират, че те разполагат с достатъчно ресурси за изпълнение на възложените им задачи по ефективен и ефикасен начин. В нея също така се изисква държавите членки да определят способностите, активите и процедурите, които могат да бъдат

---

1 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.

2 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).

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

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

(29) Като част от действията за готовност, за да се насърчи последователен подход и да се укрепи сигурността в целия Съюз и неговия вътрешен пазар, следва да се предостави подкрепа за координирано изпитване и оценка на киберсигурността на субектите, извършващи дейност във висококритични сектори, определени съгласно Директива (ЕС) 2022/2555. За тази цел Комисията, с подкрепата на ENISA и в сътрудничество с групата за сътрудничество за МИС, създадена с Директива (ЕС) 2022/2555, следва редовно да определя съответните сектори или подсектори, които следва да отговарят на условията за получаване на финансова подкрепа за координирани изпитвания на равнището на Съюза. Секторите или подсекторите следва да бъдат избрани от приложение I към Директива (ЕС) 2022/2555 („Сектори с висока степен на критичност“). Координираните изпитвания следва да се основават на общи сценарии на риска и методологии. При подбора на секторите и разработването на сценариите на риска следва да се вземат предвид съответните оценки на риска и сценарии на риска за целия Съюз, включително необходимостта от избягване на дублиране, като например оценката на риска и сценариите на риска, за които се призовава в заключенията на Съвета относно установяването на позицията на Европейския

съюз в киберпространството и които трябва да бъдат извършени от Комисията, върховния представител и групата за сътрудничество за МИС, в координация със съответните граждански и военни органи и агенции и установените мрежи, включително EU-CyCLONe, както и оценката на риска на комуникационните мрежи и инфраструктури, поискана от съвместния призив на министрите от Невер и извършена от групата за сътрудничество за МИС, с подкрепата на Комисията и ENISA и в сътрудничество с Органа на европейските регулатори в областта на електронните съобщения (ОЕРЕС), координираните оценки на риска, които ще бъдат извършени съгласно член 22 от Директива (ЕС) 2022/2555, и изпитването на оперативната устойчивост на цифровите технологии, както е предвидено в Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета[1]. При подбора на секторите следва да се вземе предвид и препоръката на Съвета относно координиран подход на равнището на Съюза за укрепване на устойчивостта на инфраструктурата от критично значение.

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

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

(32) Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да подкрепя помощта, предоставяна от държавите

[1] 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.

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

(33) Постепенно следва да бъде създаден резерв за киберсигурност на равнището на Съюза, състоящ се от услуги на частни доставчици на управлявани услуги за сигурност, който да подпомага действията за реагиране и незабавно възстановяване в случаи на значителни или мащабни киберинциденти. Резервът за киберсигурност на ЕС следва да гарантира наличността и готовността на услугите***, като същевременно укрепва устойчивостта на Съюза, включително участието на европейски доставчици на управлявани услуги за сигурност, които са МСП, и като гарантира създаването на екосистема за киберсигурност, по-специално микропредприятия, МСП, включително новосъздадени предприятия, с инвестиции в научни изследвания и иновации (НИИ) за разработване на най-съвременни технологии, като например тези, свързани с облачните технологии и изкуствения интелект***. ***Доверените доставчици, включително МСП, следва да могат да си сътрудничат, за да изпълнят горепосочените критерии.*** Услугите от резерва за киберсигурност на ЕС следва да подпомагат националните органи при предоставянето на помощ на засегнатите субекти, извършващи дейност в критични или висококритични сектори, като допълнение към собствените им действия на национално равнище. ***Поради това резервът за киберсигурност следва да стимулира инвестициите в научни изследвания и иновации, за да се стимулира развитието на тези технологии. Когато е целесъобразно, могат да се провеждат съвместни учения с доверените доставчици и потенциалните ползватели на резерва за киберсигурност, за да се гарантира ефективното функциониране на резерва, когато е необходимо.*** Когато искат подкрепа от резерва за киберсигурност на ЕС, държавите членки следва да посочат подкрепата, предоставена на засегнатия субект на национално равнище, която следва да бъде взета предвид при оценката на искането на държавата членка. Услугите от резерва за киберсигурност на ЕС

могат да служат и за подкрепа на институциите, органите, службите и агенциите на ЕС при сходни условия. ***Комисията следва да гарантира участието на държавите членки и обширен обмен с тях с цел избягване на дублирането с подобни инициативи, включително в рамките на Организацията на Северноатлантическия договор (НАТО).***

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

(35) За да подкрепи създаването на резерва за киберсигурност на ЕС, Комисията би могла да обмисли възможността да поиска от ENISA да изготви схема за сертифициране на кандидати съгласно Регламент (ЕС) 2019/881 за управлявани услуги за сигурност в областите, обхванати от Механизма за действие при извънредни ситуации в областта на киберсигурността. ***За да изпълни допълнителните задачи, произтичащи от настоящата разпоредба, ENISA следва да получи подходящо допълнително финансиране.***

(36) За да се подкрепят целите на настоящия регламент за насърчаване на споделената ситуационна осведоменост, повишаване на устойчивостта на Съюза и осигуряване на ефективно реагиране на значителни и мащабни киберинциденти, EU-CyCLONe, мрежата на ЕРИКС или Комисията следва да могат да поискат от ENISA да направи преглед и оценка на заплахите, уязвимостите и действията за смекчаване на последиците по отношение на конкретен значителен или мащабен киберинцидент. След приключване на прегледа и оценката на даден инцидент ENISA следва да изготви доклад за преглед на инцидента в сътрудничество със съответните заинтересовани страни, включително представители на частния сектор, държавите членки, Комисията и други съответни институции, органи, служби и агенции на ЕС. Що се отнася до частния сектор, ENISA разработва канали за обмен на информация със специализирани доставчици, включително

доставчици на управлявани решения за сигурност и потенциални оференти, за да допринесе за мисията на ENISA за постигане на високо общо ниво на киберсигурност в целия Съюз. Въз основа на сътрудничеството със заинтересованите страни, включително частния сектор, докладът за преглед на конкретни инциденти следва да има за цел да оцени причините, въздействията и мерките за смекчаване от даден инцидент след неговото възникване. Особено внимание следва да се обърне на приноса и изводите, споделени от доставчиците на управлявани услуги за сигурност, които отговарят на условията за най-висока професионална почтеност, безпристрастност и необходим технически опит, както се изисква в настоящия регламент. Докладът следва да бъде представен и използван в работата на EU-CyCLONe, мрежата на ЕРИКС и Комисията. Когато инцидентът се отнася до трета държава, Комисията споделя доклада също с върховния представител.

