Съвет на
Европейския съюз

Брюксел, 1 март 2018 г.
(OR. en)

12183/2/17
REV 2

Междуинституционално досие:
2017/0225 (COD)

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139
CSC 276
CSCI 68

ПРЕДЛОЖЕНИЕ

№ док. Ком.:	COM(2017) 477 final/3
Относно:	Предложение за РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА относно ENISA — Агенцията на ЕС за киберсигурност, и за отмяна на Регламент (ЕС) № 526/2013, както и относно сертифицирането на киберсигурността на информационните и комуникационните технологии („Акт за киберсигурността“)

Приложено се изпраща на делегациите документ COM(2017) 477 final/3.

Приложение: COM(2017) 477 final/3

ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 22.2.2018 г.
COM(2017) 477 final/3

2017/0225 (COD)

CORRIGENDUM

This document corrects document COM(2017)477 final of 04.10.2017

Concerns all language versions.

Correction of errors of a clerical nature, correction of some references and adding the title of an article.

The text shall read as follows:

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно ENISA — Агенцията на ЕС за киберсигурност, и за отмяна на Регламент (ЕС) № 526/2013, както и относно сертифицирането на киберсигурността на информационните и комуникационните технологии („Акт за киберсигурността“)

(текст от значение за ЕИП)

{SWD(2017) 500 final} - {SWD(2017) 501 final} - {SWD(2017) 502 final}

ОБЯСНИТЕЛЕН МЕМОРАНДУМ

1. КОНТЕКСТ НА ПРЕДЛОЖЕНИЕТО

• Основания и цели на предложението

Европейският съюз предприе редица действия за повишаване на своята устойчивост и подобряване на своята подготвеност по отношение на киберсигурността. В първата стратегия на ЕС за киберсигурност[1], приета през 2013 г., се определят стратегически цели и конкретни действия за постигане на устойчивост, намаляване на киберпрестъпността, разработване на политика и способности за киберотбрана, разработване на промишлени и технологични ресурси и създаване на последователна международна политика на Европейския съюз по отношение на киберпространството. Оттогава насам в този контекст настъпиха важни промени, като наред с другото по-конкретно беше предоставен втори мандат на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA)[2] и беше приета **Директивата относно сигурността на мрежите и информационните системи**[3] („Директивата за МИС“), които са в основата на настоящото предложение.

Освен това през **2016 г. Европейската комисия прие съобщение, озаглавено „Укрепване на отбранителната способност на Европа срещу кибератаки и изграждане на конкурентен и иновативен сектор на киберсигурността“**[4], в което бяха обявени допълнителни мерки за засилване на сътрудничеството, обмена на информация и на знания, както и за повишаване на устойчивостта и подготвеността на ЕС, с оглед на възможността за широкомащабни инциденти и евентуална общоевропейска криза в областта на киберсигурността. В този контекст Комисията обяви, че ще изтегли напред **оценката** и **преразглеждането** на Регламент (ЕС) № 526/2013 на Европейския парламент и на Съвета относно ENISA и за отмяна на Регламент (ЕО) № 460/2004 („регламент за ENISA“). Процесът на оценяване би могъл да доведе до евентуална реформа на Агенцията и укрепване на нейните способности и нейния капацитет да подкрепя трайно държавите членки. По този начин Агенцията би получила по-активна и централна роля за постигането на киберустойчивост, както и потвърждение чрез новия си мандат на своите нови отговорности съгласно Директивата за МИС.

С Директивата за МИС се прави първа значителна стъпка за насърчаване на развитието на култура на управление на риска, като се въвеждат изисквания за сигурност под формата на правни задължения за основните икономически субекти, по-специално за операторите, предоставящи основни услуги (оператори на основни услуги — ООУ) и доставчиците на някои основни цифрови услуги (доставчици на цифрови услуги — ДЦУ). Предвид особената важност, придавана на изискванията за сигурност за

---

[1] Съвместно съобщение на Европейската комисия и Европейската служба за външна дейност: Стратегия на Европейския съюз за киберсигурност: отворено, безопасно и сигурно киберпространство – JOIN(2013).

[2] Регламент (ЕС) № 526/2013 относно Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) и за отмяна на Регламент (ЕО) № 460/2004.

[3] Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза.

[4] Съобщение на Комисията „Укрепване на отбранителната способност на Европа срещу кибератаки и изграждане на конкурентен и иновативен сектор на киберсигурността“, COM/2016/0410 final.

опазването на ползите от развитието на цифровизацията на обществото, и предвид бързото нарастване на броя на свързаните устройства (интернет на нещата), в съобщението от 2016 г. се предлага също идеята за създаване на рамка за сертифициране на сигурността на ИКТ продукти и услуги, с цел да се повишат доверието в цифровия единен пазар и неговата сигурност. Сертифицирането на киберсигурността на ИКТ става особено актуална тема с оглед на нарасналото използване на технологии, които изискват високо равнище на киберсигурност, като например свързаните автомобили и автомобилите с автоматично управление, електронното здравеопазване или системите за управление на промишлената автоматизация (IACS).

Тези политически мерки и съобщения бяха допълнително подсилени от **заключенията на Съвета** от 2016 г., в които се потвърждава, че „заплахите и уязвимите места в кибернетично отношение продължават да еволюират и да стават все повече, което ще изисква непрекъснато и по-тясно сътрудничество, особено за справяне с мащабни трансгранични инциденти в сферата на киберсигурността“. В заключенията се потвърждава, че регламентът за ENISA е един от „централните елементи на рамката на ЕС за отбранителна способност срещу кибератаки“[5], и се призовава Комисията да предприеме допълнителни стъпки за решаване на въпроса за сертифицирането на европейско равнище.

