Съвет на
Европейския съюз

Брюксел, 22 март 2022 г.
(OR. en)

7474/22

Междуинституционално досие:
2022/0085(COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

ПРЕДЛОЖЕНИЕ

От:	Генералния секретар на Европейската комисия, подписано от г-жа Martine DEPREZ, директор
Дата на получаване:	22 март 2022 г.
До:	Г-н Jeppe TRANHOLM-MIKKELSEN, генерален секретар на Съвета на Европейския съюз
№ док. Ком.:	COM(2022) 122 final
Относно:	Предложение за РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза

Приложено се изпраща на делегациите документ COM(2022) 122 final.

Приложение: COM(2022) 122 final

ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 22.3.2022 г.
COM(2022) 122 final

2022/0085 (COD)

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза

{SWD(2022) 67 final} - {SWD(2022) 68 final}

ОБЯСНИТЕЛЕН МЕМОРАНДУМ

1. КОНТЕКСТ НА ПРЕДЛОЖЕНИЕТО

• Основания и цели на предложението

С настоящото предложение се създава рамка за осигуряване на общи правила и мерки в областта на киберсигурността в институциите, органите и агенциите на Съюза. То има за цел да се подобрят допълнително устойчивостта на всички субекти и капацитетът им за реагиране при инциденти. То е съобразено с приоритетите на Комисията за привеждане на Европа в готовност за цифровата ера и за изграждането на приспособена към бъдещите предизвикателства икономика, която работи в интерес на хората. Освен това осигуряването на сигурна и устойчива публична администрация е крайъгълен камък в цифровата трансформация на обществото като цяло.

Настоящото предложение се основава на Стратегията на ЕС за Съюза на сигурност (COM(2020) 605 final) и Стратегията на ЕС за киберсигурност за цифровото десетилетие (JOIN(2020) 18 final).

С предложението се модернизира съществуващата правна уредба на CERT-EU и се отчитат промените и повишаването на цифровизацията в институциите, органите и агенциите през последните години, както и развиващата се картина на заплахите за киберсигурността. Тези две тенденции на развитие се засилиха допълнително след началото на кризата с COVID-19, като броят на инцидентите продължава да нараства с осъществяването на все по-сложни атаки от широк кръг източници.

С предложението CERT-EU се преименува от „екип за незабавно реагиране при компютърни инциденти“ на „Център за киберсигурност“ за институциите, органите и агенциите на Съюза в съответствие с развитието в държавите членки и в световен мащаб, при което много екипи за незабавно реагиране при компютърни инциденти се преименуват на центрове за киберсигурност, но се запазва краткото наименование „CERT-EU“ тъй като то вече е познато.

• Съгласуваност с действащите разпоредби в тази област на политиката

Целта на настоящото предложение е да се повиши устойчивостта в областта на киберсигурността на институциите, органите и агенциите на Съюза срещу киберзаплахи, като същевременно то е съгласувано с действащото законодателство:

- Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза; То също така е съгласувано с предложението за Директива (ЕС) XXXX/XXXX относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148 [предложение за МИС 2];

- Регламент (ЕС) 2019/881 относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии (Акт за киберсигурността);

- предложение за Регламент (ЕС) XXXX/XXXX относно информационната сигурност в институциите, органите, службите и агенциите на Съюза.

- Препоръка на Комисията от 23 юни 2021 г. за изграждането на съвместно киберзвено;

- Препоръка (ЕС) 2017/1584 на Комисията от 13 септември 2017 г. относно координирана реакция на мащабни киберинциденти и кризи.

В приложението към Препоръка (ЕС) 2017/1584 на Комисията от 13 септември 2017 г. относно координирана реакция на мащабни киберинциденти и кризи се определя концепцията за координирана реакция на мащабни трансгранични киберинциденти и кризи.

В резолюцията си от 9 март 2021 г. Съветът на Европейския съюз подчерта, че киберсигурността е от жизненоважно значение за функционирането на публичната администрация както на национално равнище, така и на равнище ЕС, а също и за обществото и икономиката като цяло, като подчерта значението на стабилната и последователна рамка за сигурност с цел защита на всички служители, данни, комуникационни мрежи, информационни системи и процеси по вземане на решения на ЕС. По-специално това трябва да се постигне чрез повишаване на устойчивостта и подобряване на културата на сигурност в институциите, органите и агенциите на Съюза. Трябва да се осигурят достатъчно ресурси и капацитет, включително в контекста на укрепването на мандата на CERT-EU.

2. ПРАВНО ОСНОВАНИЕ, СУБСИДИАРНОСТ И ПРОПОРЦИОНАЛНОСТ

• Правно основание

Правното основание за настоящия регламент е член 298 от Договора за функционирането на Европейския съюз (ДФЕС), който предвижда, че институциите, органите, службите и агенциите на Съюза изпълняват своите задачи с подкрепата на открита, ефикасна и независима европейска администрация. В съответствие с правилника и условията за работа, приети въз основа на член 336, Европейският парламент и Съветът, като действат чрез регламенти, в съответствие с обикновената законодателна процедура, приемат разпоредби за тази цел.

Информационните технологии осигуряват за институциите, органите и агенциите на Съюза нови начини за работа, взаимодействие с гражданите и подобряване на цялостната им дейност. Тъй като технологиите продължават да се развиват, картината на киберзаплахите се развива успоредно с тях. Институциите, органите и агенциите на Съюза се превърнаха в изключително привлекателни обекти на сложни кибератаки. Създаването на системи и изисквания за гарантиране на киберсигурността изглежда допринася за ефективността и независимостта на европейската администрация, така че институциите, органите, службите и агенциите на Съюза да могат да работят по-ефективно в цифровия свят при изпълнението на своите мисии.

Освен това, както е обяснено в раздел 3 по-долу, съществуващите понастоящем различия по отношение на ситуацията в институциите, органите и агенциите на Съюза и следвания от тях подход по отношение на киберсигурността са допълнителни пречки пред постигането на открита, ефикасна и независима европейска администрация. Без

общ подход ситуацията в отделните институции, органи и агенции на Съюза по отношение на киберсигурността ще продължи да се развива в различни посоки. Следователно това правно основание е целесъобразно, като се има предвид, че Регламентът има за цел да създаде обща правна уредба за киберсигурността в рамките на институциите, органите, службите и агенциите на Съюза.

- **Субсидиарност**

Регламентът за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза попада в рамките на изключителната компетентност на Съюза.

- **Пропорционалност**

Правилата, предложени в настоящия регламент, не надхвърлят необходимото за постигането на конкретните цели по задоволителен начин. Предвидените мерки ще допринесат за постигането на високо общо ниво на киберсигурност, без да се надхвърля необходимото за постигане на целта с оглед на все по-големите рискове, пред които са изправени институциите и органите на Съюза.

- **Избор на инструмент**

Счита се, че изборът на регламент, който е пряко приложим, е подходящият правен инструмент за определяне и рационализиране на задълженията, наложени на институциите, органите и агенциите на Съюза. Регламентът е най-подходящият правен инструмент, за да се даде възможност за целенасочени подобрения.

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

- **Предварителни оценки**

CERT-EU извърши оценка на основните киберзаплахи, на които институциите, органите и агенциите на Съюза са изложени понастоящем или е вероятно да бъдат изложени в обозримо бъдеще.

В анализа бяха използвани три категории наблюдения:

- опити за пробив в ИТ инфраструктурата на институциите, органите и агенциите на Съюза (когато са успешни, те се третират като инциденти, а в останалите случаи се регистрират като засечени опити);
- засечени заплахи в близост до институциите, органите и агенциите на Съюза (например в свързаните с тяхната дейност сектори, в общностите на техните заинтересовани страни или в Европа);
- основни тенденции по отношение на заплахите, наблюдавани в световен мащаб.

Освен това в рамките на анализа беше отчетено как основните текущи промени се отразяват на начините, по които институциите на Съюза управляват и използват своята ИТ инфраструктура и услуги. Тези промени включват:

- увеличаване на работата от разстояние;
- прехвърляне на системи към изчислителния облак;
- увеличаване на възлагането на ИТ услуги на подизпълнители.

Между 2019 г. и 2021 г. броят на значимите инциденти[1], засягащи институциите, органите и агенциите на Съюза, предизвикани от автори на т.нар. „съвременни упорити заплахи“ (APT), нарасна драстично. През първата половина на 2021 г. броят на значимите инциденти съответстваше на инцидентите през цялата 2020 г. Това проличава и от броя на цифровите копия за криминалистична експертиза (копия на съдържанието на засегнатите системи или устройства към даден момент), анализирани от CERT-EU през 2020 г., който се утрои в сравнение с 2019 г., като броят на значимите инциденти се увеличи повече от десет пъти от 2018 г. насам.

През 2020 г. управителният съвет на CERT-EU определи нова стратегическа цел за CERT-EU, а именно да гарантира всеобхватно ниво на кибернетична отбрана за всички институции, органи и агенции с подходящ обхват и дълбочина, която непрекъснато се адаптира към актуални или предстоящи заплахи, включително атаки срещу мобилни устройства, облачната среда и устройства, свързани към интернет на предметите.

В допълнение към извършения от CERT-EU анализ на заплахите Комисията извърши оценка на функционирането на киберсигурността на 20 институции, органи и агенции на Съюза. Това даде представа за установените практики в областта на киберсигурността и за капацитета за управление на киберсигурността чрез външна сравнителна оценка на някои технически проверки, свързани със сигурността.

Тази оценка се основаваше на въпросници, на които тези институции, органи и агенции предоставиха отговори, на публично достъпни данни и на данни, предоставени пряко от самите институции, органи и агенции на Съюза. Тя осигурява достатъчно информация за настоящата ситуация, която позволява да се достигне до следните заключения:

- степента на зрялост на киберсигурността, размерът на ИТ инфраструктурата и равнищата на капацитета се различават значително сред оценените институции, органи и агенции на Съюза;
- макар че много институции, органи и агенции на Съюза като цяло разполагат с развит капацитет за откриване и реагиране на киберзаплахи, капацитетът им за управление на киберсигурността се характеризира с различни равнища на интегрирано управление на риска;
- макар че като цяло рамките за киберсигурност (стратегия, политика и база от правила) на оценените институции, органи и агенции на Съюза са добре

[1] „Значим инцидент“ означава всеки инцидент, освен ако е с ограничено въздействие и има вероятност вече да е добре изяснен от гледна точка на метода или технологията.

установени в основните области на киберсигурността, изброени в приложение I към Регламента, в някои институции, органи и агенции на Съюза управлението на непрекъснатостта на дейностите, спазването на изискванията, одитът и непрекъснатото подобряване не са достатъчно зрели;

- беше установено, че техническите мерки, считани за най-добри практики, не се прилагат по еднакъв начин от оценените институции, органи и агенции на Съюза.

Накратко, анализът на 20-те институции, органи и агенции на Съюза показва, че тяхното управление, киберхигиена, цялостен капацитет и зрялост варират в широк спектър. Поради това изискването всички институции, органи и агенции на Съюза да прилагат базов набор от мерки за киберсигурност е от основно значение за преодоляване на това несъответствие в степента на зрялост и за постигане на високо общо ниво на киберсигурност във всички институции, органи и агенции на Съюза.