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

(37а) Трети държави биха могли да получат достъп до ресурси и подкрепа съгласно настоящия регламент, като използват подкрепата за реагиране при киберинциденти от резерва за киберсигурност на ЕС. Освен това за предоставянето на специфични услуги в резерва за киберсигурност на ЕС

може да са необходими доставчици от трети държави на услуги за реагиране при инциденти, включително трети държави, асоциирани към програмата „Цифрова Европа“, или други международни партньорски държави и членове на НАТО. Чрез дерогация от Регламент (ЕС, Евратом) 2018/1046, за да се укрепят технологичният суверенитет на Съюза и неговата отворена стратегическа автономност, конкурентоспособност и устойчивост и да се защитят стратегическите активи, интереси или сигурност на Съюза, на субекти, установени в трети държави, които не са страни по СДП и не са били подложени на скрининг по смисъла на Регламент (ЕС) 2019/452 на Европейския парламент и на Съвета[1] и, при необходимост, на смекчаващи мерки, като се вземат предвид целите, посочени в настоящия регламент, не следва да се разрешава да участват. Външното измерение на настоящия регламент следва да бъде в съответствие с установените разпоредби в споразумението за асоцииране в рамките на програмата „Цифрова Европа“. Участието на трети държави следва да подлежи на обществен контрол с участието на законодателните власти, за да се гарантира, че гражданите могат да участват в процеса.

(38) За да се осигурят еднакви условия за прилагането на настоящия регламент, на Комисията следва да се предоставят изпълнителни правомощия за определяне на условията за оперативна съвместимост между трансграничните ЦОС; определяне на процедурните правила за обмен на информация, свързана с потенциален или текущ мащабен киберинцидент, между трансграничните ЦОС и субектите на Съюза; определяне на технически изисквания за гарантиране на сигурността на европейския киберщит; определяне на видовете и броя на услугите за реагиране, необходими за резерва за киберсигурност на ЕС; и допълнително уточняване на подробните договорености за разпределяне на услугите за подкрепа от резерва за киберсигурност на ЕС. Тези правомощия следва да бъдат упражнявани в

[1] Регламент (ЕС) 2019/452 на Европейския парламент и на Съвета от 19 март 2019 г. за създаване на рамка за скрининг на преки чуждестранни инвестиции в Съюза (ОВ L 79I, 21.3.2019 г., стр. 1), ELI: https://eur-lex.europa.eu/eli/reg/2019/452/oj?locale=bg.

съответствие с Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета*.

---

* ***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).***

(38а) За ефективното прилагане на европейския киберщит и Механизма за действие при извънредни ситуации в областта на киберсигурността е наложително наличието на квалифициран персонал, който да е в състояние надеждно да предоставя съответните услуги в областта на киберсигурността, като спазва най-високи стандарти. Поради това е обезпокоително, че Съюзът е изправен пред недостиг на таланти, който се характеризира с недостиг на квалифицирани специалисти, докато същевременно е изправен пред бързо променяща се картина на заплахите, както се признава в съобщението на Комисията от 18 април 2023 г. относно Академията на ЕС за киберумения. Важно е този недостиг на таланти да се преодолее чрез засилване на сътрудничеството и координацията между различните заинтересовани страни, включително частния сектор, академичните среди, държавите членки, Комисията и ENISA, за да се увеличат и създадат полезни взаимодействия, във всички територии, за инвестициите в образование и обучение, развитието на публично-частни партньорства, подкрепата за инициативи за научни изследвания и иновации, разработването и взаимното признаване на общи стандарти и сертифициране на умения в областта на киберсигурността, включително чрез Европейската рамка за умения в областта на киберсигурността. Това следва също така да улесни мобилността на специалистите в областта на киберсигурността в рамките на Съюза. Настоящият регламент следва да има за цел да насърчава по-разнообразна работна сила в областта на киберсигурността. Всички мерки, насочени към повишаване на уменията в

областта на киберсигурността, изискват гаранции, за да се избегне „изтичането на мозъци“ и риск за трудовата мобилност.

(38б) Необходимо е засилване на специализираните, междудисциплинарните и общите умения и компетентности в Съюза със специален акцент върху жените, тъй като в областта на киберсигурността продължава да съществува неравенство между половете, като жените съставляват 20% от средното присъствие в световен мащаб. Жените трябва да присъстват и да участват в проектирането на цифровото бъдеще и неговото управление.

(38в) Засилването на научните изследвания и иновациите (НИИ) в областта на киберсигурността има за цел да повиши устойчивостта и отворената стратегическа автономност на Съюза. Също така е важно да се създадат полезни взаимодействия с програмите за научни изследвания и иновации и със съществуващите инструменти и институции, както и да се засилят сътрудничеството и координацията между различните заинтересовани страни, включително частния сектор, гражданското общество, академичните среди, държавите членки, Комисията и ENISA;

(38г) Настоящият регламент следва да допринесе за ангажимента по Европейската декларация относно цифровите права и принципи за цифровото десетилетие, свързан със защитата на интересите на нашите демокрации, хора, предприятия и публични институции срещу свързаните с киберсигурността рискове и киберпрестъпността, включително срещу нарушения на сигурността на данните и кражба или манипулиране на самоличността. Прилагането на настоящия регламент следва също така да допринесе за подобряване на прилагането на други законодателни актове, например в областта на изкуствения интелект, неприкосновеността на данните и регулирането на данните по отношение на киберсигурността и киберустойчивостта.