Създаването на система за сертифициране изисква създаването на подходяща система на управление на равнище ЕС, включително задълбочен експертен опит, предоставян от независима агенция на ЕС. В това отношение в настоящото предложение ENISA се разглежда като естествен кандидат за орган на равнището на ЕС, който е компетентен по въпросите на киберсигурността и следва да поеме една такава роля за обединяване и координиране на работата на националните компетентни органи в областта на сертифицирането.

В своето съобщение относно **средносрочния преглед на стратегията за цифровия единен пазар през май 2017 г.** Комисията уточни, че ще преразгледа мандата на ENISA до септември 2017 г. Това се прави с цел да се определи ролята на ENISA в изменената екосистема на киберсигурността и да се разработят мерки за стандарти в областта на киберсигурността, сертифицирането и етикетирането, чрез които да се подобри киберсигурността на системи, изградени на базата на ИКТ, включително на свързани обекти[6]. В **заключенията на Европейския съвет** от юни 2017 г.[7] се приветства намерението на Комисията да направи преглед на стратегията за киберсигурността през септември и да предложи допълнителни целенасочени действия преди края на 2017 г.

В предложения регламент се предвижда цялостен набор от мерки, основаващи се на предишни действия, и се насърчават взаимно подсилващи се конкретни цели:

- увеличаване на **способностите и подготвеността** на държавите членки и предприятията;

---

5 Заключения на Съвета относно укрепването на отбранителната способност на Европа срещу кибератаки и изграждането на конкурентен и иновативен сектор на киберсигурността – 15 ноември 2016 г.

6 Съобщение на Комисията относно междинния преглед на изпълнението на стратегията за цифров единен пазар — COM(2017) 228.

7 Заседание на Европейския съвет (22 и 23 юни 2017 г.), заключения — EUCO 8/17.

- подобряване на **сътрудничеството и координацията** между държавите членки и институциите, агенциите и органите на ЕС;
- увеличаване на **способностите на равнище ЕС за допълване на действията на държавите членки**, особено в случай на трансгранични киберкризи;
- повишаване на **осведомеността** на гражданите и предприятията по въпроси, свързани с киберсигурността;
- повишаване на цялостната **прозрачност на обезпечаването на киберсигурността**[8] на ИКТ продукти и услуги, с цел да се укрепи доверието в цифровия единен пазар и в цифровите иновации; и
- избягване на **разпокъсаност на схемите за сертифициране** в ЕС и свързаните с тях изисквания за сигурност и критерии за оценка в различните държави членки и сектори.

В следващата част на обяснителния меморандум се разяснява по-подробно основанието за инициативата по отношение на предложените действия за ENISA и сертифицирането на киберсигурността.

[8] Прозрачност на обезпечаването на киберсигурността означава да се предостави на потребителите достатъчно информация за свойствата по отношение на киберсигурността, за да могат те да определят обективно степента на сигурност на даден ИКТ продукт, дадена ИКТ услуга или даден ИКТ процес.

ENISA

ENISA функционира като център за експертен опит, чиято цел е да подобри мрежовата и информационната сигурност в Съюза и да подкрепи изграждането на капацитет в държавите членки.

ENISA беше създадена през 2004 г.[9], с цел да се подпомогне постигането на общата цел за гарантиране на високо ниво на мрежова и информационна сигурност в ЕС. През 2013 г. с Регламент (ЕС) № 526/2013 беше установен нов мандат на Агенцията за период от седем години, до 2020 г. Агенцията се намира в Гърция, по-конкретно нейното административно седалище е в Хераклион (Крит), а оперативната ѝ централа се намира в Атина.

ENISA е малка агенция с малък бюджет и брой служители в сравнение с всички останали агенции на ЕС. Нейният мандат е за ограничен срок.

ENISA подкрепя европейските институции, държавите членки и предприемаческата общност в дейностите им за **справяне с проблеми на мрежовата и информационната сигурност, за реагиране на такива проблеми и особено за тяхното предотвратяване**. За целта тя развива поредица от дейности в пет области, набелязани в нейната стратегия[10]:

- Експертен опит: предоставяне на информация и експертен опит по основни въпроси на мрежовата и информационната сигурност.
- Политика: подкрепа за създаването и изпълнението на политики в Съюза.
- Капацитет: подкрепа за изграждането на капацитет в Съюза (напр. чрез обучения, препоръки, дейности за повишаване на информираността).
- Общност: насърчаване на изграждането на общност за мрежова и информационна сигурност (напр. подкрепа за екипите за незабавно реагиране при компютърни инциденти (CERT), координиране на общоевропейски киберучения).
- Създаване на възможности за други участници (напр. сътрудничество със заинтересованите страни и развиване на международните връзки).

В хода на преговорите по Директивата за МИС, съзаконодателите на ЕС решиха да възложат на ENISA важна роля при прилагането на тази директива. По-специално Агенцията осигурява секретариата на мрежата на CSIRT (създадена, за да насърчава бързата и ефективна оперативна координация между държавите членки по конкретни киберинциденти и споделянето на информация относно рискове), като от нея се очаква също да подпомага групата за сътрудничество при изпълнението на нейните задачи. В допълнение директивата изисква ENISA да подпомага държавите членки и Комисията, като предоставя на разположение своя експертен опит, дава консултации и улеснява обмена на най-добри практики.