Към настоящия момент няма законодателство на Съюза, което да е насочено към киберсигурността на институциите, органите и агенциите на Съюза и да предвижда мерки за цялостно справяне със заплахите за киберсигурността и с нововъзникващите ИТ рискове, породени от цифровизацията.

- **Консултации със заинтересованите страни**

Комисията проведе консултации със заинтересованите страни във всички институции, органи и агенции на Съюза, както и с представители на държавите членки в Съвета и със заинтересованите страни в Европейския парламент. На 25 юни 2021 г. представители на държавите членки и съответните заинтересовани страни от институциите, органите и агенциите на Съюза участваха в организиран от Комисията работен семинар за обсъждане на съдържанието на бъдещото предложение за регламент.

- **Оценка на въздействието**

Настоящото предложение ще окаже въздействие върху институциите, органите и агенциите на Съюза. Тъй като то няма да се прилага за държавите членки, не е необходима конкретна оценка на въздействието.

- **Основни права**

Европейският съюз е поел ангажимент да гарантира високи стандарти на защита на основните права. Цялото споделяне на информация въз основа на настоящия регламент би се осъществявало в надеждна среда при пълно зачитане на правото на защита на личните данни, предвидено в член 8 от Хартата на основните права на Европейския съюз и в съответното законодателство за защита на данните, по-специално Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета.

4. ОТРАЖЕНИЕ ВЪРХУ БЮДЖЕТА

Сравнителните пазарни оценки и проучванията[2] сочат, че преките разходи за киберсигурност обикновено варират между 4 и 7 % от общите разходи за ИТ на организациите. Извършеният от CERT-EU анализ на заплахите в подкрепа на настоящото законодателно предложение обаче показва, че международните органи и политическите организации са изправени пред повишени рискове, поради което изглежда по-подходящо да се заложи цел от 10 % на ИТ разходите за киберсигурност. Точните разходи за тези усилия не могат да бъдат определени поради липсата на подробна информация относно ИТ разходите на институциите, органите и агенциите на Съюза и относно съответния дял на разходите за киберсигурност.

Макар че поради това много институции, органи и агенции на Съюза вероятно изразходват по-малко средства за киберсигурност, отколкото би следвало, настоящият регламент сам по себе си няма да доведе до увеличение на тези текущи разходи. Дори без регламента всеки субект ще трябва да гарантира адекватно ниво на киберсигурност. С регламента се продължава предишното сътрудничество в рамките на управителния съвет на CERT-EU и се придава официален характер на вече съществуващия понастоящем частичен обмен на информация. Както е посочено в законодателната финансова обосновка, CERT-EU ще се нуждае от допълнителни ресурси, за да изпълнява своята разширена роля, и тези ресурси следва да бъдат преразпределени от институциите, органите и агенциите на Съюза, които се ползват от услугите на CERT-EU.

5. ДРУГИ ЕЛЕМЕНТИ

- **Механизми за прилагане, мониторинг, оценка и докладване**

Междуинституционалният съвет по киберсигурността (МСК), със съдействието на CERT-EU, следва да провежда прегледи на функционирането на настоящия регламент, да извършва оценки и да представя на Комисията доклади за констатациите си. Комисията следва да докладва редовно на Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите.

CERT-EU може да изготви предложение за документ с насоки или за препоръка, което МСК може да избере да приеме. Документът с насоки представлява документ със съвети, насочен към всички институции, органи и агенции на Съюза или към част от тях, докато препоръката е насочена към отделни институции, органи и агенции на Съюза. Призивът за действие представлява документ със съвети на CERT-EU, в който се описват спешни мерки за сигурност, които институциите, органите и агенциите на Съюза настоятелно се призовават да предприемат в рамките на определен срок.

- **Подробно разяснение на отделните разпоредби на предложението**

[2] Източник: Gartner, „Identifying the Real Information Security Budget“ (Определяне на реалния бюджет за информационна сигурност) (2016 г.). Това е в допълнение към непреките разходи за ИТ сигурност, например за мрежова сигурност като защитни стени, антивирусни програми и отговорности на собственика на системата, като например оценка на риска и прилагането на проверки, свързани със сигурността. В документ от 2020 г. разходите за киберсигурност във финансовите институции се определят на 10—11 % от ИТ разходите, източник: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

Общи разпоредби

С Регламента се определят мерки за гарантиране на високо общо ниво на киберсигурност, като той се прилага към институциите, органите и агенциите на Съюза, за да им се даде възможност да изпълняват съответните си задачи по открит, ефикасен и независим начин. (членове 1—3 и 23—25)

Мерки за високо общо ниво на киберсигурност

Институциите, органите и агенциите на Съюза са задължени да създадат вътрешна рамка за управление, ръководство и контрол на рисковете за киберсигурността, която да гарантира ефективно и разумно управление на всички рискове за киберсигурността. Освен това институциите, органите и агенциите приемат базов набор от мерки за киберсигурност, насочен към преодоляване на установените рискове в съответствие с рамката, извършват редовни оценки на зрелостта на киберсигурността и приемат план за киберсигурност. (членове 4—8)

Междуинституционален съвет по киберсигурност

Създава се Междуинституционален съвет по киберсигурност, който отговаря за наблюдението на прилагането на настоящия регламент от страна на институциите, органите и агенциите на Съюза, за надзора по отношение на изпълнението на общите приоритети и цели от страна на CERT-EU и за предоставянето на стратегически насоки на CERT-EU. (членове 9—11)

CERT-EU

CERT-EU допринася за сигурността на ИТ средата на всички институции, органи и агенции на Съюза, като им предоставя съвети, осигурява подкрепа за предотвратяването, откриването, смекчаването и реагирането на инциденти и действа като техен координационен център за обмен на информация и реагиране при инциденти в областта на киберсигурността. (членове 12—17)

Задължения за сътрудничество и докладване

Регламентът гарантира сътрудничеството и обмена на информация между CERT-EU и институциите, органите и агенциите на Съюза с цел изграждане на доверие. За тази цел CERT-EU може да поиска от институциите, органите и агенциите на Съюза да му предоставят съответната информация и може да обменя информация за конкретни инциденти с институциите, органите и агенциите на Съюза, за да се улесни откриването на подобни киберзаплахи или инциденти, без да е необходимо съгласието на засегнатия заинтересован субект. CERT-EU може да обменя информация за конкретен инцидент, от която става ясна мишената на киберинцидента, само със съгласието на засегнатия заинтересован субект.

По-специално всички институции, органи и агенции на Съюза уведомяват CERT-EU за значителни киберзаплахи, значителни уязвимости и значими инциденти без ненужно забавяне и във всеки случай не по-късно от 24 часа след като са узнали за тях. (членове 18—22)

2022/0085 (COD)

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз, и по-специално член 298 от него,

като взеха предвид Договора за създаване на Европейската общност за атомна енергия, и по-специално член 106а него от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

(1) В цифровата ера информационните и комуникационните технологии са крайъгълен камък на откритата, ефикасна и независима администрация на Съюза. Развиващите се технологии и повишената сложност и взаимосвързаност на цифровите системи увеличават рисковете за киберсигурността, в резултат на което администрацията на Съюза става по-уязвима за киберзаплахи и киберинциденти, което в крайна сметка поражда заплахи за непрекъснатостта на нейната дейност и за способността ѝ да гарантира сигурността на своите данни. Въпреки че в днешно време засиленото използване на облачни услуги, повсеместното използване на информационни технологии, високата степен на цифровизация, дистанционната работа и развиващите се технологии и свързаност представляват основни характеристики на всички дейности на образуванията, изграждащи администрацията на Съюза, все още не е налице достатъчно ниво на цифрова устойчивост.

(2) Картината на киберзаплахите, пред които са изправени институциите, органите и агенциите на Съюза, непрекъснато се развива. Тактиката, техниките и процедурите, използвани от авторите на заплахи, непрекъснато се развиват, докато най-честите мотиви за подобни атаки почти не се променят: от кражба на ценна неразкрита информация до сдобиване с парични средства, манипулиране на общественото мнение или подкопаване на цифровата инфраструктура. Продължава да расте темпът, с който те осъществяват своите кибератаки, а същевременно кампаниите им стават все по-сложни и автоматизирани, като са

насочени срещу открити за атаки области, които продължават да се разширяват, и уязвимостите бързо се използват.

(3) ИТ средите на институциите, органите и агенциите на Съюза се характеризират с взаимозависимост и с интегрирани потоци от данни, а ползвателите им са изградили тясно сътрудничество. Тази взаимосвързаност означава, че всяко прекъсване, дори когато първоначално е ограничено само до една институция, орган или агенция на Съюза, може да породи каскадни ефекти в по-широк план, което потенциално да доведе до широкообхватни и дълготрайни отрицателни въздействия върху останалите субекти. Освен това ИТ средите на някои институции, органи и агенции са свързани с ИТ средите на държавите членки, в резултат на което инцидент в един субект на Съюза би могъл да породи риск за киберсигурността на ИТ средите на държавите членки и обратното.

(4) Институциите, органите и агенциите на Съюза са привлекателни мишени, като са изправени пред висококвалифицирани и добре обезпечени с ресурси автори на заплахи, както и пред други заплахи. Същевременно съществуват значителни разлики в нивото и зрелостта на кибернетичната устойчивост на тези субекти и в способността им за откриване и реагиране на злонамерени действия в киберпространството. Поради това за функционирането на европейската администрация е необходимо институциите, органите и агенциите на Съюза да се постигне високо общо ниво на киберсигурност чрез базов набор от мерки за киберсигурност (набор от минимални правила за киберсигурност, които мрежите и информационните системи и техните оператори и ползватели трябва да спазват, за да се сведат до минимум рисковете за киберсигурността), обмен на информация и сътрудничество.

(5) Директивата [предложение за МИС 2] относно мерки за високо общо ниво на киберсигурност в целия Съюз има за цел да се подобрят допълнително устойчивостта в областта на киберсигурността и капацитетът за реагиране при инциденти на публичните и частните субекти, на националните компетентни органи и субекти, както и на Съюза като цяло. Поради това е необходимо институциите, органите и агенциите на Съюза да последват този пример чрез осигуряването на правила, които са в съответствие с Директивата [предложение за МИС 2] и се характеризират със същото равнище на амбиция.

(6) За да се постигне високо общо ниво на киберсигурност, е необходимо всяка институция, орган и агенция на Съюза да създаде вътрешна рамка за управление, ръководство и контрол на рисковете за киберсигурността, която да гарантира ефективно и разумно управление на всички рискове за киберсигурността и в която да се вземат предвид управлението на кризи и непрекъснатостта на дейността.

(7) Разликите между институциите, органите и агенциите на Съюза изискват гъвкавост при изпълнението, тъй като няма да е възможно използването на универсално решение. Мерките за високо общо ниво на киберсигурност не следва да включват задължения, които директно възпрепятстват изпълнението на задачите на институциите, органите и агенциите на Съюза или нарушават тяхната институционална автономност. Поради това тези институции, органи и агенции следва да създадат свои собствени рамки за управление, ръководство и

контрол на рисковете за киберсигурността и да приемат свои собствени базови набори от мерки и планове за киберсигурност.