(38д) Повишаването на културата на киберсигурност, при която сигурността, включително тази на цифровата среда, се разбира като обществено благо, ще бъде от основно значение за успешното прилагане на настоящия регламент. Ето защо разработването на мерки, които да включват и

повишават осведомеността на гражданите, следва да бъде още един начин за гарантиране на опазването на нашите демокрации и основни ценности.

(38е) За да бъдат допълнени някои несъществени елементи на настоящия регламент, на Комисията следва да се делегира правомощието да приема актове в съответствие с член 290 от ДФЕС за определяне на условията за оперативна съвместимост между трансграничните ЦОС, установяване на процедурните разпоредби за обмена на информация между трансграничните ЦОС, от една страна, и EU-CyCLONe, мрежата на ЕРИКС и Комисията, от друга страна, определяне на видовете и броя на необходимите услуги за реагиране при инциденти за резерва за киберсигурност на ЕС и допълнително уточняване на подробните условия за разпределяне на услугите за подкрепа от 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, установени в Междуинституционалното споразумение от 13 април 2016 г. за по-добро законотворчество*. По-специално, с цел осигуряване на равно 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.

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

(39) ***Тъй като целите*** на настоящия регламент***, а именно да се укрепи капацитетът на Съюза за предотвратяване, откриване и реагиране на киберзаплахи и за възстановяване от тях, както и да се създаде обща рамка, която да премахне отделните комуникационни канали, не могат да бъдат постигнати в достатъчна степен от държавите членки,*** а могат да бъдат постигнати по-добре на равнището на Съюза. Поради това Съюзът може да приеме мерки в

съответствие с принципите на субсидиарност и пропорционалност, уредени в член 5 от Договора за Европейския съюз. ***В съответствие с принципа на пропорционалност, уреден в същия член, настоящият*** регламент не надхвърля необходимото за постигането на тази цел.

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

Глава I

ОБЩИ ЦЕЛИ, ПРЕДМЕТ И ОПРЕДЕЛЕНИЯ

Член 1

Предмет и цели

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

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

б) създаване на Механизъм за действие при извънредни ситуации в областта на киберсигурността, който да подпомага държавите членки при подготовката, реагирането и незабавното възстановяване след значителни и мащабни киберинциденти;

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

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

а) засилване на общото за Съюза откриване на киберзаплахи и инциденти и ситуационна осведоменост, като по този начин се дава възможност за ***подкрепа за***

промишления капацитет на Съюза и на държавите членки в сектора на киберсигурността, и за укрепване на конкурентната позиция на промишлеността***, по-специално микропредприятията, МСП, включително новосъздадените предприятия,*** и сектора на услугите в Съюза в цифровата икономика и се допринася за технологичния суверенитет на Съюза в областта на киберсигурността, ***неговата отворена стратегическа автономност, конкурентоспособност и устойчивост в този сектор, като се укрепи екосистемата на киберсигурността с цел да се гарантират силни способности на Съюза, включително в сътрудничество с международни партньори***;

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

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

ва) развиване по координиран начин на умения, знания и компетентности на работната сила, за да се гарантира киберсигурността и да се създадат полезни взаимодействия с Академията на ЕС за киберумения.

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

Член 2

Определения

За целите на настоящия регламент се прилагат следните определения:

(-1a) „национален център за операции по сигурността“ или „национален ЦОС“ означава централизиран национален капацитет, който непрекъснато събира и анализира разузнавателна информация за киберзаплахи и подобрява състоянието на киберсигурността в съответствие с член 4;

(1) „**трансграничен център за операции по сигурността**“ ***или*** „**трансграничен ЦОС**“ означава многонационална платформа, която обединява в координирана мрежова структура национални ЦОС ***в съответствие с член 5;***

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

(3) „**консорциум, осигуряващ хостинг**“ означава консорциум, съставен от участващи държави, представлявани от национални ЦОС ***в съответствие с член 5***;

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

(4а) „критичен субект“ означава критичен субект съгласно определението в член 2, точка 1 от Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета[2];

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

(5а) „действия при инцидент“ означава действия при инцидент съгласно определението в член 6, точка 8 от Директива (ЕС) 2022/2555;

(5б) „риск“ означава риск съгласно определението в член 6, точка 9 от Директива (ЕС) 2022/2555;

---

1 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).

2 ***Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14 декември 2022 г. за устойчивостта на критичните субекти и за отмяна на Директива 2008/114/ЕО на Съвета (ОВ L 333, 27.12.2022 г., стр. 164, ELI:. https://eur-lex.europa.eu/eli/dir/2022/2557/oj?locale=bg).***

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

(6а) „значителна киберзаплаха“ означава значителна киберзаплаха съгласно определението в член 6, точка 11 от Директива (ЕС) 2022/2555;

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

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

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

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

(10а) „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;

(11) **„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 16 от настоящия регламент.