---

9 Регламент (ЕО) № 460/2004 на Европейския парламент и на Съвета от 10 март 2004 г. относно създаване на Европейската агенция за мрежова и информационна сигурност (ОВ L 77, 13.3.2004 г., стр. 1).

10 https://www.enisa.europa.eu/publications/corporate/enisa-strategy

В съответствие с регламента за ENISA Комисията извърши оценка на Агенцията, включваща независимо проучване и обществена консултация. При оценката бяха разгледани значимостта, въздействието, ефективността, ефикасността, съгласуваността и добавената стойност за ЕС на Агенцията с оглед на нейното функциониране, управление, вътрешна организационна структура и работни практики през периода 2013—2016 г.

Цялостното функциониране на ENISA бе оценено положително от мнозинството от участвалите[11] в обществената консултация (74 %). Повечето от отговорилите също така считат, че ENISA постига различните поставени ѝ цели (най-малко 63 % за всяка от целите). Услугите и продуктите на ENISA се ползват редовно (веднъж месечно или по-често) от почти половината от отговорилите (46 %) и се ценят поради факта, че са предоставени от орган на равнище ЕС (83 %), както и заради качеството им (62 %).

При все това голямо мнозинство (88 %) от отговорилите считат настоящите инструменти и механизми, които са на разположение на равнището на ЕС, за недостатъчни или само частично адекватни за преодоляването на актуалните предизвикателства в областта на киберсигурността. Голямо мнозинство от отговорилите (98 %) посочиха, че с тези потребности следва да се заеме орган на ЕС, като 99 % от тях считат, че ENISA е подходящата за целта организация. В допълнение, 67,5 % от отговорилите изразиха мнение, че ENISA може да има роля при създаването на хармонизирана рамка за сертифициране на сигурността на ИКТ продукти и услуги.

В общата оценка (основаваща се както на обществената консултация, така и на редица допълнителни индивидуални интервюта, целеви проучвания и семинари) се правят следните заключения:

- Целите на ENISA продължават да са актуални и днес. В контекста на бързо развиващите се технологии и променящите се заплахи и с оглед на нарастването на глобалните рискове за киберсигурността е налице ясна потребност да продължава да се насърчава и укрепва техническият експертен опит на високо равнище по въпросите на киберсигурността. В държавите членки трябва да се изгради капацитет за разбиране на заплахите и съответно реагиране и заинтересованите страни трябва да си сътрудничат отвъд границите на конкретни тематични области и конкретни институции.
- Независимо от малкия си бюджет Агенцията е използвала ефикасно своите ресурси в оперативен план и при изпълнението на своите задачи. В резултат на разделянето на функциите между Атина и Ираклион обаче са възникнали също допълнителни административни разходи.
- По отношение на ефективността ENISA е изпълнила частично своите цели. Агенцията успешно е допринесла за подобряване на мрежовата и информационна сигурност в Европа, предлагайки изграждане на капацитет в 28 държави членки[12], съдействайки за укрепването на сътрудничеството между

[11] 90 заинтересовани страни от 19 държави членки отговориха на консултацията (88 отговора и 2 документа за изразяване на позиция), в това число национални органи от 15 държави членки и 8 асоциации, представляващи значителен брой европейски предприятия.

[12] Участващите в обществената консултация бяха помолени да коментират кои според тях са основните постижения на ENISA в периода 2013—2016 г. Според участници в консултацията от всички групи (общо 55, от които 13 от национални органи, 20 от частния сектор и 22 от групата „други“) основните постижения на ENISA са следните: 1) координирането на ученията „Cyber

държавите членки и заинтересованите страни в областта на мрежовата и информационната сигурност и предоставяйки експертен опит, изграждане на общности и подкрепа за разработването на политики. Като цяло усилията на ENISA бяха надлежно съсредоточени върху изпълнението на нейната работна програма и тя беше надежден партньор за своите заинтересовани страни в област, чието важно трансгранично значение беше осъзнато едва неотдавна.

- ENISA успя, поне в известна степен, да упражни своето влияние в огромната област на мрежовата и информационната сигурност, но не успя напълно да си създаде име и да придобие достатъчна популярност, за да бъде призната като „най-важен“ център на експертен опит в Европа. Това се обяснява с широкия мандат на ENISA, който не беше подкрепен от пропорционални и достатъчни ресурси. Освен това ENISA остава единствената агенция на ЕС с мандат с фиксиран срок, което ограничава нейните възможности да развива дългосрочна концепция и да оказва трайна подкрепа на съответните заинтересовани страни. Това също така е в противоречие с разпоредбите на Директивата за МИС, с които на ENISA се възлагат задачи без краен срок. И накрая, оценката показа, че тази ограничена ефективност може отчасти да се обясни с преобладаващото използване на външен експертен опит за сметка на вътрешния, както и с трудностите при набирането и задържането на квалифициран персонал.
- Не на последно място, оценката стига до заключението, че добавената стойност на ENISA се дължи предимно на нейната способност да подобрява сътрудничеството, основно между държавите членки, и по-специално сътрудничеството със съответните общности в областта на мрежовата и информационната сигурност (по-специално между екипите CSIRT). Няма друг участник на равнище ЕС, който да подкрепя такъв широк обхват от заинтересовани страни в областта на мрежовата и информационната сигурност. Въпреки това, поради необходимостта от строго приоритизиране на дейностите на ENISA, нейната работна програма е съобразена предимно с потребностите на държавите членки. В резултат на това в нея не се отделя достатъчно внимание на потребностите на други заинтересовани страни, по-специално на промишлеността. Това доведе също до начин на работа, при който Агенцията само реагира на потребностите на своите основни заинтересовани страни, вместо да се заеме проактивно с тях, което не ѝ позволява да постигне по-голямо въздействие. Поради това добавената от Агенцията стойност бе различна и зависеше от потребностите на заинтересованите страни и степента, в която тя беше в състояние да ги удовлетвори (например с оглед на противопоставянето на интересите на големите и на малките държави членки; на интересите на държавите членки и тези на промишлеността).