(8) С цел да се избегне налагането на несъразмерна финансова и административна тежест върху институциите, органите и агенциите на Съюза изискванията за управление на риска за киберсигурността следва да бъдат съразмерни с риска, който съществува по отношение на съответната мрежа и информационна система, като се отчитат последните постижения в областта на тези мерки. Всяка институция, орган и агенция на Съюза следва да се стреми да отдели подходяща част от своя ИТ бюджет за подобряване на равнището си на киберсигурност, като в дългосрочен план следва да бъде заложена цел от порядъка на 10 %.

(9) Високото общо ниво на киберсигурност изисква поставянето на киберсигурността под надзора на най-високото равнище на управление на всяка институция, орган и агенция на Съюза, като то следва да одобри базов набор от мерки за киберсигурност, насочен към преодоляване на рисковете, установени в съответствие с рамката, която трябва да се въведе от всяка институция, орган и агенция. Предприемането на действия във връзка с културата на киберсигурност, т.е. ежедневното практикуване на киберсигурност, е неразделна част от базовия набор от мерки за киберсигурност във всички институции, органи и агенции на Съюза.

(10) Институциите, органите и агенциите на Съюза следва да оценяват рисковете в отношенията с доставчиците на стоки и услуги, включително доставчиците на услуги за съхранение и обработка на данни или на услуги за управление на сигурността, и да предприемат подходящи мерки за справяне с тях. Тези мерки следва да представляват част от базовия набор от мерки за киберсигурност и да бъдат допълнително уточнени в документи с насоки или препоръки, отправени от CERT-EU. При определянето на мерки и насоки следва надлежно да се вземат предвид съответното законодателство и политики на ЕС, включително оценките на риска и препоръките, отправени от групата за сътрудничество за МИС, като например координираната оценка на риска на равнището на ЕС и инструментариума на ЕС за киберсигурност на 5G технологиите. Освен това би могло да се изисква сертифициране на съответните ИКТ продукти, услуги и процеси съгласно конкретни схеми на ЕС за сертифициране на киберсигурността, приети в съответствие с член 49 от Регламент (ЕС) 2019/881.

(11) През май 2011 г. генералните секретари на институциите и органите на Съюза решиха да създадат експериментален екип за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на Съюза (CERT-EU), чийто контрол се осъществява от междуинституционален управителен съвет. През юли 2012 г. генералните секретари потвърдиха практическите договорености и постигнаха съгласие CERT-EU да просъществува като постоянна структура и да продължи да спомага за подобряването на общото ниво на сигурност на информационните технологии на институциите, органите и агенциите на Съюза като пример за видимо междуинституционално сътрудничество в областта на киберсигурността. CERT-EU беше създаден през септември 2012 г. като работна група на Европейската комисия с междуинституционален мандат. През декември 2017 г. институциите и органите на Съюза сключиха междуинституционална договореност относно

организацията и функционирането на CERT-EU[3]. Тази договореност следва да продължи да се развива в подкрепа на прилагането на настоящия регламент.

(12) CERT-EU следва да се преименува от „екип за незабавно реагиране при компютърни инциденти“ на „Център за киберсигурност“ за институциите, органите и агенциите на Съюза в съответствие с развитието в държавите членки и в световен мащаб, при което много екипи за незабавно реагиране при компютърни инциденти се преименуват на центрове за киберсигурност, но следва да се запази краткото наименование „CERT-EU“ тъй като то вече е познато.

(13) Много кибератаки представляват част от по-широкообхватни кампании, насочени към групи от институции, органи и агенции на Съюза или заинтересовани общности, които включват институции, органи и агенции на Съюза. За да се даде възможност за проактивно откриване и реагиране на инциденти или предприемане на смекчаващи мерки, институциите, органите и агенциите на Съюза следва да уведомяват CERT-EU за значителни киберзаплахи, значителни уязвимости и значими инциденти и да споделят подходящи технически подробности, които позволяват откриване или смекчаване, както и реагиране на подобни киберзаплахи, уязвимости и инциденти в други институции, органи и агенции на Съюза. Като се следва същият подход като предвидения в Директива [предложение за МИС 2], когато субектите узнаят за значим инцидент, те следва да бъдат задължени да подадат първоначално уведомление до CERT-EU в срок от 24 часа. Този обмен на информация следва да даде възможност на CERT-EU да разпространи информацията до останалите институции, органи и агенции на Съюза, както и до подходящи партньори, за да се спомогне за защитата на ИТ средите на Съюза и тези на неговите партньори срещу подобни инциденти, заплахи и уязвимости.

(14) В допълнение към възлагането на повече задачи и разширена роля на CERT-EU следва да се създаде Междуинституционален съвет по киберсигурност (МСК), който следва да улеснява високото общо ниво на киберсигурност сред институциите, органите и агенциите на Съюза чрез мониторинг на прилагането на настоящия регламент от страна на институциите, органите и агенциите на Съюза, чрез надзор на изпълнението на общите приоритети и цели от страна CERT-EU и чрез предоставяне на стратегически насоки на CERT-EU. МСК следва да гарантира представителство на институциите и да включва представители на агенциите и органите чрез Мрежата от агенции на Съюза.

(15) CERT-EU следва да подпомага изпълнението на мерки за високо общо ниво на киберсигурност чрез представяне на предложения за документи с насоки и за препоръки на МСК или чрез отправяне на призиви за действие. Тези документи с насоки и препоръки следва да се одобряват от МСК. При необходимост CERT-EU следва да отправя призиви за действие с описани спешни мерки за сигурност, които институциите, органите и агенциите на Съюза настоятелно се призовават да предприемат в рамките на определен срок.

[3] ОВ C 12, 13.1.2018 г., стр. 1—11.

(16) МСК следва да наблюдава спазването на настоящия регламент и предприемането на последващи действия във връзка с документите с насоки, препоръките и призивите за действие, отправени от CERT-EU. МСК следва да се подпомага по технически въпроси от технически консултативни групи, съставени по преценка на МСК, които следва да работят в тясно сътрудничество със CERT-EU, с институциите, органите и агенциите на Съюза и с други заинтересовани страни, ако е необходимо. При необходимост МСК следва да отправя необвързващи предупреждения и да препоръчва провеждането на одити.

(17) На CERT-EU следва да е възложена мисията да допринася за сигурността на ИТ средата на всички институции, органи и агенции на Съюза. CERT-EU следва да действа като еквивалент на определения координатор за институциите, органите и агенциите на Съюза с цел координирано оповестяване на уязвимости в Европейския регистър на уязвимостите, както е посочено в член 6 от Директива [предложение за МИС 2].

(18) През 2020 г. управителният съвет на CERT-EU определи нова стратегическа цел за CERT-EU, а именно да гарантира всеобхватно ниво на кибернетична отбрана за всички институции, органи и агенции на Съюза с подходящ обхват и дълбочина, която непрекъснато се адаптира към актуални или предстоящи заплахи, включително атаки срещу мобилни устройства, облачната среда и устройства, свързани към интернет на предметите. Стратегическата цел включва също така широкообхватни центрове за операции по сигурността (ЦОС), които наблюдават мрежите, както и 24-часово наблюдение 7 дни в седмицата за заплахи със сериозни последици. По отношение на по-големите институции, органи и агенции на Съюза CERT-EU следва да подпомага техните ИТ екипи, включително чрез 24-часово наблюдение 7 дни в седмицата на първа линия. Що се отнася до по-малките и някои средни институции, органи и агенции на Съюза, CERT-EU следва да предоставя всички услуги.

(19) CERT-EU следва също така да изпълнява предвидената му роля в Директива [предложение за МИС 2] по отношение на сътрудничеството и обмена на информация с мрежата на екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС). Освен това в съответствие с Препоръка (ЕС) 2017/1584 на Комисията[4] CERT-EU следва да си сътрудничи и да координира реакцията със съответните заинтересовани страни. За да допринесе за постигането на високо ниво на киберсигурност навсякъде в Съюза, CERT-EU следва да споделя с националните партньори информация за конкретни инциденти. CERT-EU следва също така да си сътрудничи с други публични и частни партньори, включително в НАТО, след предварително одобрение от МСК.

(20) При подпомагане на оперативната киберсигурност CERT-EU следва да използва наличния експертен опит на Агенцията на Европейския съюз за киберсигурност чрез структурирано сътрудничество, както е предвидено в Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета[5]. Когато е целесъобразно,

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

[5] 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

следва да бъдат сключени специални договорености между двете организации, за да се определи практическото изражение на това сътрудничество и да се избегне дублирането на дейности. CERT-EU следва да си сътрудничи с Агенцията на Европейския съюз за киберсигурност във връзка с анализа на заплахите и редовно да споделя с Агенцията своя доклад относно картината на заплахите.

(21) При подпомагане на съвместното киберзвено, изградено в съответствие с препоръката на Комисията от 23 юни 2021 г.[6], CERT-EU следва да си сътрудничи и да обменя информация със заинтересованите страни, за да се насърчи оперативното сътрудничество и да се даде възможност на съществуващите мрежи да реализират пълния си потенциал за защита на Съюза.

(22) Всяко обработване на лични данни съгласно настоящия регламент следва да се извършва в съответствие със законодателството за защита на данните, включително Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета[7].

(23) При обработката на информация от страна на CERT-EU и институциите, органите и агенциите на Съюза следва да се спазват правилата, определени в Регламент [предложения регламент относно информационната сигурност]. За да се гарантира координация по въпросите на сигурността, всички контакти със CERT-EU, инициирани или поискани от националните служби за сигурност и разузнаване, следва да бъдат съобщавани без ненужно забавяне на дирекцията по сигурността на Комисията и на председателя на МСК.

(24) Тъй като услугите и задачите на CERT-EU са в интерес на всички институции, органи и агенции на Съюза, всяка институция, орган и агенция на Съюза с ИТ разходи следва да участва със справедлив дял в тези услуги и задачи. Тези вноски не засягат бюджетната автономност на институциите, органите и агенциите на Съюза.

(25) МСК, със съдействието на CERT-EU, следва да извършва преглед и оценка на прилагането на настоящия регламент и да докладва констатациите си на Комисията. Въз основа на тази информация Комисията следва да докладва на Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите,

---

киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019 г., стр. 15).

6 Препоръка C(2021) 4520 на Комисията от 23.6.2021 г. за изграждането на съвместно киберзвено.

7 Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39).

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

ГЛАВА I
ОБЩИ РАЗПОРЕДБИ

Член 1
Предмет

С настоящия регламент се определят:

а) задължения за институциите, органите и агенциите на Съюза да създадат вътрешна рамка за управление, ръководство и контрол на рисковете за киберсигурността;

б) задължения за институциите, органите и агенциите на Съюза за управление и докладване на рисковете за киберсигурността;

в) правила за организацията и функционирането на Центъра за киберсигурност за институциите, органите и агенциите на Съюза (CERT-EU) и за организацията и функционирането на Междуинституционалния съвет по киберсигурност.