Глава II

ЕВРОПЕЙСКИ КИБЕРЩИТ

Член 3

Създаване на европейски киберщит

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

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

2. Европейският киберщит:

а) обединява и обменя данни за киберзаплахи и инциденти от различни източници чрез трансграничните ЦОС***, а когато е относимо – обменя информация с мрежата на ЕРИКС***;

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

в) допринася за по-добра защита и реагиране на киберзаплахите, ***включително чрез предоставяне на конкретни препоръки на субектите***;

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

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

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

Член 4

Национални центрове за операции по сигурността

1. За да ***може да*** участва в европейския киберщит, всяка държава членка определя поне един национален ЦОС. Националният ЦОС е ***централизиран капацитет в*** публичен орган. ***Когато е възможно, националните ЦОС се включват в ЕРИКС или в други съществуващи инфраструктури и управленски органи в областта на киберсигурността.***

Той има способност да действа като отправна точка и портал за други публични и частни организации на национално равнище***, особено техните национални ЦОС,*** за събиране и анализиране на информация относно киберзаплахите и инцидентите ***и, когато е относимо, да споделя тази информация с членовете на мрежата на ЕРИКС на посочената държава членка,*** както и да допринася за работата на трансграничен ЦОС. Той е оборудван с най-съвременни технологии, способни да ***предотвратяват,*** откриват, обобщават и анализират данни, свързани с киберзаплахите и инцидентите.

Национален ЦОС или ЕРИКС може да поиска телеметрични, сензорни или регистрационни данни за своите национални критични субекти от доставчици на управлявани услуги за сигурност, които предоставят услуга на критичния субект. Тези данни се споделят в съответствие с правото на Съюза в областта на защитата на данните и единствено с цел подпомагане на националния ЦОС или ЕРИКС при откриването и предотвратяването на киберзаплахи и инциденти.

2. След покана за заявяване на интерес националните ЦОС ***могат да бъдат избрани*** от Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността („ЕСCС“), за да участват с ЕСCС в съвместна обществена поръчка за инструменти и инфраструктури. ЕСCС може да отпуска безвъзмездни средства на избраните национални ЦОС за финансиране на функционирането на тези инструменти и инфраструктури. Финансовото участие на Съюза покрива до 50 % от разходите за придобиване на инструментите и инфраструктурите и до 50 % от оперативните разходи, а останалите разходи се поемат

от държавата членка. Преди да започнат процедурата за придобиване на инструментите и инфраструктурите, ЕССС и националният ЦОС сключват споразумение за хостинг и използване, което урежда използването на инструментите и инфраструктурите.

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

Член 5

Трансгранични центрове за операции по сигурността

1. Консорциум, осигуряващ хостинг, състоящ се от най-малко три държави членки, представени от национални ЦОС, които са поели ангажимент да работят заедно, за да координират своите дейности по откриване и наблюдение на киберзаплахи, има право да участва в действията за създаване на трансграничен ЦОС. ***Трансграничният ЦОС е проектиран така, че да открива и анализира киберзаплахи, да предотвратява инциденти и да подпомага изготвянето на висококачествена разузнавателна информация, по-специално чрез обмен на данни от различни източници, публични и частни, както и чрез споделяне на най-съвременни инструменти и чрез съвместно разработване на способности за киберотриване, анализ, превенция и защита в доверителна и сигурна среда.***

2. След покана за заявяване на интерес ЕССС ***може да избере*** консорциум, осигуряващ хостинг, който да участва ***с него*** в съвместна обществена поръчка за инструменти и инфраструктури. ЕССС може да отпусне на консорциума, осигуряващ хостинг, безвъзмездни средства за финансиране на функционирането на инструментите и инфраструктурите. Финансовото участие на Съюза покрива до 75 % от разходите за придобиване на инструментите и инфраструктурите и до 50 % от оперативните разходи,

а останалите разходи се поемат от консорциума, осигуряващ хостинг. Преди да започнат процедурата за придобиване на инструментите и инфраструктурите, ЕССС и консорциумът, осигуряващ хостинг, сключват споразумение за хостинг и използване, което урежда използването на инструментите и инфраструктурите.

2а. Чрез дерогация от член 176 от Регламент (ЕС, Евратом) 2018/1046 субектите, установени в трети държави, които не са страни по СДП, не участват в съвместното възлагане на обществени поръчки за инструменти и инфраструктури.

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

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

Член 6

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

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

а) ***подобрява обмена на разузнавателна информация за киберзаплахи между национални и трансгранични ЦОС и центрове за обмен на информация и анализ (ISAC) за промишлеността с цел превенция, откриване или смекчаване на заплахи;***

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

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

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

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

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

3. За насърчаването на обмена на информация между трансграничните ЦОС ***и с центровете за обмен на информация и анализ (ISAC) за промишлеността***, трансграничните ЦОС гарантират високо ниво на оперативна съвместимост помежду си ***и по възможност с ISAC за промишлеността***. За улесняването на оперативната съвместимост между трансграничните ЦОС ***и с ISAC за промишлеността, стандартите и протоколите за обмен на информация могат да бъдат хармонизирани с международните стандарти и най-добрите практики в сектора***. ***Насърчава се и съвместното възлагане на обществени поръчки за киберинфраструктури, услуги и инструменти.*** Освен това, след като се консултира с ЕССС ***и ENISA, на Комисията се предоставя правомощието до ... [шест месеца от датата на влизане в сила на настоящия регламент] да приема делегирани актове в съответствие с член 20а за допълване на настоящия регламент чрез определяне*** на условията за тази оперативна съвместимост ***в тясно сътрудничество с***

трансграничните ЦОС и въз основа на международните стандарти и най-добрите промишлени практики.