В крайна сметка резултатите от консултациите със заинтересованите страни и оценката показаха, че ресурсите и мандатът на ENISA трябва да бъдат адаптирани така, че

Europe“; 2) предоставянето на помощ на екипи CERT/CSIRT чрез обучение и семинари за насърчаване на координацията и обмена; 3) публикациите на ENISA (насоки и препоръки, прегледи на актуалните заплахи, стратегии за докладване на инциденти и за управление на кризи и т.н.), които се считат за полезни както за създаването и актуализирането на националните рамки за сигурност, така и в качеството им на справочни документи за създателите на политики и работещите в областта на кибертехнологии; 4) помощта при практическото прилагане на Директивата за МИС; 5) усилията за повишаване на осведомеността в областта на киберсигурността чрез провеждането на месец на киберсигурността.

агенцията да може да играе адекватна роля при преодоляването на настоящи и бъдещи предизвикателства.

С оглед на тези съображения в настоящото предложение се прави преглед на текущия мандат на ENISA и се определя нов набор от задачи и функции с цел ефективна и ефикасна подкрепа за усилията на държавите членки, институциите на ЕС и други заинтересовани страни за постигането на сигурно киберпространството в Европейския съюз. Целта на предложения нов мандат е да се предостави на Агенцията по-силна и по-централна роля, в която тя по-специално да подкрепя държавите членки в прилагането на Директивата за МИС и да противодейства на определени заплахи по-активно (оперативен капацитет), както и да се превърне в център на експертен опит в подкрепа на държавите членки и на Комисията при сертифицирането на киберсигурността. Съгласно настоящото предложение:

- ENISA ще получи постоянен мандат и по този начин ще бъде поставена на стабилна основа в бъдеще. Мандатът, целите и задачите следва да се подлагат на редовен преглед.
- Предложеният мандат изяснява допълнително ролята на ENISA като агенцията на ЕС за киберсигурност и като отправна точка в екосистемата на киберсигурността в ЕС, действаща в тясно сътрудничество с всички други съответни органи на тази екосистема.
- Организацията и управлението на Агенцията, които получиха положителни отзиви в хода на оценката, ще бъдат умерено преработени, по-специално, за да се гарантира, че работата на Агенцията отразява по-добре потребностите на по-широка общност от заинтересовани страни.
- Предложеният обхват на мандата е очертан така, че да укрепи капацитета на Агенцията в областите, където тя е доказала ясно своята добавена стойност, и да добави новите области, в които е необходима подкрепа с оглед на новите приоритети на политиката и инструменти, по-специално Директивата за МИС, прегледа на стратегията на ЕС за киберсигурност, разработваната в момента концепция на ЕС за киберсигурността относно сътрудничеството при киберкризи и сертифицирането на сигурността на ИКТ:
    - **Разработване и изпълнение на политики на ЕС:** ENISA ще бъде натоварена със задачата да допринася проактивно за разработването на политиката в областта на мрежовата и информационната сигурност, както и за други политически инициативи с елементи на киберсигурност в различни сектори (например енергетика, транспорт, финанси). За тази цел тя ще има силна консултативна роля, която би могла да изпълнява, като предоставя независими становища и извършва подготвителна работа за разработването и актуализирането на политиката и правото. ENISA ще подпомага също политиката и правото на ЕС в областта на електронните съобщения, електронната идентификация и удостоверителните услуги, с цел да се насърчи едно по-високо равнище на киберсигурност. На етапа на изпълнение, по-специално в рамките на групата за сътрудничество във връзка с МИС, ENISA ще подпомага държавите членки в постигането на последователен подход относно трансграничното и междусекторното прилагане на Директивата за МИС, както и при други политики и закони от значение. В подкрепа на редовното преразглеждане на политиките и законите в областта на киберсигурността ENISA ще предоставя също така

редовни доклади относно състоянието на прилагането на правната рамка на ЕС.

- **Изграждане на капацитет:** ENISA ще допринася за подобряването на способностите и експертния опит на ЕС и на националните публични органи, включително по въпросите на реагирането при инциденти и надзора на изпълнението на регулаторните мерки, свързани с киберсигурността. От Агенцията ще се иска също да допринася за създаването на центрове за споделяне и анализ на информация (ISACS) в различни сектори чрез предоставянето на най-добри практики и насоки относно наличните инструменти и процедури, както чрез подходящо разглеждане на регулаторните въпроси, свързани с обмена на информация.

- **Знания и информация, повишаване на осведомеността:** ENISA ще се превърне в информационен център на ЕС. Това предполага насърчаването и обмена на най-добри практики и инициативи в целия ЕС чрез обединяване на информацията относно киберсигурността, произхождаща от европейските и националните институции, агенции и органи. Агенцията също така ще предоставя консултации, насоки и най-добри практики относно сигурността на критичната инфраструктура. Освен това, след значителни трансгранични киберинциденти ENISA ще изготвя доклади с цел да се предоставят насоки на предприятията и гражданите в целия ЕС. Този работен поток ще включва също така редовното организиране на дейности за повишаване на осведомеността в координация с органите на държавите членки.