Член 2
Обхват

Настоящият регламент се прилага за управлението, ръководството и контрола на рисковете за киберсигурността от страна на всички институции, органи и агенции на Съюза, както и за организацията и функционирането на CERT-EU и Междуинституционалния съвет по киберсигурност.

Член 3
Определения

За целите на настоящия регламент се прилагат следните определения:

1) „институции, органи и агенции на Съюза“ означава институциите, органите и агенциите на Съюза съгласно или въз основа на Договора за Европейския съюз, Договора за функционирането на Европейския съюз или Договора за създаване на Европейската общност за атомна енергия;

2) „мрежа и информационна система“ означава мрежа и информационна система по смисъла на член 4, параграф 1 от Директива [предложение за МИС 2];

3) „сигурност на мрежите и информационните системи“ означава сигурност на мрежите и информационните системи по смисъла на член 4, параграф 2 от Директива [предложение за МИС 2];

4) „киберсигурност“ означава киберсигурност по смисъла на член 4, параграф 3 от Директива [предложение за МИС 2];

5) „най-високо равнище на управление“ означава ръководител, ръководство или координационен и надзорен орган на най-високото административно равнище, като се вземат предвид структурите за управление на високо равнище във всяка институция, орган или агенция на Съюза;

6) „инцидент“ означава инцидент по смисъла на член 4, параграф 5 от Директива [предложение за МИС 2];

7) „значим инцидент“ означава всеки инцидент, освен ако е с ограничено въздействие и има вероятност вече да е добре изяснен от гледна точка на метода или технологията;

8) „голяма атака“ означава всеки инцидент, изискващ повече ресурси от наличните в засегнатата институция, орган или агенция на Съюза и в CERT-EU;

9) „действия при инцидент“ означава действията при инцидент по смисъла на член 4, параграф 6 от Директива [предложение за МИС 2];

10) „киберзаплаха“ означава киберзаплаха по смисъла на член 2, параграф 8 от Регламент (ЕС) 2019/881;

11) „значителна киберзаплаха“ означава киберзаплаха, при която са налице намерение, възможност и способност за причиняване на значим инцидент;

12) „уязвимост“ означава уязвимост по смисъла на член 4, параграф 8 от Директива [предложение за МИС 2];

13) „значителна уязвимост“ означава уязвимост, използването на която вероятно ще доведе до значим инцидент;

14) „риск за киберсигурността“ означава разумно установимо обстоятелство или събитие, което може да има неблагоприятно въздействие върху сигурността на мрежите и информационните системи;

15) „съвместно киберзвено“ означава виртуална и физическа платформа за сътрудничество между различните общности в областта на киберсигурността в Съюза, като се поставя акцент върху оперативната и техническата координация срещу големи трансгранични киберзаплахи и инциденти по смисъла на Препоръката на Комисията от 23 юни 2021 г.;

16) „базов набор от мерки за киберсигурност“ означава набор от минимални правила за киберсигурност, които трябва да се спазват от мрежите и информационните системи и техните оператори и ползватели, за да се сведат до минимум рисковете за киберсигурността.

Глава II
МЕРКИ ЗА ВИСОКО ОБЩО НИВО НА КИБЕРСИГУРНОСТ

Член 4

Управление, ръководство и контрол на рисковете

1. Всяка институция, орган и агенция на Съюза, като упражнява своята институционална автономност, създава своя собствена вътрешна рамка за управление, ръководство и контрол на рисковете за киберсигурността („рамката“) в подкрепа на мисията на субекта. Тази дейност се извършва под надзора на най-високото равнище на управление в субекта, за да се гарантира ефективно и разумно управление на всички рискове за киберсигурността. Рамката се въвежда най-късно до [….] [15 месеца след влизането в сила на настоящия регламент].

2. Рамката обхваща цялата ИТ среда на съответната институция, орган или агенция, включително всяка ИТ среда в техните помещения, активи и услуги в условията на компютърни услуги „в облак“, възложени на подизпълнители или хоствани от трети страни, мобилни устройства, корпоративни мрежи, бизнес мрежи, които не са свързани с интернет, и всякакви устройства, свързани с ИТ средата. В рамката се взема предвид управлението на кризи и непрекъснатостта на дейността и се отчита сигурността на веригата на доставки, както и управлението на рискове вследствие на човешки действия, които биха могли да окажат въздействие върху киберсигурността на съответната институция, орган или агенция на Съюза.

3. Висшето ръководство на всяка институция, орган и агенция на Съюза осигурява надзор върху спазването от страна на тяхната организация на задълженията, свързани с управлението, ръководството и контрола на рисковете за киберсигурността, без това да засяга официалните отговорности на други равнища на управление относно спазването на изискванията и управлението на риска в техните съответни области на отговорност.

4. Всяка институция, орган и агенция на Съюза разполага с ефективни механизми, за да гарантира, че подходящ процент от ИТ бюджета се изразходва за киберсигурност.

5. Всяка институция, орган и агенция на Съюза назначава местен служител по киберсигурността или служител на равностойна позиция, който действа като единно звено за контакт по отношение на всички аспекти на киберсигурността.

Член 5

Базов набор от мерки за киберсигурност

1. Най-високото равнище на управление на всяка институция, орган и агенция на Съюза одобрява собствения базов набор от мерки за киберсигурност на субекта, насочен към преодоляване на установените рискове в съответствие с рамката, посочена в член 4, параграф 1. Субектът извършва тази дейност в подкрепа на мисията си и като упражнява своята институционална

автономност. Базовият набор от мерки за киберсигурност се въвежда най-късно до [….] [18 месеца след влизането в сила на настоящия регламент] и обхваща областите, изброени в приложение I, и мерките, изброени в приложение II.

2. Висшето ръководство на всяка институция, орган и агенция на Съюза редовно преминава специфични обучения, за да придобие достатъчно знания и умения с цел разбиране и оценка на риска за киберсигурността и на управленските практики, свързани с киберсигурността, както и на тяхното въздействие върху дейността на организацията.

Член 6
Оценки на зрелостта

Всяка институция, орган и агенция на Съюза извършва оценка на зрелостта на киберсигурността най-малко веднъж на всеки три години, като включва всички елементи на своята ИТ среда, както е описано в член 4, при отчитане на съответните документи с насоки и препоръки, приети в съответствие с член 13.

Член 7
Планове за киберсигурност

1. Като следва заключенията от оценката на зрелостта и като отчита активите и установените рискове съгласно член 4, най-високото равнище на управление на всяка институция, орган и агенция на Съюза одобрява план за киберсигурност без ненужно забавяне след създаването на рамката за управление, ръководство и контрол на рисковете за киберсигурността и базовия набор от мерки за киберсигурност. Планът цели повишаване на цялостната киберсигурност на съответния субект, като по този начин допринася за постигането или подобряването на високо общо ниво на киберсигурност сред всички институции, органи и агенции на Съюза. За да подкрепя мисията на субекта въз основа на неговата институционална автономност, планът включва най-малко областите, изброени в приложение I, мерките, изброени в приложение II, и мерките, свързани с готовността за действие, реагирането и възстановяването при инциденти, като например мониторинг на сигурността и водене на регистри. Планът се преразглежда най-малко на всеки три години след оценките на зрелостта, които се извършват съгласно член 6.

2. В плана за киберсигурност се посочват ролите и отговорностите на членовете на персонала във връзка с неговото изпълнение.

3. В плана за киберсигурност се отчитат всички приложими документи с насоки и препоръки, отправени от CERT-EU.

Член 8
Прилагане

1. След приключване на оценките на зрелостта институциите, органите и агенциите на Съюза ги представят на Междуинституционалния съвет по киберсигурност. След изготвяне на плановете за сигурност институциите,

органите и агенциите на Съюза уведомяват Междуинституционалния съвет по киберсигурност за това. По искане на Междуинституционалния съвет те докладват за специфични аспекти от настоящата глава.

2. Документите с насоки и препоръките, отправени в съответствие с член 13, подпомагат изпълнението на разпоредбите, предвидени в настоящата глава.

Глава III
МЕЖДУИНСТИТУЦИОНАЛЕН СЪВЕТ ПО КИБЕРСИГУРНОСТ

Член 9
Междуинституционален съвет по киберсигурност

1. Създава се Междуинституционален съвет по киберсигурност (МСК).

2. МСК отговаря за:

   а) мониторинга на прилагането на настоящия регламент от институциите, органите и агенциите на Съюза;

   б) надзора по отношение на изпълнението на общите приоритети и цели от страна на CERT-EU и предоставянето на стратегически насоки на CERT-EU.

3. МСК се състои от трима представители, определени от Мрежата от агенции на Съюза (EUAN) по предложение на нейния Консултативен комитет за ИКТ, които да представляват интересите на агенциите и органите, управляващи своя собствена ИТ среда, както и от по един представител, определен от всеки от следните органи:

   а) Европейския парламент;

   б) Съвета на Европейския съюз;

   в) Европейската комисия;

   г) Съда на Европейския съюз;

   д) Европейската централна банка;

   е) Европейската сметна палата;

   ж) Европейската служба за външна дейност;

   з) Европейския икономически и социален комитет;

   и) Европейския комитет на регионите;

   й) Европейската инвестиционна банка;

к) Агенцията на Европейския съюз за киберсигурност.

Членовете може да се подпомагат от заместник. Председателят може да покани и други представители на изброените по-горе организации или на други институции, органи и агенции на Съюза да присъстват на заседанията на МСК без право на глас.

4. МСК приема своя вътрешен процедурен правилник.

5. В съответствие с вътрешния си процедурен правилник МСК определя председател измежду своите членове за срок от четири години. Неговият или нейният заместник става пълноправен член на МСК за същия срок.

6. МСК провежда заседания по инициатива на своя председател, по искане на CERT-EU или по искане на някой от неговите членове.

7. Всеки член на МСК разполага с един глас. Решенията на МСК се вземат с обикновено мнозинство, освен ако в настоящия регламент е предвидено друго. Председателят не гласува, освен в случай на равен брой гласове, при което може да участва в гласуването с решаващ глас.

8. МСК може да предприема действия чрез опростена писмена процедура, инициирана в съответствие с вътрешния процедурен правилник на МСК. Съгласно тази процедура съответното решение се счита за одобрено в определения от председателя срок, освен ако някой от членовете подаде възражение.

9. Ръководителят на CERT-EU или неговият или нейният заместник участва в заседанията на МСК, освен ако МСК реши друго.

10. Секретариатът на МСК се осигурява от Комисията.

11. Представителите, определени от EUAN по предложение на Консултативния комитет за ИКТ, предават решенията на МСК на агенциите и съвместните предприятия на Съюза. Всяка агенция и орган на Съюза има право да отправя до представителите или до председателя на МСК всякакви въпроси, които счита, че трябва да бъдат отнесени до МСК.

12. МСК може да предприема действия чрез опростена писмена процедура, инициирана от председателя, съгласно която съответното решение се счита за одобрено в определения от председателя срок, освен ако някой от членовете подаде възражение.

13. МСК може да определи изпълнителен комитет, който да го подпомага в неговата работа, и да му делегира някои от своите задачи и правомощия. МСК определя процедурния правилник на изпълнителния комитет, включително неговите задачи и правомощия, както и мандата на неговите членове.