4. Трансграничните ЦОС сключват споразумения за сътрудничество помежду си ***и, когато е целесъобразно, с ISAC за промишлеността,*** в които се посочват принципите за обмен на информация ***и оперативна съвместимост*** между трансграничните платформи***, като се вземат предвид вече съществуващите съответни механизми за обмен на информация, предвидени в Директива (ЕС) 2022/2555. Когато е целесъобразно, трансграничните ЦОС сключват споразумения за сътрудничество с ISAC за промишлеността. В контекста на потенциален или текущ мащабен киберинцидент механизмите за обмен на информация спазват съответните разпоредби на Директива (ЕС) 2022/2555.***

Член 7

Сътрудничество и обмен на информация с *мрежата на* ЕРИКС

1. Когато трансграничните ЦОС получат информация, свързана с потенциален или текущ мащабен киберинцидент***, за целите на общата ситуационна осведоменост, координиращият ЦОС*** незабавно предоставя съответната информация на ***своя ЕРИКС или компетентен орган, който ще докладва за това на*** EU-CyCLONe, мрежата на ЕРИКС и Комисията ***и ENISA в съответствие със*** съответните им функции ***и процедури*** по управление на кризи в съответствие с Директива (ЕС) 2022/2555. ***Настоящият параграф не налага допълнителни задължения на публичноправни или частноправни субекти да съобщават за потенциален или текущ мащабен киберинцидент за изпълнението на задълженията, определени в Директива (ЕС) 2022/2555.***

2. На Комисията ***се предоставя правомощието да приема делегирани актове в съответствие с член 20а след като се е консултирала с мрежата на ЕРИКС за допълване на настоящия регламент чрез определяне на*** процедурните разпоредби за обмена на информация, предвиден в параграф 1 ***от настоящия член и в съответствие с Директива (ЕС) 2022/2555.***

Член 8

Сигурност

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

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

3. Комисията може да приема актове за изпълнение за определяне на техническите изисквания, които държавите членки трябва да спазват, за да изпълнят задълженията си по параграфи 1 и 2. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 21, параграф 2 от настоящия регламент. ***Те са в съответствие с директиви (ЕС) 2022/2555 и (ЕС) 2022/2557***. ***В своите актове за изпълнение*** Комисията, подпомагана от върховния представител, взема предвид съответните стандарти за сигурност на ниво отбрана, за да улесни сътрудничеството с военните участници.

Глава III

МЕХАНИЗЪМ ЗА ДЕЙСТВИЕ ПРИ ИЗВЪНРЕДНИ СИТУАЦИИ В ОБЛАСТТА НА КИБЕРСИГУРНОСТТА

Член 9

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

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

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

Член 10

Вид действия

1. Механизмът подпомага следните видове действия:

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

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

в) действия за взаимопомощ, състоящи се в предоставяне на помощ от националните органи на една държава членка на друга държава членка, по-

специално както е предвидено в член 11, параграф 3, буква е) от Директива (ЕС) 2022/2555.

1а. След задействането на Механизма всяка година Комисията прави оценка и публикува доклад както за положителните, така и за отрицателните аспекти на работата на Механизма, включително дали са необходими допълнителни изисквания за сътрудничество или обучение.

Член 11

Координирано изпитване на готовността на субектите

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

2. Групата за сътрудничество за МИС, в сътрудничество с Комисията, ENISA, върховния представител ***и субектите, подлежащи на координирано изпитване на готовността съгласно параграф 1***, разработва общи сценарии за риска и методологии за координираните изпитвания ***на готовността, което води до разработването на съгласуван план за работа. Субектите, подлежащи на координирано изпитване на готовността, разработват и прилагат корективен план, в който се изпълняват препоръките, произтичащи от изпитванията на готовността.***

Групата за сътрудничество за МИС може да информира за приоритизирането на секторите или подсекторите за координираните изпитвания на готовността.

Член 12

Създаване на резерва за киберсигурност на ЕС

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

Когато е очевидно, че възложените услуги не могат да се използват пълноценно за предоставяне на подкрепа за реагиране при значителни или мащабни инциденти, тези услуги могат, по изключение, да се преобразуват в упражнения или обучения за справяне с инциденти и, при поискване, да се предоставят на потребителите от възлагащия орган.

2. Резервът за киберсигурност на ЕС се състои от услуги за реагиране при инциденти, предоставяни от доверителни доставчици на ***управлявани услуги за сигурност***, избрани в съответствие с критериите, посочени в член 16. ***Резервът за киберсигурност на ЕС*** включва предварително заявени услуги. Услугите могат да бъдат предоставяни във всички държави членки ***и те укрепват технологичния суверенитет на Съюза, както и неговата отворена стратегическа автономност, конкурентоспособност и устойчивост в сектора на киберсигурността, включително чрез стимулиране на иновациите в цифровия единен пазар в рамките на Съюза.***

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

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

б) институции, органи и агенции на Съюза, ***както е посочено в член 3, параграф 1 от Регламент (ЕС) .../2023 на Европейския парламент и на Съвета[1] и CERT-EU.***

[1] ***Регламент (ЕС) .../2023 за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза (ОВ C , , стр., , ELI: ...).***

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

5. Комисията носи цялостна отговорност за изпълнението на резерва за киберсигурност на ЕС. Комисията определя приоритетите и развитието на резерва за киберсигурност на ЕС, ***в координация с групата за координация на МИС 2 и*** в съответствие с изискванията на ползвателите, посочени в параграф 3, и упражнява надзор върху неговото изпълнение, като осигурява взаимно допълване, съгласуваност, полезни взаимодействия и връзки с други действия за подкрепа съгласно настоящия регламент, както и с други действия и програми на Съюза.

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

7. За да подпомогне Комисията при създаването на резерва за киберсигурност на ЕС, ENISA изготвя картографиране на необходимите услуги, ***включително необходимите умения и капацитета на служителите в областта на киберсигурността,*** след като се консултира с държавите членки и Комисията, ***и, по целесъобразност, с доставчиците на управлявани услуги за сигурност и други представители на сектора на киберсигурността***. След консултация с Комисията***, с доставчиците на управлявани услуги за сигурност и, по целесъобразност, с други представители на сектора на киберсигурността,*** ENISA изготвя подобно картографиране за определяне на нуждите на трети държави, които отговарят на условията за получаване на подкрепа от резерва за киберсигурност на ЕС съгласно член 17. Когато е уместно, Комисията се консултира с върховния представител ***и информира Съвета за потребностите на трети държави***.