- **Задачи, свързани с пазара (стандартизиране, сертифициране на киберсигурността):** ENISA ще изпълнява редица функции, които конкретно подпомагат вътрешния пазар и служат като „обсерватория на пазара“ на киберсигурността, като анализира съответните тенденции на този пазар с цел да се постигне по-добро съответствие между търсенето и предлагането, и като подкрепя разработването на политиката на ЕС в областите на стандартизацията на ИКТ и сертифицирането на киберсигурността на ИКТ. По-конкретно, в областта на стандартизацията тя ще улеснява създаването и внедряването на стандарти за киберсигурността. ENISA ще изпълнява също задачите, предвидени в контекста на бъдещата рамка за сертифициране (вж. следващия раздел).

- **Научни изследвания и иновации:** ENISA ще предоставя своя експертен опит чрез консултации на органи на ЕС и на национални органи относно определянето на приоритетите в областта на научните изследвания и разработки, включително в рамките на договорното публично-частно партньорство в областта на киберсигурността (ДПЧП). Консултациите на ENISA относно научните изследвания ще бъдат включени в новия Европейски експертен център за научни изследвания в областта на киберсигурността в рамките на следващата многогодишна финансова рамка. По искане на Комисията ENISA ще участва също в изпълнението на програмите на ЕС за финансиране на научни изследвания и иновации.

- **Оперативно сътрудничество и управление на кризи:** този работен поток следва да се основава на укрепването на съществуващите оперативни способности за превенция, по-специално чрез подобряване на

общоевропейските учения в областта на киберсигурността (Cyber Europe), като се предвижда ежегодното им провеждане, както и на поддържащата роля при оперативното сътрудничество в ролята на секретариат на мрежата на CSIRT (съгласно разпоредбите на Директивата за МИС), като осигурява, наред с другото, доброто функциониране на ИТ инфраструктурата и каналите за комуникация на мрежата на CSIRT. В този контекст ще е необходимо структурирано сътрудничество с CERT-EU, Европейския център за борба с киберпрестъпността (European Cybercrime Centre — EC3) и други съответни органи на ЕС. Освен това едно структурирано сътрудничество с CERT-EU в непосредствена географска близост следва да доведе до създаване на възможности за предоставяне на техническа помощ в случай на значителни инциденти и да подкрепи анализите на инцидентите. При поискване държавите членки ще получават помощ при справянето с инциденти, както и подкрепа за извършването на анализи на уязвими точки, артефакти и инциденти, с цел да укрепят своите собствени способности за превенция и реагиране.

- ENISA ще има също роля в **концепцията на ЕС за киберсигурността**, която представлява част от настоящия пакет и в която Комисията препоръчва на държавите членки да координират реакцията си при мащабни трансгранични инциденти и кризи в областта на киберсигурността на равнище ЕС[13]. ENISA ще улесни сътрудничеството между отделните държави членки за незабавното реагиране чрез анализ и обобщение на националните доклади за ситуацията въз основа на информацията, предоставена на Агенцията на доброволни начала от държавите членки и други субекти.

- **Сертифициране на киберсигурността на ИКТ продукти и услуги**

За изграждането на доверие и постигането на сигурност, а също и за тяхното запазване, е необходимо характеристики за сигурност да бъдат включвани още в първите етапи на техническото проектиране и разработване на ИКТ продукти и услуги („сигурност още при проектирането“). Освен това трябва да е възможно за клиентите и потребителите да се уверяват в равнището на обезпечаване на сигурността при продуктите и услугите, които те придобиват или закупуват.

Важна роля за повишаване на доверието в продуктите и услугите и подобряване на тяхната сигурност играе сертифицирането, чиито елементи са официалното оценяване от независим и акредитиран орган на продукти, услуги и процеси спрямо определен набор от стандарти и критерии и издаването на сертификат, доказващ наличието на съответствие. Докато оценяването на сигурността е доста техническа дейност, сертифицирането има за цел да даде информация и увереност на купувачите и потребителите относно свързаните със сигурността характеристики на ИКТ продуктите и услугите, които те купуват или използват. Както е посочено по-горе, това се отнася особено за новите системи, широко използващи цифрови технологии и изискващи

[13] „Концепцията“ ще се прилага по отношение на инциденти с киберсигурността, които предизвикват смущения, по-големи от тези, с които отделна държава членка би могла да се справи сама, или засягат две или повече държави членки и имат толкова широкообхватно и значително въздействие или политическо значение, че изискват своевременна политическа координация и реакция на политическото равнище на Съюза.

висока степен на сигурност, напр. свързани автомобили и автомобили с автоматично управление, електронно здравеопазване, системи за управление на промишлената автоматизация (IACS)[14] или интелигентни енергийни мрежи.

Понастоящем картината в областта на сертифицирането на киберсигурността на ИКТ продукти и услуги в ЕС е доста неоднородна. Съществуват редица международни инициативи, като например т. нар. „Общи критерии (ОК) за оценяване на сигурността на информационните технологии“ (ISO 15408), представляващи международен стандарт за оценка на сигурността на компютърни системи. Тази инициатива се основава на оценка от трета страна и предвижда седем нива за оценяване на обезпечеността (Evaluation Assurance Levels — EAL). ОК и придружаващата ги обща методология за оценка на сигурността на информационните технологии (CEM) са техническата основа за международно споразумение, т.нар. „Договореност за признаване на общите критерии“ (CCRA), която гарантира, че ОК сертификатите се признават от всички подписали CCRA страни. Съгласно настоящата версия на CCRA обаче взаимно се признават само оценки до ниво EAL 2. Освен това само 13 държави членки са подписали тази договореност.