Член 10
Задачи на МСК

При упражняване на своите отговорности МСК по-специално:

а) извършва преглед на всички поискани от CERT-EU доклади за напредъка по прилагането на настоящия регламент от страна на институциите, органите и агенциите на Съюза;

б) одобрява годишната работна програма на CERT-EU въз основа на предложение на ръководителя на CERT-EU и наблюдава нейното изпълнение;

в) одобрява каталог на услугите на CERT-EU въз основа на предложение на ръководителя на CERT-EU;

г) одобрява годишното финансово планиране на приходите и разходите за дейностите на CERT-EU, включително неговия персонал, въз основа на предложение, представено от ръководителя на CERT-EU;

д) одобрява условията за споразуменията за нивото на обслужване въз основа на предложение на ръководителя на CERT-EU;

е) разглежда и одобрява годишния доклад, изготвен от ръководителя на CERT-EU, който обхваща дейностите на CERT-EU и управлението на средствата от страна на CERT-EU;

ж) одобрява и наблюдава ключовите показатели за ефективност по отношение на CERT-EU, които са определени въз основа на предложение на ръководителя на CERT-EU;

з) одобрява договорености за сътрудничество, договорености за нивото на обслужване или договори между CERT-EU и други субекти съгласно член 17;

и) създава толкова технически консултативни групи, колкото е необходимо, за да подпомага работата на МСК, одобрява техния мандат и определя съответните им председатели.

Член 11
Спазване

МСК наблюдава прилагането на настоящия регламент и на приетите документи с насоки, препоръки и призиви за действие от страна на институциите, органите и агенциите на Съюза. Когато МСК установи, че институции, органи или агенции на Съюза не прилагат ефективно или не изпълняват настоящия регламент или документите с насоки, препоръките и призивите за действие, отправени съгласно настоящия регламент, той може, без да се засягат вътрешните процедури на съответната институция, орган или агенция на Съюза:

а) да отправи предупреждение; при необходимост, с оглед на неизбежен риск за киберсигурността, да ограничава аудиторията на предупреждението по подходящ начин;

б) да препоръча съответната служба за одит да извърши одит.

Глава IV
CERT-EU

Член 12
Мисия и задачи на CERT-EU

1. Мисията на CERT-EU, автономния междуинституционален център за киберсигурност за всички институции, органи и агенции на Съюза, е да допринася за сигурността на некласифицираната ИТ среда на всички институции, органи и агенции на Съюза посредством предоставяне на съвети в областта на киберсигурността, осигуряване на подкрепа за предотвратяването, откриването, смекчаването и реагирането на инциденти и осъществяване на дейност като техния координационен център за обмен на информация и реагиране при инциденти в областта на киберсигурността.

2. CERT-EU изпълнява следните задачи за институциите, органите и агенциите на Съюза:

   а) подпомага ги при прилагането на настоящия регламент и допринася за координацията във връзка с прилагането на настоящия регламент чрез мерките, изброени в член 13, параграф 1, или чрез доклади ad-hoc, поискани от МСК;

   б) подпомага ги с пакет от услуги за киберсигурност, описани в неговия каталог на услугите („базови услуги“);

   в) поддържа мрежа от партньори и колеги с цел подпомагане на услугите, посочени в членове 16 и 17;

   г) насочва вниманието на МСК към всеки въпрос, свързан с прилагането на настоящия регламент и с прилагането на документите с насоки, препоръките и призивите за действие;

   д) докладва относно киберзаплахите, пред които са изправени институциите, органите и агенциите на Съюза, и допринася за ситуационната осведоменост на ЕС по отношение на кибернетичното пространство.

3. CERT-EU допринася за съвместното киберзвено, създадено в съответствие с Препоръката на Комисията от 23 юни 2021 г., включително в следните области:

   а) готовност, координация при инциденти, обмен на информация и реакция на техническо равнище при кризи в случаи, свързани с институции, органи и агенции на Съюза;

   б) оперативно сътрудничество във връзка с мрежата на екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС), включително по

отношение на взаимопомощта, както и с по-широкообхватната общност в областта на киберсигурността;

в) разузнавателни данни за киберзаплахи, включително ситуационна осведоменост;

г) по всяка тема, за която се изисква експертният технически опит на CERT-EU в областта на киберсигурността.

4. CERT-EU участва в структурирано сътрудничество с Агенцията на Европейския съюз за киберсигурност с цел изграждане на капацитет, оперативно сътрудничество и дългосрочни стратегически анализи на киберзаплахите в съответствие с Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета.

5. CERT-EU може да предоставя следните услуги, които не са описани в неговия каталог на услугите („услуги, за които се събира такса“):

а) услуги за подпомагане на киберсигурността на ИТ средата на институции, органи и агенции на Съюза, различни от посочените в параграф 2, въз основа на споразумения за нивото на обслужване и в зависимост от наличните ресурси;

б) услуги за подпомагане на свързани с киберсигурността операции или проекти на институции, органи и агенции на Съюза, различни от насочените към защитата на тяхната ИТ среда, въз основа на писмени споразумения и с предварителното одобрение на МСК;

в) услуги за подпомагане на сигурността на ИТ средата на организации, различни от институциите, органите и агенциите на Съюза, които си сътрудничат тясно с институциите, органите и агенциите на Съюза, например чрез възлагане на задачи или отговорности съгласно правото на Съюза, въз основа на писмени споразумения и с предварителното одобрение на МСК.

6. CERT-EU може да организира учения в областта на киберсигурността или да препоръчва участие в съществуващи учения, по целесъобразност в тясно сътрудничество с Агенцията на Европейския съюз за киберсигурност, така че да се изпита нивото на киберсигурност на институциите, органите и агенциите на Съюза.

7. CERT-EU може да предоставя съдействие на институциите, органите и агенциите на Съюза във връзка с инциденти в класифицирани ИТ среди, ако съответният заинтересован субект изрично поиска това.

Член 13

Документи с насоки, препоръки и призиви за действие

1. CERT-EU подпомага прилагането на настоящия регламент, като отправя:

а) призиви за действие, в които се описват спешни мерки за сигурност, които институциите, органите и агенциите на Съюза настоятелно се призовават да предприемат в рамките на определен срок;

б) предложения до МСК за документи с насоки, насочени към всички институции, органи и агенции на Съюза или към част от тях;

в) предложения до МСК за препоръки, насочени към отделни институции, органи и агенции на Съюза.

2. Документите с насоки и препоръките може да включват:

а) реда и условията за или подобренията на управлението на риска за киберсигурността, както и базовия набор от мерки за киберсигурност;

б) реда и условията за оценките на зрелостта и плановете за киберсигурност; както и

в) когато е целесъобразно, използването на обща технология и архитектура и свързаните с тях най-добри практики с цел постигане на оперативна съвместимост и общи стандарти по смисъла на член 4, параграф 10 от Директива [предложение за МИС 2].

3. МСК може да приема документи с насоки или препоръки по предложение на CERT-EU.

4. МСК може да инструктира CERT-EU да отправи, оттегли или измени предложение за документ с насоки или за препоръка или призив за действие.

Член 14
Ръководител на CERT-EU

Ръководителят на CERT-EU редовно представя на МСК и на председателя на МСК доклади относно резултатите от дейността на CERT-EU, финансовото планиране, приходите, изпълнението на бюджета, сключените споразумения за нивото на обслужване и писмени споразумения, сътрудничеството с партньори и колеги и предприетите от персонала мисии, включително докладите, посочени в член 10, параграф 1.

Член 15
Финансови въпроси и въпроси, свързани с персонала

1. Комисията назначава ръководителя на CERT-EU, след като получи единодушното одобрение на МСК. Консултации с МСК се провеждат на всички етапи на процедурата преди назначаването на ръководителя на CERT-EU, и по-специално при изготвянето на обявленията за свободна длъжност, разглеждането на кандидатурите и назначаването на комисии за подбор във връзка с тази длъжност.

2. По отношение на прилагането на административните и финансовите процедури ръководителят на CERT-EU действа под ръководството на Комисията.

3. Задачите и дейностите на CERT-EU, включително услугите, предоставяни на институциите, органите и агенциите на Съюза съгласно член 12, параграфи 2, 3, 4 и 6 и член 13, параграф 1, които подлежат на финансиране от функцията на многогодишната финансова рамка, предназначена за европейската публична администрация, се финансират чрез отделен бюджетен ред от бюджета на Комисията. Определените за CERT-EU длъжности се описват подробно в бележка под линия към щатното разписание на Комисията.

4. Институциите, органите и агенциите на Съюза, различни от посочените в параграф 3, правят годишни финансови вноски за дейността на CERT-EU с цел покриване на услугите, предоставяни от CERT-EU съгласно параграф 3. Съответните вноски се правят въз основа на насоките, дадени от МСК и договорени между всеки субект и CERT-EU в споразуменията за нивото на обслужване. Вноските представляват справедлив и пропорционален дял от общите разходи за предоставените услуги. Те се получават по отделния бюджетен ред, посочен в параграф 3, като целеви приходи, както е предвидено в член 21, параграф 3, буква в) от Регламент (ЕС, Евратом) 2018/1046 на Европейския парламент и на Съвета[8].

5. Разходите за задачите, определени в член 12, параграф 5, се възстановяват от институциите, органите и агенциите на Съюза, които използват услугите на CERT-EU. Приходите се разпределят по бюджетните редове в подкрепа на разходите.

Член 16

Сътрудничество между CERT-EU и партньори от държавите членки

1. CERT-EU си сътрудничи и обменя информация с националните си партньори в държавите членки, включително с екипите за незабавно реагиране при компютърни инциденти, националните центрове за киберсигурност, ЕРИКС и единните звена за контакт, посочени в член 8 от Директива [предложение за МИС 2], по отношение на киберзаплахи, уязвимости и инциденти, по евентуални мерки за противодействие и по всички въпроси от значение за подобряването на защитата на ИТ средите на институциите, органите и агенциите на Съюза, включително чрез мрежата на ЕРИКС, посочена в член 13 на Директива [предложение за МИС 2].

2. CERT-EU може да обменя информация за конкретни инциденти с националните партньори в държавите членки, за да се улесни откриването на подобни киберзаплахи или инциденти, без да е необходимо съгласието на засегнатия заинтересован субект. CERT-EU може да обменя информация за

[8] 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).

конкретен инцидент, от която става ясна мишената на киберинцидента, само със съгласието на засегнатия заинтересован субект.

Член 17

Сътрудничество между CERT-EU и партньори от държави извън ЕС

1. CERT-EU може да си сътрудничи с партньори от държави извън ЕС, включително с партньори от специфични промишлени отрасли, във връзка с инструменти и методи, например техники, тактики, процедури и най-добри практики, както и във връзка с киберзаплахи и уязвимости. За всяко сътрудничество с такива партньори, включително в рамки, в които партньори от държави извън ЕС си сътрудничат с националните партньори на държавите членки, CERT-EU иска предварително одобрение от МСК.

2. CERT-EU може да си сътрудничи с други партньори, като например търговски субекти, международни организации, национални субекти от държави извън Европейския съюз или отделни експерти, с цел събиране на информация относно общи и специфични киберзаплахи, уязвимости и възможни мерки за противодействие. За по-широкообхватно сътрудничество с такива партньори CERT-EU иска предварително одобрение от МСК.