8. ***На*** Комисията ***се предоставя правомощието да приема делегирани актове в съответствие с член 20а с цел допълване на настоящия регламент чрез определяне на*** видовете и броя на услугите за реагиране, необходими за резерва за киберсигурност на ЕС.▌..

Член 13

Искания за подкрепа от резерва за киберсигурност на ЕС

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

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

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

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

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

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

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

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

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

7. ***На*** Комисията ***се предоставя правомощието да приема делегирани актове в съответствие с член 20а за допълване на настоящия регламент чрез определяне на*** подробните условия за разпределяне на услугите за подкрепа от резерва за киберсигурност на ЕС. ▌

Член 14

Изпълнение на подкрепата от резерва за киберсигурност на ЕС

1. Исканията за подкрепа от резерва за киберсигурност на ЕС се оценяват от Комисията с подкрепата на ENISA или както е определено в споразуменията за финансов принос по член 12, параграф 6, а отговорът се предава ***незабавно*** на ползвателите, посочени в член 12, параграф 3, ***и при всички случаи – в рамките на 24 часа.***

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

а) сериозността на киберинцидента;

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

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

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

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

3. Услугите в рамките на резерва за киберсигурност на ЕС се предоставят в съответствие със специални споразумения между доставчика на услуги и ползвателя, на когото се предоставя подкрепата в рамките на резерва за киберсигурност на ЕС. Тези споразумения включват условия за отговорност ***и всякакви други разпоредби, които страните по споразумението считат за необходими за предоставянето на съответната услуга***.

4. 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.***

5. Комисията и ENISA не носят договорна отговорност за вреди, причинени на трети лица от услугите, предоставяни в рамките на изпълнението на резерва за киберсигурност на ЕС, ***освен в случаи на груба небрежност при оценяването на заявлението на доставчика на услуги или когато Комисията или ENISA са ползватели на резерва за киберсигурност на ЕС съгласно член 14, параграф 3.***

6. В срок от един месец след края на действието за подкрепа ползвателите предоставят на Комисията, на ENISA, ***на мрежата на ЕРИКС и, по целесъобразност, на EU-CyCLONe*** обобщен доклад за предоставената услуга, постигнатите резултати и извлечените поуки. Когато ползвателят е от трета държава, както е посочено в член 17, този доклад се предоставя на върховния представител.
Докладът е в съответствие с правото на Съюза и националното право относно защитата на чувствителна или класифицирана информация.

7. Комисията докладва ***редовно и най-малко два пъти годишно*** на групата за сътрудничество за МИС за използването и резултатите от подкрепата. ***Поверителната информация в него е защитена в съответствие с правото на Съюза и националното право относно защитата на чувствителна или класифицирана информация.***

Член 15

Координация с механизмите за управление на кризи

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

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

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

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

Член 16

Доверителни доставчици

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

а) гарантиране, че резервът за киберсигурност на ЕС включва услуги, които могат да се използват във всички държави членки, като се вземат предвид по-

[1] 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).

специално националните изисквания за предоставяне на такива услуги, включително сертифициране или акредитация;

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

в) гарантиране, че резервът за киберсигурност на ЕС носи добавена стойност за ЕС, като допринася за постигането на целите, посочени в член 3 от Регламент (ЕС) 2021/694, включително за насърчаване на развитието на умения в областта на киберсигурността в ЕС ***и за постигането на баланс между половете в сектора, както и за укрепване на технологичния суверенитет, отворената стратегическа автономност, конкурентоспособността и устойчивостта на Съюза.***

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

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

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

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

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

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

е) доставчикът разполага с ***актуализирано*** хардуерно и софтуерно техническо оборудване, необходимо за поддържане на търсената услуга ***и, според случая, спазва Регламент (ЕС) .../... на Европейския парламент и на Съвета[1] (2022/0272(COD))***;

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

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

и) доставчикът е в състояние да достави услугата на местния език на държавата(ите) членка(и) ***или на един от работните езици на институциите на Съюза***, в които той 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, след като схемата бъде приета***, доставчикът се сертифицира в съответствие с тази схема.

йа) доставчикът е в състояние да предоставя услугата самостоятелно, а не като част от пакет, като по този начин той гарантира възможността ползвателят да премине към друг доставчик на услуги;

йб) за целите на член 12, параграф 1 доставчикът включва в предложението по тръжната процедура възможността за преобразуване на неизползваните услуги за реагиране при инциденти в упражнения или обучения;

йв) доставчикът и неговите изпълнителни управленски структури се намират в Съюза, в асоциирана държава или в трета държава, която е страна по Споразумението за държавните поръчки („СДП“) на Световната търговска организация;

йг) . доставчикът не подлежи на контрол от страна на неасоциирана трета държава или субект, който не е страна по СДП, или като друга възможност,

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

този субект се подлага на скрининг по смисъла на Регламент (ЕС) 2019/452 и, при необходимост, на смекчаващи мерки, като се вземат предвид целите, посочени в настоящия регламент.

Член 17

Подкрепа за трети държави

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

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

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

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

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

6. ***Без ненужно забавяне*** Комисията ***уведомява Съвета и*** координира с върховния представител получените искания и изпълнението на подкрепата, предоставена на трети държави от резерва за киберсигурност на ЕС.