Сертифициращите органи на 12 държави членки са сключили споразумение за взаимно признаване на сертификати, издадени в съответствие със споразумението въз основа на Общите критерии[15]. Освен това в държавите членки понастоящем съществуват или са в процес на установяване редица инициативи за сертифициране на ИКТ. Въпреки своята важност те пораждат риск от разпокъсване на пазара и проблеми с оперативната съвместимост. Вследствие на това, може да се наложи едно предприятие да премине през няколко процедури по сертифициране в различните държави членки, за да може да предлага продукта си на множество пазари. Например, ако даден производител на интелигентен измервателен уред иска да продава продуктите си в три държави членки, напр. Германия, Франция и Обединеното кралство, към момента той трябва да спазва три различни схеми за сертифициране. Това са „Commercial Product Assurance (CPA)“ в Обединеното кралство, „Certification de Sécurité de Premier Niveau in France (CSPN)“ във Франция и специален защитен профил, основаващ се на Общите критерии, в Германия.

Това води до по-високи разходи и представлява значителна административна тежест за предприятията, които работят в няколко държави членки. Въпреки че разходите за сертифициране може да се различават чувствително в зависимост от продукта/услугата, изискваното ниво за оценка на обезпечеността и/или други компоненти, като цяло те обикновено са доста значителни за предприятията. Например разходите за сертификата BSI „Smart Meter Gateway“ възлизат на повече от един милион евро (най-високо ниво на изпитване и обезпеченост, което се отнася не само за един продукт, а за цялата инфраструктура около него). Разходите за сертифициране за интелигентни измервателни уреди в Обединеното кралство са почти 150 000 EUR. Във Франция

[14] ГД JRC публикува доклад, който предлага първоначален набор от общи европейски изисквания и общи насоки във връзка със сертифицирането на киберсигурността на компоненти на системи за управление на промишлената автоматизация. Документът е достъпен на адрес: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

[15] Групата на висшите служители по сигурността на информационните системи (SOG-IS) включва 12 държави членки плюс Норвегия и е разработила няколко защитни профила за ограничен брой продукти, като например цифров подпис, цифров тахограф и карти с чип. Участниците работят заедно за координиране на стандартизирането на защитните профили на базата на ОК и координират разработването на защитни профили. Държавите членки често изискват сертифициране по SOG-IS при националните търгове за обществени поръчки.

разходите са подобни на тези в Обединеното кралство — около 150 000 EUR или повече.

Основни публични и частни заинтересовани страни признаха, че в отсъствието на общоевропейска схема за сертифициране на киберсигурността, предприятията в много случаи трябва да бъдат сертифицирани във всяка държава членка, което води до разпокъсване на пазара. Най-важното е, че при липсата на законодателство за хармонизиране на равнище ЕС за ИКТ продукти и услуги, различията в стандартите за сертифициране на киберсигурността и практиките в държавите членки могат да породят 28 различни пазара в областта на сигурността в ЕС, всеки от тях със свои собствени технически изисквания, методики за изпитване и процедури за сертифициране на киберсигурността. Ако не бъдат предприети подходящи действия на равнище ЕС, тези различаващи се подходи на национално равнище могат да доведат до значителни пречки за осъществяването на цифровия единен пазар и да забавят или предотвратят свързаните с него положителни ефекти по отношение на растежа и работните места.

Въз основа на посоченото по-горе в предложения регламент се създава Европейска рамка за сертифициране на киберсигурността на ИКТ продукти и услуги („**Рамката**“) и се определят основните функции и задачи на ENISA в областта на сертифицирането на киберсигурността. Настоящото предложение предвижда цялостна рамка от правила, регламентиращи европейските схеми за сертифициране на киберсигурността. С предложението не се въвеждат пряко действащи схеми за сертифициране, а се установява система (рамка) за създаването на специфични схеми за сертифициране на конкретни ИКТ продукти/услуги (т.нар. „европейски схеми за сертифициране на киберсигурността“). Създаването на европейски схеми за сертифициране на киберсигурността в съответствие с рамката ще позволи сертификатите, издавани по тези схеми, да са валидни и да се признават във всички държави членки и ще бъде принос към решаването на проблема с разпокъсаността на пазара понастоящем.

Общото предназначение на една европейска схема за сертифициране на киберсигурността е да удостоверява, че ИКТ продуктите и услугите, които са сертифицирани по тази схема, съответстват на посочените изисквания в областта на киберсигурността. Това ще включва например способността им да защитават данните (независимо дали те се съхраняват, предават или обработват по друг начин) срещу случайно или незаконно съхраняване, обработка, достъп, разкриване, унищожаване, случайна загуба или промяна. Схемите на ЕС за сертифициране на киберсигурността ще се основават на съществуващите стандарти по отношение на техническите изисквания и процедурите за оценка, на които продуктите трябва да съответстват, но няма да разработват самите технически стандарти[16]. Например едно обхващащо целия ЕС сертифициране на продукти като картите с чип, които понастоящем се изпитват (а преди това са били описани) съгласно международните ОК стандарти в рамките на многостранната схема SOG-IS, би означавало, че тази схема става валидна в целия ЕС.

Освен конкретен набор от цели по отношение на сигурността, които да се вземат предвид при проектирането на конкретна европейска схема за сертифициране на киберсигурността, в предложението се определя какво най-малко би трябвало да съдържат тези схеми. Тези схеми ще трябва да включват, наред с другото, редица

[16] В случай на европейски стандарти това се извършва чрез европейските организации за стандартизация и се одобрява от Европейската комисия чрез публикация в *Официален вестник на Европейския съюз* (вж. Регламент (ЕС) № 1025/2012).