3. CERT-EU може, със съгласието на заинтересования субект, който е засегнат от инцидент, да предоставя информация във връзка с инцидента на партньори, които могат да допринесат за неговия анализ.

Глава V
ЗАДЪЛЖЕНИЯ ЗА СЪТРУДНИЧЕСТВО И ДОКЛАДВАНЕ

Член 18

Обработка на информация

1. CERT-EU и институциите, органите и агенциите на Съюза спазват задължението за професионална тайна в съответствие с член 339 от Договора за функционирането на Европейския съюз или равностойни приложими уредби.

2. Разпоредбите на Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета[9] се прилагат по отношение на искания за публичен достъп до документи, съхранявани от CERT-EU, включително предвиденото в този регламент задължение за консултиране с други институции, органи и агенции на Съюза, когато дадено искане се отнася до техни документи.

3. По отношение на обработването на лични данни, извършвано съгласно настоящия регламент, се прилага Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета.

[9] Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета от 30 май 2001 г. относно публичния достъп до документи на Европейския парламент, на Съвета и на Комисията (ОВ L 145, 31.5.2001 г., стр. 43).

4. При обработката на информация от страна на CERT-EU и от институциите, органите и агенциите на Съюза се спазват правилата, определени в [предложения регламент относно информационната сигурност].

5. Всички контакти със CERT-EU, инициирани или поискани от националните служби за сигурност и разузнаване, се съобщават без ненужно забавяне на дирекцията по сигурността на Комисията и на председателя на МСК.

Член 19
Задължения за споделяне

1. За да може CERT-EU да координира управлението на уязвимостите и реакцията при инциденти, той може да поиска от институциите, органите и агенциите на Съюза да му предоставят информация от регистрите на техните ИТ системи, която е от значение за осъществяваната от CERT-EU подкрепа. Институцията, органът или агенцията, към която е отправено искането, предава исканата информация и всички последващи актуализации по нея без ненужно забавяне.

2. Институциите, органите и агенциите на Съюза предоставят на CERT-EU, при искане от негова страна и без ненужно забавяне, цифрова информация, създадена чрез използването на електронните устройства, засегнати от съответните инциденти. CERT-EU може да поясни допълнително какъв вид цифрова информация му е необходима за постигане на ситуационна осведоменост и за реагиране при инциденти.

3. CERT-EU може да обменя информация за конкретен инцидент, която разкрива кои са институциите, органите или агенциите на Съюза, засегнати от инцидента, само със съгласието на съответните субекти. CERT-EU може да обменя информация за конкретен инцидент, която разкрива субекта, станал цел на киберинцидента, само със съгласието на засегнатия от инцидента субект.

4. Задълженията за споделяне не обхващат класифицирана информация на ЕС (КИЕС) и информация, която институция, орган или агенция на Съюза е получила от служба за сигурност или разузнаване или от правоприлагаща агенция на държава членка с изричното условие да не се споделя със CERT-EU.

Член 20
Задължения за уведомяване

1. Всички институции, органи и агенции на Съюза отправят първоначално уведомление до CERT-EU за значителни киберзаплахи, значителни уязвимости и значими инциденти без ненужно забавяне и във всеки случай не по-късно от 24 часа, след като са узнали за тях.

В надлежно обосновани случаи и със съгласието на CERT-EU съответната институция, орган или агенция на Съюза може да се отклони от крайния срок, определен в предходния параграф.

2. Освен това институциите, органите и агенциите на Съюза съобщават на CERT-EU без ненужно забавяне подходящи технически подробности за киберзаплахите, уязвимостите и инцидентите, които дават възможност за откриване и реагиране на инциденти или за предприемане на смекчаващи мерки. Уведомлението включва следната информация, ако е налична:

   а) съответните показатели за компрометиране на информация;

   б) съответните механизми за откриване;

   в) потенциалното въздействие;

   г) съответните смекчаващи мерки.

3. CERT-EU представя ежемесечно на ENISA обобщен доклад, включващ анонимизирани и обобщени данни относно значителните киберзаплахи, значителните уязвимости и значимите инциденти, за които е уведомен в съответствие с параграф 1.

4. МСК може да издава документи с насоки или препоръки относно реда и условията за изготвянето на уведомлението и относно неговото съдържание. CERT-EU разпространява подходящите технически подробности, които дават възможност за проактивно откриване и реагиране на инциденти или за предприемане на смекчаващи мерки от страна на институциите, органите и агенциите на Съюза.

5. Задълженията за уведомяване не обхващат КИЕС и информация, която институция, орган или агенция на Съюза е получила от служба за сигурност или разузнаване или от правоприлагаща агенция на държава членка с изричното условие да не се споделя със CERT-EU.

Член 21

Координация и сътрудничество при реагиране на инциденти в случай на значими инциденти

1. При осъществяване на дейност като координационен център за обмен на информация и реагиране при инциденти в областта на киберсигурността CERT-EU улеснява обмена на информация по отношение на киберзаплахи, уязвимости и инциденти между:

   а) институциите, органите и агенциите на Съюза;

   б) партньорите, посочени в членове 16 и 17.

2. CERT-EU улеснява координацията между институциите, органите и агенциите на Съюза във връзка с реагирането при инциденти, което включва:

   а) принос за съгласувани външни комуникации;

   б) взаимопомощ;

   в) оптимално използване на оперативните ресурси;

г) координация с други механизми за реакция при кризи на равнището на Съюза.

3. CERT-EU подпомага институциите, органите и агенциите на Съюза по отношение на ситуационната осведоменост във връзка с киберзаплахи, уязвимости и инциденти.

4. МСК отправя насоки относно координацията и сътрудничеството при реагиране на инциденти в случай на значими инциденти. Когато се подозира, че даден инцидент е с престъпен характер, CERT-EU предоставя съвети как да се съобщи за инцидента на правоприлагащите органи.

Член 22
Големи атаки

1. CERT-EU координира реакциите на институциите, органите и агенциите на Съюза в случай на големи атаки. Той поддържа опис на техническия експертен опит, който би бил необходим при реагиране на инциденти в случай на такива атаки.

2. Институциите, органите и агенциите на Съюза допринасят за описа на техническия експертен опит, като предоставят ежегодно актуализиран списък на наличните в техните организации експерти с подробно описание на техните специфични технически умения.

3. С одобрението на съответните институции, органи и агенции на Съюза CERT-EU може да се обърне и към експертите от списъка, посочен в параграф 2, за да допринесат за реакцията в случай на голяма атака в държава членка, в съответствие с оперативните процедури на съвместното киберзвено.

Глава VI
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 23
Първоначално преразпределяне на бюджета

Комисията предлага преразпределяне на персонал и финансови ресурси от съответните институции, органи и агенции на Съюза към бюджета на Комисията. Преразпределянето се извършва едновременно с първия бюджет, който се приема след влизането в сила на настоящия регламент.

Член 24
Преглед

1. МСК, със съдействието на CERT-EU, периодично докладва на Комисията за прилагането на настоящия регламент. МСК може също да отправя препоръки към Комисията във връзка с предлагането на изменения на настоящия регламент.

2. Комисията представя доклад за прилагането на настоящия регламент на Европейския парламент и на Съвета най-късно 48 месеца след влизането в сила на настоящия регламент, след което докладва на всеки три години.

3. Комисията извършва оценка на функционирането на настоящия регламент и докладва на Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите не по-рано от пет години след датата на влизане в сила.

Член 25
Влизане в сила

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

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

Съставено в Брюксел на […] година.

За Европейския парламент	*За Съвета*
Председател	*Председател*

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1. Наименование на предложението/инициативата

1.2. Съответни области на политиката

1.3. Предложението/инициативата е във връзка с:

1.4. Цели

1.4.1. Общи цели

1.4.2. Конкретни цели

1.4.3. Очаквани резултати и отражение

1.4.4. Показатели за изпълнението

1.5. Мотиви за предложението/инициативата

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

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

1.5.3. Изводи от подобен опит в миналото

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

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

1.6. Продължителност и финансово отражение на предложението/инициативата

1.7. Планирани методи на управление

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

2.2. Системи за управление и контрол

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

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

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

2.3. Мерки за предотвратяване на измами и нередности

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

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

3.2. Очаквано финансово отражение на предложението върху бюджетните кредити

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

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

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

3.2.4. Съвместимост с настоящата многогодишна финансова рамка

3.2.5. Финансов принос от трети страни

3.3. Очаквано отражение върху приходите

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1. Наименование на предложението/инициативата

Предложение за Регламент на Европейския парламент и на Съвета за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза

1.2. Съответни области на политиката

Европейска публична администрация

Предложението се отнася до мерки, с които се гарантира високо общо ниво на киберсигурност в рамките на институциите, органите и агенциите на Съюза

1.3. Предложението/инициативата е във връзка с:

☑**ново действие**

☐ **ново действие след пилотен проект/подготвително действие**[10]

☐ **продължаване на съществуващо действие**

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

1.4. Цели

1.4.1. Общи цели

– Създаване на рамка, с която се гарантира високо общо ниво на киберсигурност в рамките на институциите, органите и агенциите на Съюза

– Осигуряване на ново правно основание за CERT-EU с цел укрепване на неговия мандат и финансиране

1.4.2. Конкретни цели

1) Определяне на задължения за институциите, органите и агенциите на Съюза да създадат вътрешна рамка за управление, ръководство и контрол на рисковете за киберсигурността

2) Определяне на задължения за институциите, органите и агенциите на Съюза да докладват за своята вътрешна рамка за управление, ръководство и контрол на рисковете за киберсигурността, както и за киберинциденти

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

3) Определяне на правила за организацията и функционирането на Центъра за киберсигурност за институциите, органите и агенциите на Съюза (CERT-EU) и за организацията и функционирането на Междуинституционалния съвет по киберсигурност (МСК)

4) Принос към съвместното киберзвено

1.4.3. Очаквани резултати и отражение

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

– Вътрешни рамки за управление, ръководство и контрол на рисковете за киберсигурността, базов набор от мерки за киберсигурност, редовни оценки на зрелостта и планове за киберсигурност в институциите, органите и агенциите на Съюза – Подобряване на устойчивостта в областта на киберсигурността и на капацитета за реагиране при инциденти в институциите, органите и агенциите на Съюза – Модернизиране на CERT-EU – Принос към съвместното киберзвено

1.4.4. Показатели за изпълнението

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

– Въвеждане на рамки и базови набори от мерки, извършване на редовни оценки на зрелостта и изпълнение на планове за киберсигурност в институциите, органите и агенциите на Съюза – Подобрени действия при инциденти – Повишена осведоменост на висшето ръководно равнище на институциите, органите и агенциите на Съюза относно рисковете за киберсигурността – Изравняване на разходите за сигурността на ИКТ като процент от общите разходи за ИКТ – Силно лидерство на МСК и CERT-EU – Засилено споделяне на информация между институциите, органите и агенциите на Съюза и със съответните органи и заинтересовани страни в ЕС – Засилено сътрудничество в областта на киберсигурността със съответните органи и заинтересовани страни в ЕС чрез CERT-EU и ENISA

1.5. Мотиви за предложението/инициативата

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

Предложението има за цел да повиши нивото на кибернетичната устойчивост на институциите, органите и агенциите на Съюза, да намали несъответствията в устойчивостта сред тези субекти и да подобри нивото на съвместната ситуационна осведоменост и колективната способност за подготовка и реагиране.