Глава IV

МЕХАНИЗЪМ ЗА ПРЕГЛЕД НА КИБЕРИНЦИДЕНТИ

Член 18

Механизъм за преглед на киберинциденти

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

2. За изготвянето на доклада за преглед на инцидент, посочен в параграф 1, ENISA си сътрудничи ***и събира обратна информация от*** всички съответни заинтересовани страни, включително представители на държавите членки, Комисията, други съответни институции, органи, ***служби*** и агенции на ЕС, доставчиците на управлявани услуги за сигурност ***в национални и трансгранични ЦОС*** и ползвателите на услуги за киберсигурност, ***с допълнителни гаранции и наблюдение, които са достатъчни, за да се гарантира, че извлечените поуки и идентифицираните най-добри практики са подкрепени от участниците в сектора на услугите за киберсигурност.*** Когато е целесъобразно, ENISA си сътрудничи и със субекти, засегнати от значителни или мащабни киберинциденти. За да подпомогне прегледа, ENISA може да се консултира и с други видове заинтересовани страни. Консултираните представители оповестяват всеки потенциален конфликт на интереси.

3. Докладът обхваща преглед и анализ на конкретния значителен или мащабен киберинцидент, включително основните причини, уязвимостите и извлечените поуки. Поверителната информация в него е защитена в съответствие с правото на Съюза или националното право относно защитата на чувствителна или класифицирана информация. ***Той не включва подробности за активно използвани уязвимости, които остават некоригирани.***

3а. Докладът, посочен в параграф 1 от настоящия член, съдържа извлечените поуки от партньорските проверки, извършени съгласно член 19 от Директива (ЕС) 2022/2555.

4. Когато е целесъобразно, докладът съдържа препоръки, ***включително за всички съответни заинтересовани страни***, за подобряване на състоянието на киберсигурността на Съюза.

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

Глава V

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 19

Изменения на Регламент (ЕС) 2021/694

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

(1) Член 6 се изменя, както следва:

а) параграф 1 се изменя, както следва:

i) вмъква се следната буква аа):

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

ii) добавя се следната буква ж):

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

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*, с изключение на действията за изпълнение на резерва за киберсигурност на ЕС, които се изпълняват от Комисията и 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 (OB L 202, 8.6.2021 г., стр. 1, ***ELI: https://eur-lex.europa.eu/eli/reg/2021/887/oj?locale=bg).“;***

(2) Член 9 се изменя, както следва:

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

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

в) ***1 620 566 000*** евро за специфична цел 3 — Киберсигурност и доверие;

г) ***500 347 000*** евро за специфична цел 4 — Задълбочени цифрови умения“;

аа) вмъква се следният нов параграф 2а:

„ (2а). Сумата по параграф 2, буква в) се използва основно за постигане на оперативните цели, посочени в член 6, параграф 1, букви а – е) от

програмата.“;

аб) вмъква се следният нов параграф 2б:

„ (2б). Сумата за създаването и прилагането на резерва за киберсигурност на ЕС не надвишава 27 милиона евро за планирания срок на действие на Регламента за определяне на мерки за укрепване на солидарността и способностите на Съюза за откриване, подготовка и реагиране при киберзаплахи и инциденти.“;

б) добавя се следният параграф 8:

„8. ***Чрез*** дерогация ***от*** член 12, параграф 4 от Регламент (ЕС, Евратом) 2018/1046 неизползваните бюджетни кредити за поети задължения и за плащания за действия ***в контекста на изпълнението на резерва за киберсигурност на ЕС***, 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.“;

Комисията информира Парламента и Съвета за пренесените бюджетни кредити съгласно член 12, параграф 6 от Регламент (ЕС, Евратом) 2018/1046.

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

„2. Програмата може да предоставя финансиране под всяка една от формите, предвидени в Регламент ***(ЕС, Евратом) 2018/1046***, включително по-специално чрез поръчки, като основна форма, или чрез безвъзмездни средства и награди.

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

Когато за постигането на целите на действието е необходимо предоставянето на иновативни стоки или услуги, които все още не са налични на широка търговска

основа, възлагащият орган или възложителят може да разреши възлагането на множество договори в рамките на една и съща процедура за възлагане на поръчка.

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

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

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

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

(4) Добавя се следният член 16а:

„Член 16а

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

(5) Член 19 се заменя със следното:

„Безвъзмездните средства по Програмата се отпускат и управляват в съответствие с дял VIII от ***Регламент (ЕС, Евратом) 2018/1046*** и могат да покриват до 100 % от допустимите разходи, без да се засяга принципът на съфинансиране, установен в член 190 от ***Регламент (ЕС, Евратом) 2018/1046***. Такива безвъзмездни средства се отпускат и управляват, както е посочено за всяка специфична цел.

Подкрепа под формата на безвъзмездни средства може да бъде отпускана пряко от ЕССС без покана за представяне на предложения на националните ЦОС, посочени в член 4 от Регламент ***(ЕС) .../...***, и на консорциума, осигуряващ хостинг, посочен в член 5 от Регламент ***(ЕС) .../...***, в съответствие с член 195, параграф 1, буква г) от ***Регламент (ЕС, Евратом) 2018/1046***.

Подкрепа под формата на безвъзмездни средства за Механизма за действие при извънредни ситуации в областта на киберсигурността, както е посочено в член 10 от Регламент ***(ЕС) .../...***, 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 ***Регламент (ЕС, Евратом) 2018/1046***.

За действията, посочени в член 10, параграф 1, буква в) 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.

За подпомагане на взаимопомощта за реагиране на значителен или мащабен киберинцидент, както е определено в член 10, буква в) от Регламент ***(ЕС) .../...***, и в

съответствие с член 193, параграф 2, втора алинея, буква а) от ***Регламент (ЕС, Евратом) 2018/1046***, в надлежно обосновани случаи разходите могат да се считат за допустими, дори ако са направени преди подаването на заявлението за безвъзмездни средства.“

(6) Приложения I и II към Регламент (ЕС) 2021/694 се изменят в съответствие с приложението към настоящия регламент.

Член 19а

Допълнителни ресурси за ENISA

ENISA получава допълнителни ресурси за изпълнение на допълнителните си задачи, които са ѝ възложени с настоящия регламент. Допълнителната подкрепа, включително финансиране, не застрашава постигането на целите на другите програми на Съюза, по-специално програмата „Цифрова Европа“.