конкретни елементи, определящи обхвата и предмета на сертифицирането на киберсигурността. Сред тях са определянето на обхванатите от схемата категории продукти и услуги, подробното специфициране на изискванията в областта на киберсигурността (например чрез позоваване на съответните стандарти или технически спецификации), специфичните критерии и методи за оценка и нивото на обезпечаване на сигурноста, което те трябва да гарантират (т.е. „основно“, „значително“ или „високо“).

Европейските схеми за сертифициране на киберсигурността ще бъдат изготвяни от ENISA с подкрепата, експертния опит и тясното сътрудничество на Европейската група по сертифициране на киберсигурността (вж. по-долу) и ще се приемат от Комисията посредством актове за изпълнение. Когато бъде установена необходимост от схема за сертифициране на киберсигурността, Комисията ще възлага на ENISA да изготви схема за конкретните ИКТ продукти или услуги. ENISA ще работи по схемата в тясно сътрудничество с националните надзорни органи за сертифицирането, представени в групата. Държавите членки и групата могат да предложат на Комисията да възложи на ENISA да изготви дадена схема.

Сертифицирането може да бъде много скъп процес, което от своя страна би могло да доведе до по-високи цени за клиентите и потребителите. Необходимостта от сертифициране също може да е много различна в зависимост от конкретния контекст на употреба на продуктите и услугите и скоростта на технологичните промени. Поради това европейското сертифициране на киберсигурността следва да остане доброволно, освен ако не е предвидено друго в законодателството на Съюза, определящо изискванията за сигурност на ИКТ продукти и услуги.

С цел да се осигури хармонизиране и да се избегне разпокъсаност в областта на киберсигурността, националните схеми или процедури за сертифициране на ИКТ продукти и услуги, обхванати от дадена европейска схема за сертифициране на киберсигурността, престават да се прилагат от датата, определена в акта за изпълнение, с който се приема схемата. Освен това държавите членки следва да не въвеждат нови национални схеми за сертифициране на киберсигурността на ИКТ продукти и услуги, които са вече обхванати от съществуваща европейска схема за сертифициране на киберсигурността.

След като дадена европейска схема за сертифициране на киберсигурността бъде приета, производителите на ИКТ продукти или доставчиците на ИКТ услуги ще могат да подават заявления за сертифициране на своите продукти или услуги до орган за оценяване на съответствието по техен избор. Органите за оценяване на съответствието следва да се акредитират от орган по акредитация, ако отговарят на определени конкретни изисквания. Акредитацията се издава за максимален срок от пет години и може да бъде подновена при същите условия, ако органът за оценяване на съответствието отговаря на изискванията. Органите по акредитация ще отнемат акредитацията на органа за оценяване на съответствието, ако условията за акредитация не са били спазени или вече не се спазват, или ако органът за оценяване на съответствието е предприел действия, които нарушават разпоредбите на настоящия регламент.

Съгласно предложението задачите по мониторинга, надзора и правоприлагането са задължение на държавите членки. Държавите членки трябва да предвидят надзорен орган за сертифицирането. Този орган ще бъде натоварен с надзора на органите за оценяване на съответствието, както и на сертификатите, издадени от такива органи, установени на тяхна територия, във връзка със спазването на изискванията на

настоящия регламент и на относимите европейски схеми за сертифициране на киберсигурността. Националните надзорни органи за сертифицирането ще имат правомощия да разглеждат жалбите, подадени от физически или юридически лица по отношение на сертификатите, издадени от органите за оценяване на съответствието, установени на тяхна територия. Те ще разследват предмета на жалбата в подходяща степен и ще информират жалбоподателя за напредъка на разследването и резултатите от него в разумен срок. Освен това те ще си сътрудничат с други надзорни органи за сертифицирането или други публични органи, например чрез споделяне на информация за възможни несъответствия на ИКТ продукти и услуги с изискванията на настоящия регламент или със съответните европейски схеми за сертифициране на киберсигурността.

И накрая, с предложението се създава Европейска група за сертифициране на киберсигурността („групата“), състояща се от национални надзорни органи за сертифицирането от всички държави членки. Основната задача на групата е да съветва Комисията по въпроси, свързани с политиката за киберсигурност, и да си сътрудничи с ENISA по разработването на проекти за европейски схеми за сертифициране на киберсигурността. ENISA ще подпомага Комисията при осигуряването на секретариата на групата и ще поддържа актуален публично достъпен опис на схемите, одобрени съгласно Европейската рамка за сертифициране на киберсигурността. ENISA ще си сътрудничи с органите по стандартизация, за да бъде гарантирана целесъобразността на стандартите, използвани в одобрените схеми, и да бъдат определени областите, в които са необходими стандарти за киберсигурност.