Предложението е напълно последователно и съгласувано с други свързани инициативи, и по-специално с предложението за Директива относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148 [предложение за МИС 2].

Предложението е съществена част от стратегията на ЕС за Съюза на сигурност и от стратегията на ЕС за киберсигурност за цифровото десетилетие.

Предвижда се Регламентът да бъде предложен от Европейската комисия през октомври 2021 г., като се очаква Европейският парламент и Съветът да го приемат през 2022 г., а разпоредбите ще започнат да се прилагат от датата на влизане в сила на Регламента. Предвижда се финансовото въздействие и въздействието върху човешките ресурси, очертани в настоящата законодателна финансова обосновка, да започнат да пораждат ефект през 2023 г. През 2021 г. вече започна подготвителен период, но подготвителните дейности през 2021 г. и 2022 г. попадат извън обхвата на финансовото въздействие на предложението.

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

Основания за действие на европейско равнище (ex-ante)

Между 2019 г. и 2021 г. броят на значимите инциденти, засягащи институциите, органите и агенциите на Съюза, предизвикани от автори на т.нар. „съвременни упорити заплахи“, нарасна драстично. През първата половина на 2021 г. броят на значимите инциденти съответстваше на инцидентите през цялата 2020 г. Това проличава и от броя на цифровите копия за криминалистична експертиза (копия на съдържанието на засегнатите системи или устройства към даден момент), анализирани от CERT-EU през 2020 г., който се утрои в сравнение с 2019 г., като броят на значимите инциденти се увеличи повече от десет пъти от 2018 г. насам.

Равнищата на зрялост на киберсигурността на отделните субекти се различават значително[11]. С настоящия регламент се гарантира, че всички институции, органи и агенции на Съюза ще прилагат базов набор от мерки за сигурност и ще си сътрудничат взаимно с цел откритото и ефикасно функциониране на администрацията на Съюза.

Системите, които трябва да бъдат защитени, попадат в обхвата на автономността на институциите, органите и агенциите на Съюза и се управляват от тях, поради което предложените действия не биха могли да бъдат извършени от държавите членки.

1.5.3. Изводи от подобен опит в миналото

Директивата за МИС е първият хоризонтален инструмент на вътрешния пазар, насочен към подобряването на устойчивостта на мрежите и системите в Съюза срещу рискове за киберсигурността. От влизането си в сила през 2016 г. тя допринесе значително за повишаването на общото равнище на киберсигурност сред държавите членки. Предложението за Директива за МИС 2 има за цел да подобри допълнително тези мерки.

Регламентът цели да осигури подобни мерки за институциите, органите и агенциите на Съюза.

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

Предложението е в съответствие с многогодишната финансова рамка и е съществена част от стратегията на ЕС за Съюза на сигурност и от стратегията на ЕС за киберсигурност за цифровото десетилетие.

В предложението се предвижда прилагането на мерки за високо общо ниво на киберсигурност по отношение на институциите, органите и агенциите на Съюза. Предложението е в съответствие с предложението за Директива относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148 [предложение за МИС 2].

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

Управлението на задачите от страна на CERT-EU изисква специфични профили и допълнително работно натоварване, което не може да бъде поето без увеличаване на човешките и финансовите ресурси.

[11] Препратка: [Специален доклад на ЕСП относно киберсигурността в институциите, органите и агенциите на Съюза].

1.6. Продължителност и финансово отражение на предложението/инициативата

☐ **ограничен срок на действие**

– ☐ в сила от [ДД/ММ]ГГГГ до [ДД/ММ]ГГГГ

– ☐ Финансово отражение от ГГГГ до ГГГГ за бюджетни кредити за поети задължения и от ГГГГ до ГГГГ за бюджетни кредити за плащания.

☑ **неограничен срок на действие**

– Финансовото отражение следва да започне с първия бюджет, който се приема след влизането в сила на Регламента. През първата година, която се счита за преходна година, ще се извърши преразпределяне на ресурси от институциите и основните органи на Съюза към Комисията; това и друго (пре)разпределяне на ресурсите ще бъдат извършени в рамките на годишните бюджети. Ако регламентът бъде приет през 2022 г., финансовата 2023 година ще бъде преходният период, а през 2024 г. ще е налице функциониране с пълен капацитет.

1.7. Планирани методи на управление[12]

☑ **Пряко управление** от Комисията и от всяка институция, орган и агенция на Съюза

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

– ☐ от изпълнителните агенции

☐ **Споделено управление** с държавите членки

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

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

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

– ☐ ЕИБ и Европейския инвестиционен фонд;

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

– ☐ публичноправни органи;

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

[12] Подробности във връзка с методите на управление и позоваванията на Финансовия регламент могат да бъдат намерени на уебсайта BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

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

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

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

Забележки

За прилагането на административните и финансовите процедури CERT-EU действа под ръководството на Комисията. Допълнителни ресурси, произтичащи от проекта за Регламент: Прилагането на член 12 и 13 от проекта за Регламент води до разширен каталог на услугите с допълнителни базови услуги. При функциониране с пълен капацитет ще бъдат необходими следните допълнителни ресурси (до приключването на МФР в края на 2027 г.): 21 ЕПРВ и 14,05 милиона EUR. Разпределението на допълнителните средства по бюджета за различните задачи е, както следва:

а) за изпълнението на задачите за институциите, органите и агенциите на Съюза, описани подробно в член 12, параграф 2, букви а), б), в) и д): 13,75 ЕПРВ и 11,275 милиона EUR;

б) за изпълнението на задачите, описани подробно в член 12, параграф 3 (принос към съвместното киберзвено): 2 ЕПРВ и 381 000 EUR;

в) за изпълнението на задачите, описани подробно в член 12, параграф 4 (структурирано сътрудничество с ENISA): 0,25 ЕПРВ и 236 000 EUR;

г) за изпълнението на задачите, описани подробно в член 12, параграф 6 (учения в областта на киберсигурността): 0,25 ЕПРВ и 79 000 EUR;

д) за изпълнението на задачите, описани подробно в член 12, параграф 2, буква г) и член 13 (анализ и докладване относно прилагането на Регламента, изготвяне на документи с насоки, препоръки и призиви за действие): 3,75 ЕПРВ и 2,079 милиона EUR;

е) за изпълнението на задачите за подпомагане на секретариата на Междуинституционалния съвет за киберсигурност (МСК): 1 ЕПРВ.

Преглед на настоящите ресурси и преход към функциониране с пълен капацитет: През септември 2021 г. CERT-EU е работил със следните ресурси: - постоянни и командировани длъжности: 14 ЕПРВ;

- договорно наети служители, финансирани по споразумения за нивото на обслужване: 24 ЕПРВ;

- общо 38 ЕПРВ.

Бюджетът на CERT-EU през 2020 г. е бил: 250 000 EUR от бюджета на Комисията, 3,5 милиона евро чрез целеви приходи от споразумения за нивото на обслужване. Общо: 3,75 милиона евро. Това представлява целият бюджет на CERT-EU, който обхваща обучение, хардуер, софтуер, мисии, подкрепа, договорно наети служители и конференции.

След влизането в сила на Регламента се предвижда бъдещите ресурси на CERT-EU да бъдат:

- постоянни длъжности: 34 ЕПРВ,

- договорно наети служители: 15 ЕПРВ,

- общо 49 ЕПРВ, т.е. нетно увеличение с 11 ЕПРВ.

Промяната в съотношението между постоянните длъжности и договорно наетите служители е свързана със съответния проблем да се наемат и задържат старши специалисти в областта на киберсигурността поради недостига им на пазара на труда.

Освен това в рамките на генерална дирекция „Информатика“ на Комисията ще бъде необходим 1 договорно нает служител в ЕПРВ, който да подпомага МСК (Междуинституционалния съвет по киберсигурност).

Следователно за прилагането на Регламента ще са необходими общо 21 допълнителни ЕПРВ (20 ЕПРВ за CERT-EU и 1 ЕПРВ за генерална дирекция „Информатика“ на Комисията). Това ще бъде компенсирано с паралелно намаляване с 9 договорно наети служители в ЕПРВ в CERT-EU, които преди това са били финансирани чрез целеви приходи от споразумения за нивото на обслужване.

След преходния период бюджетът на CERT-EU през 2024 г. за ресурси, различни от човешки, ще покрива задачите, изброени по-горе в букви а)—д), и се предвижда да бъде финансиран, както следва:

- 8,921 милиона евро годишно от институциите на Съюза, финансирани по функция 7 от бюджета на Съюза;

- 2,459 милиона евро от институции, органи и агенции на Съюза, финансирани по функции 1—6 от бюджета на Съюза;

- 2,670 милиона евро от самофинансиращи се институции, органи и агенции на Съюза;

- общ бюджет на CERT-EU: 14,05 милиона евро.

Задачите, изброени в член 12, параграф 5, не са описани в неговия каталог на услугите, като това са услуги, за които се събира такса. Те са спомагателни услуги, които се характеризират с относително ниски суми, като цяло са временни и разходите за тях ще

бъдат възстановени от бенефициерите на услугите чрез споразумения за нивото на обслужване или писмени споразумения.

По отношение на приноса за персонала на CERT-EU: институциите и основните органи на Съюза допринасят със справедлив дял, пропорционален на съответния дял на постоянните длъжности AD в организацията. Следва да се уточни дали ЕЦБ и ЕИБ също могат да допринасят със справедлив дял чрез командироване на постоянен персонал.

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

Да се посочат честотата и условията.

С помощта на МСК и CERT-EU Комисията периодично ще извършва преглед на функционирането на Регламента и ще докладва на Европейския парламент и на Съвета за първи път не по-късно от 48 месеца след влизането в сила на настоящия регламент и на всеки три години след това.

Източниците на данни, използвани за прегледите, ще са предимно от МСК и CERT-EU. Освен това при необходимост биха могли да се използват специфични инструменти за събиране на данни, например проучвания на институциите, органите и агенциите на Съюза, ENISA или мрежата на ЕРИКС.

2.2. Системи за управление и контрол

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

Действията, произтичащи от Регламента, ще се управляват в рамките на всяка институция, орган и агенция на Съюза в съответствие с техните приложими правила и разпоредби.

Административното и финансовото управление на дейностите на CERT-EU е интегрирано в администрацията на Комисията и следва нейните приложими механизми за управление и изпълнение, условия за плащане и проверки.

Вътрешният одитор на Комисията се ползва със същите правомощия спрямо CERT-EU като тези спрямо отделите на Комисията.

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

Много нисък риск, тъй като CERT-EU вече е прикрепен административно като работна група на Комисията към генералния директор на ГД „Информатика“, а МСК е моделиран въз основа на действащия управителен съвет на CERT-EU. Следователно екосистемата за финансово управление и вътрешен контрол вече е налице.