Член 20

Оценка *и преглед*

1. До [***две*** години ***от*** датата на прилагането на настоящия регламент] ***и на всеки две години след това*** Комисията ***извършва*** оценка ***на функционирането на мерките, определени*** в настоящия регламент, ***и представя доклад*** на Европейския парламент и на Съвета.

2. В нея се оценяват по-специално:

а) използването и добавената стойност на трансграничните ЦОС и степента, до която те допринасят за ускоряване на откриването и реагирането на киберзаплахи и ситуационната осведоменост; активното участие на

националните ЦОС в европейския киберщит, включително броя на създадените национални ЦОС и трансгранични ЦОС, както и степента, в която той е допринесъл за създаването и обмена на висококачествена приложима информация и на разузнавателна информация за киберзаплахи; броя на и разходите за съвместно придобитите инфраструктури или инструменти за киберсигурност, или и двете; броя на споразуменията за сътрудничество, сключени между трансграничните ЦОС и с ISAC за промишлеността; броя на инцидентите, докладвани на мрежата на ЕРИКС, и въздействието, което той оказва върху работата на мрежата на ЕРИКС;

б) както положителните, така и отрицателните аспекти на работата на Механизма за действие при извънредни ситуации в областта на киберсигурността, включително дали са необходими допълнителни изисквания за сътрудничество или обучение;

в) приноса на настоящия регламент за укрепване на устойчивостта и отворената стратегическа автономност на Съюза, за подобряване на конкурентоспособността на съответните промишлени сектори, микропредприятията, МСП, включително новосъздадените предприятия, и за развитието на умения в областта на киберсигурността в Съюза;

г) използването и добавената стойност на резерва за киберсигурност на ЕС, включително броя на доверителните доставчици на услуги за сигурност, които са част от резерва за киберсигурност на ЕС; броя, вида, разходите и последиците от действията, извършени в подкрепа на реагирането при киберинциденти, както и на техните ползватели и доставчици; средното време, необходимо на Комисията да отчете наличието на инцидент, на резерва за киберсигурност на ЕС да бъде внедрен и да реагира, и на ползвателя да се възстанови от инцидентите; дали обхватът на резерва за киберсигурност на ЕС следва да бъде разширен, така че да включва услуги за готовност при инциденти или съвместни учения с доверителните доставчици на управлявани услуги за сигурност и потенциалните ползватели на резерва за киберсигурност на ЕС, за да се гарантира ефективното функциониране на резерва, когато е необходимо;

д) приноса на настоящия регламент за развитието и подобряването на уменията и компетентностите на работната сила в сектора на киберсигурността, необходими за укрепване на капацитета на Съюза за откриване, предотвратяване, реагиране и възстановяване от киберзаплахи и инциденти;

е) приноса на настоящия регламент за внедряването и разработването на най-съвременни технологии в Съюза.

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 20а

Упражняване на делегирането

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 6, параграф 3, член 7, параграф 2, член 12, параграф 8 и член 13, параграф 7, се предоставя на Комисията за срок от ... години, считано от ... [датата на влизане в сила на основния законодателен акт или всяка друга дата, определена от съзаконодателите]. Комисията изготвя доклад относно делегирането на правомощия не по-късно от девет месеца преди изтичането на ...годишния 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.

3. Делегирането на правомощия, посочено в член 6, параграф 3, в член 7, параграф 2, в член 12, параграф 8 и в член 13, 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 6, параграф 3, член 7, параграф 2, член 12, параграф 8 или член 13, параграф 7, влиза в сила единствено ако нито Европейският парламент, нито Съветът са направили възражения в срок от два месеца след нотифицирането на акта на Европейския парламент и на Съвета или ако преди изтичането на този срок Европейският парламент и Съветът са уведомили Комисията, че няма да представят възражения. Посоченият срок може да се удължи с [два месеца] по инициатива на Европейския парламент или на Съвета.

Член 21

Процедура на комитет

1. Комисията се подпомага от координационния комитет на програмата „Цифрова Европа“, създаден с Регламент (ЕС) 2021/694. Този комитет е комитет по смисъла на Регламент (ЕС) 182/2011.

2. При позоваване на настоящия параграф се прилага член 5 от Регламент (ЕС) 182/2011.

Член 22

Влизане в сила

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

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

Съставено в Страсбург на […] година.

За Европейския парламент	*За Съвета*
Председател	*Председател*

ПРИЛОЖЕНИЕ

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

(1) В приложение I разделът/главата „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, ситуационна осведоменост в киберпространството, включително национални ЦОС и трансгранични ЦОС, формиращи европейския киберщит, 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, ***със специален акцент върху постигането на баланс между половете в сектора,*** например чрез съгласуване на програмите за изграждане на умения в тази област с цел те да се адаптират към специфичните секторни нужди***, включително междудисциплинарна и обща насоченост,*** и да се улесни достъпът до целенасочено специализирано обучение***, за да се предостави възможност на всички хора и територии, без да се засяга възможността да се възползват от предвидените в настоящия регламент възможности***.

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

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

„Специфична цел 3 — Киберсигурност и доверие

3.1. Брой на съвместно придобитите ***като част от киберщита*** инфраструктури или инструменти за киберсигурност, или и двете

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

3.3. Брой***, вид, разходи и последици от*** действията***, извършени*** в подкрепа на готовността и реагирането при киберинциденти в рамките на Механизма за действие при извънредни ситуации в областта на киберсигурността. ***Степента, в която препоръките от изпитванията на готовността са били изпълнени и извършени от ползвателя, както и средното време, необходимо на Комисията да отчете наличието на инцидент, на резерва за киберсигурност на ЕС да реагира и на ползвателя да се възстанови от инцидентите.“***