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

Процедурите за възлагане на обществени поръчки, финансово управление и контрол вече са налице и са добре изпитани. Разходната ефективност на проверките и равнищата на риска от грешки съответстват на тези във всяка

институция, орган или агенция на Съюза, както и на тези на Комисията за дейностите на CERT-EU.

2.3. Мерки за предотвратяване на измами и нередности

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

Системите за финансово управление и вътрешен контрол на Комисията се прилагат по отношение на дейностите на CERT-EU.

С цел борба с измамите, корупцията и други незаконни действия разпоредбите на Регламент (ЕС, Евратом) № 883/2013 на Европейския парламент и на Съвета от 11 септември 2013 г. относно разследванията, провеждани от Европейската служба за борба с измамите (OLAF), се прилагат без ограничение.

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

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

- Съществуващи бюджетни редове

<u>По реда</u> на функциите от многогодишната финансова рамка и на бюджетните редове.

Функция от многогодишната финансова рамка	Бюджетен ред	Вид разход	Финансов принос			
	Номер	Многогод./ едногод.[13]	от държави от ЕАСТ[14]	от държави кандидатки[15]	от трети държави	по смисъла на член 21, параграф 2, буква б) от Финансовия регламент
1—6	Бюджетни редове, включващи вноските на Съюза за децентрализирани агенции и органи	Многогод.	НЕ	НЕ	НЕ	НЕ
7	Бюджетни редове, включващи възнагражденията на персонала, разходите за ИТ и други административни разходи в различните раздели на бюджета на ЕС	Едногод.	НЕ	НЕ	НЕ	НЕ

- Поискани нови бюджетни редове

<u>По реда</u> на функциите от многогодишната финансова рамка и на бюджетните редове.

Функция от многогодишната финансова рамка	Бюджетен ред	Вид разход	Финансов принос			
	Номер	Многогод./ едногод.	от държави от ЕАСТ	от държави кандидатки	от трети държави	по смисъла на член 21, параграф 2, буква б) от Финансовия регламент
	Няма		ДА/НЕ	ДА/НЕ	ДА/НЕ	ДА/НЕ

[13] Многогод. = Многогодишни бюджетни кредити / едногод. = едногодишни бюджетни кредити.
[14] ЕАСТ: Европейска асоциация за свободна търговия.
[15] Държави кандидатки и, ако е приложимо, потенциални кандидатки от Западните Балкани.

3.2. Очаквано финансово отражение на предложението върху бюджетните кредити

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

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

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

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

Функция от многогодишната финансова рамка	1—6	Функции, включващи вноските за децентрализирани агенции и органи

ГД: няколко			Година **2023**	Година **2024**	Година **2025**	Година **2026**	Година **2027**	**ОБЩО**
○ Бюджетни кредити за оперативни разходи								
Бюджетни редове, покриващи вноските на Съюза за децентрализирани агенции (xx 10 xx xx)[16]	Поети задължения	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Плащания	(2a)	2,459	2,459	2,459	2,459	2,459	12,293
Бюджетни кредити за административни разходи, финансирани от пакета за определени програми[17]								
Бюджетен ред		(3)						
ОБЩО бюджетни кредити	Поети задължения	=1a+1б +3	2,459	2,459	2,459	2,459	2,459	12,293

16 Съгласно официалната бюджетна номенклатура.

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

За ГД: няколко	Плащания	=2а+2б +3	2,459	2,459	2,459	2,459	2,459	12,293

○ ОБЩО бюджетни кредити за оперативни разходи	Поети задължения	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Плащания	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ ОБЩО бюджетни кредити за административни разходи, финансирани от пакета за определени програми		(6)						
ОБЩО бюджетни кредити за ФУНКЦИИ 1—6 от многогодишната финансова рамка	Поети задължения	=4+ 6	2,459	2,459	2,459	2,459	2,459	12,293
	Плащания	=5+ 6	2,459	2,459	2,459	2,459	2,459	12,293

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

○ ОБЩО бюджетни кредити за оперативни разходи (всички оперативни функции)	Поети задължения	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Плащания	(5)	2,459	2,459	2,459	2,459	2,459	12,293
ОБЩО бюджетни кредити за административни разходи, финансирани от пакета за определени програми (всички оперативни функции)		(6)						
ОБЩО бюджетни кредити за ФУНКЦИИ 1—6 от многогодишната финансова рамка (Референтна стойност)	Поети задължения	=4+ 6	2,459	2,459	2,459	2,459	2,459	12,293
	Плащания	=5+ 6	2,459	2,459	2,459	2,459	2,459	12,293

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

Тази част следва да бъде попълнена, като се използва таблицата за бюджетни данни от административно естество, която най-напред се въвежда в приложението към законодателната финансова обосновка (приложение V към вътрешните правила), което се качва в DECIDE за провеждането на вътрешни консултации между службите.

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

		Година **2023**	Година **2024**	Година **2025**	Година **2026**	**Година 2027**	**ОБЩО**
ГД: „Информатика“ (CERT-EU)							
○ Човешки ресурси		1,184	2,126	2,754	3,225	3,225	12,514
○ Други административни разходи		7,938	8,921	8,921	8,921	8,921	43,622
ОБЩО ГД „Информатика“ (CERT-EU)	Бюджетни кредити	9,122	11,047	11,675	12,146	12,146	56,136

ОБЩО бюджетни кредити за ФУНКЦИЯ 7 от многогодишната финансова рамка	(Общо поети задължения = общо плащания)	9,122	11,047	11,675	12,146	12,146	**56,136**

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

		Година 2023	Година 2024	Година 2025	Година 2026	Година 2027	**ОБЩО**
ОБЩО бюджетни кредити за ФУНКЦИИ 1—7 от многогодишната финансова рамка	Поети задължения	11,581	13,506	14,134	14,605	14,605	68,429
	Плащания	11,581	13,506	14,134	14,605	14,605	68,429

(*)							

(*) Вноските от самофинансиращите се институции, органи и агенции на Съюза се изчисляват на 2,670 милиона евро годишно (общо 13,350 милиона евро за петте години). Вноските ще представляват целеви приходи за CERT-EU. Таблиците по-горе обхващат само очакваното общо отражение върху бюджета на Съюза и не включват тези вноски.

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

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

Да се посочат целите и резултатите			Година **N**		Година **N+1**		Година **N+2**		Година **N+3**		Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)						**ОБЩО**	
	РЕЗУЛТАТИ																	
⇩	Вид[18]	Среден разход	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Общ бр.	Общо разходи
КОНКРЕТНА ЦЕЛ № 1[19]...																		
- Резултат																		
- Резултат																		
- Резултат																		
Междинен сбор за конкретна цел № 1																		
КОНКРЕТНА ЦЕЛ № 2...																		
- Резултат																		

[18] Резултатите са продуктите и услугите, които ще бъдат доставени (напр. брой финансирани обмени на учащи се, дължина на построените пътища в километри и др.).

[19] Описана в точка 1.4.2. „Конкретни цели…“.

Междинен сбор за конкретна цел № 2																
ОБЩО																

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

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

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

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

	Година 2023	Година 2024	Година 2025	Година 2026	Година 2027	**ОБЩО**
ФУНКЦИЯ 7 от многогодишната финансова рамка						
Човешки ресурси						
Постоянен персонал (степени AD)	1,099	2,041	2,669	3,14	3,14	12,089
Договорно нает персонал	0,085	0,085	0,085	0,085	0,085	0,425
Други административни разходи	7,938	8,921	8,921	8,921	8,921	43,622
Междинен сбор за ФУНКЦИЯ 7 от многогодишната финансова рамка	9,122	11,047	11,675	12,146	12,146	56,136

Извън ФУНКЦИЯ 7[20] of the multiannual financial framework						
Човешки ресурси						
Други административни разходи						
Междинен сбор извън ФУНКЦИЯ 7 от многогодишната финансова рамка						

ОБЩО	9,122	11,047	11,675	12,146	12,146	56,136

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

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

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

3.2.3.1. Очаквани нужди от човешки ресурси

– ☐ Предложението/инициативата не налага използване на човешки ресурси

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

Оценката се посочва в еквиваленти на пълно работно време

	Година 2023	Година 2024	Година 2025	Година 2026	Година 2027
○ Длъжности в щатното разписание (длъжностни лица и срочно наети служители)					
20 01 02 01 (Централа и представителства на Комисията)	7	13	17	20	20
20 01 02 03 (Делегации)					
01 01 01 01 (Непреки научни изследвания)					
01 01 01 11 (Преки научни изследвания)					
Други бюджетни редове (да се посочат)					
○ Външен персонал (в еквивалент на пълно работно време: ЕПРВ)[21]					
20 02 01 (ДНП, КНЕ, ПНА от общия финансов пакет)	1	1	1	1	1
20 02 03 (ДНП, МП, КНЕ, ПНА и МЕД в делегациите)					
XX 01 xx **yy zz** [22] - в централата					
XX 01 xx **yy zz** [22] - в делегациите					
01 01 01 02 (ДНП, КНЕ, ПНА — Непреки научни изследвания)					
01 01 01 12 (ДНП, КНЕ, ПНА — Преки научни изследвания)					
Други бюджетни редове (да се посочат)					
ОБЩО	**8**	**14**	**18**	**21**	**21**

XX е съответната област на политиката или съответният бюджетен дял.

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

Описание на задачите, които трябва да се изпълнят:

Длъжностни лица и срочно наети служители	Длъжностните лица ще изпълняват задачите и дейностите на CERT-EU съгласно Регламента, и по-специално глави IV и V.
Външен персонал	Договорно наетият служител ще подпомага работата на Междуинституционалния съвет по киберсигурност като секретариат.

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

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

3.2.4. Съвместимост с настоящата многогодишна финансова рамка

Предложението/инициативата:

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

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

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

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

– ☐ налага преразглеждане на МФР.

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

3.2.5. Финансов принос от трети страни

Предложението/инициативата:

– ☑ не предвижда съфинансиране от трети страни[23]

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

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

	Година **N**[24]	Година **N+1**	Година **N+2**	Година **N+3**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)			Общо
Да се посочи съфинансиращият орган								
ОБЩО съфинансирани бюджетни кредити								

[23] Не е извършено изчисляване на целевите приходи, произтичащи от спорадичното предоставяне на предвидените в член 12, параграф 5, буква в) услуги на организации, различни от заинтересованите субекти, тъй като тези приходи следва да бъдат незначителни.

[24] Година N е годината, през която започва да се осъществява предложението/инициативата. Буквата N да се замени с очакваната първа година от изпълнението (например 2021 г.). Същото за следващите години.

3.3. Очаквано отражение върху приходите

– ☑ Предложението/инициативата няма финансово отражение върху приходите.

– ☐ Предложението/инициативата има следното финансово отражение:

  – ☐ върху собствените ресурси

  – ☐ върху разните приходи

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

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

Приходен бюджетен ред:	Налични бюджетни кредити за текущата бюджетна година	Отражение на предложението/инициативата[25]						
		Година **N**	Година **N+1**	Година **N+2**	Година **N+3**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)		
Член …….								

За целевите приходи да се посочат съответните разходни бюджетни редове.

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

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