Европейската рамка за сертифициране на киберсигурността („рамката“) ще осигури редица ползи за гражданите и за предприятията. По-специално:

- Създаването на схеми за сертифициране на киберсигурността, валидни в целия ЕС за специфични продукти или услуги, ще предостави на предприятията „обслужване на едно гише“ за сертифицирането на киберсигурността в ЕС. Тези предприятия ще могат с едно единствено сертифициране да получат сертификат, валиден във всички държави членки. Те няма да бъдат задължени да сертифицират повторно своите продукти при други национални сертифициращи органи. Така значително ще се намалят разходите за предприятията, ще се улеснят трансграничните операции и в крайна сметка ще се намали и предотврати разпокъсването на вътрешния пазар на съответните продукти.
- С рамката се установява върховенството на европейските схеми за сертифициране на киберсигурността над националните схеми. Съгласно това правило, приемането на европейска схема за сертифициране на киберсигурността отменя всички съществуващи успоредно национални схеми за същите ИКТ продукти или услуги при дадено ниво на обезпечаване на сигурност. Това ще доведе до повече яснота и ще намали разпространението на припокриващи се и евентуално противоречащи си национални схеми за сертифициране на киберсигурността.
- Предложението подкрепя и допълва изпълнението на Директивата за МИС, като предоставя на предприятията, за които се прилага директивата, един много полезен инструмент за доказване на спазването на изискванията за МИС в целия Съюз. При разработването на нови схеми за сертифициране в областта на киберсигурността Комисията и ENISA ще обърнат особено внимание на

необходимостта да се гарантира, че изискванията за МИС са отразени в схемите за сертифициране на киберсигурността.

- Предложението ще подкрепи и улесни развитието на европейска политика за киберсигурността, като хармонизира условията и съществените изисквания за сертифициране на киберсигурността на ИКТ продукти и услуги в ЕС. Мерките за киберсигурност в европейските схеми за сертифициране ще се основават на общи стандарти или критерии на методиките за оценяване или изпитване. Това ще допринесе в значителна степен, макар и косвено, за навлизането на общи решения в областта на сигурността в ЕС, като по този начин ще се премахнат пречките пред вътрешния пазар.
- Рамката е разработена така, че да осигурява необходимата гъвкавост за схемите за сертифициране на киберсигурността. В зависимост от конкретните потребности в областта на киберсигурността даден продукт или дадена услуга могат да бъдат сертифицирани за по-високи или по-ниски нива на сигурност. Европейските схеми за сертифициране на киберсигурността ще бъдат проектирани с идеята да се постигне такава гъвкавост и следователно ще предвиждат различни нива на обезпеченост (т.е. „основно“, „значително“ или „високо“), така че да могат да се използват за различни цели или в различен контекст.
- Всички посочени по-горе елементи ще направят сертифицирането на киберсигурността по-привлекателно за предприятията, превръщайки го в ефективно средство за оповестяване на нивото на обезпечаване на киберсигурността на ИКТ продукти или услуги. Колкото по-евтино, по-ефективно и икономически по-привлекателно става сертифицирането на киберсигурността, толкова по-голям стимул ще имат предприятията да сертифицират своите продукти по отношение на рисковете, свързани с киберсигурността, като по този начин ще допринасят за разпространението на по-добри практики по отношение на киберсигурността при разработването на ИКТ продукти и услуги („киберсигурност още при проектирането“).

- **Съгласуваност с действащите разпоредби в тази област на политиката**

Съгласно Директивата за МИС операторите в отделни сектори, които са жизненоважни за нашата икономика и общество, като например енергетиката, транспорта, водните ресурси, банковото дело, инфраструктурите на финансовия пазар, здравеопазването и цифровата инфраструктура, както и доставчиците на цифрови услуги (т.е. интернет търсачки, услуги за изчисления в облак и платформи за онлайн търговия) са задължени да предприемат мерки за подходящо управление на рисковете за сигурността. Новите разпоредби на настоящото предложение допълват разпоредбите на Директивата за МИС и осигуряват съгласуваност с тях, за да бъде постигната още по-голяма киберустойчивост на ЕС чрез подобряване на способностите, сътрудничеството, управлението на риска и осведомеността.

Освен това, правилата за сертифициране на киберсигурността са основен инструмент за предприятията, за които се прилага Директивата за МИС, тъй като ще им позволят да сертифицират своите ИКТ продукти и услуги спрямо рисковете в областта на киберсигурността въз основа на схеми за сертифициране на киберсигурността, които са

валидни и признати в целия ЕС. Те ще допълват също така изискванията за сигурност, посочени в регламента за eIDAS[17] и директивата за радиосъоръженията[18].

- **Съгласуваност с другите политики на Съюза**

С Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните — **ОРЗД**)[19] се установяват разпоредби за създаване на механизми за сертифициране и на печати и маркировки за защита на данните, които трябва да доказват съответствието с посочения регламент на операциите по обработката на данни от страна на контролиращите и обработващите тези данни. Настоящият регламент не засяга сертифицирането на операции по обработката на данни съгласно ОРЗД, включително когато тези операции са включени в продукти и услуги.

Предложеният регламент осигурява съвместимост с Регламент (ЕО) № 765/2008 относно изискванията за акредитация и надзор на пазара[20], като включва препратка към правилата на тази рамка относно националните органи по акредитация и органите за оценяване на съответствието. Що се отнася до надзорните органи, предложеният регламент ще изисква от държавите членки да определят национални надзорни органи за сертифицирането, които да поемат отговорност за надзора, мониторинга и прилагането на правилата. Тези органи ще бъдат различни от органите за оценяване на съответствието, както е предвидено в Регламент (ЕО) № 765/2008.

2. ПРАВНО ОСНОВАНИЕ, СУБСИДИАРНОСТ И ПРОПОРЦИОНАЛНОСТ

- **Правно основание**

Правното основание за действия на равнище ЕС е член 114 от Договора за функционирането на Европейския съюз (ДФЕС), с който се урежда сближаването на законодателствата на държавите членки с цел постигане на целите на член 26 от ДФЕС, а именно, правилното функциониране на вътрешния пазар.

Правното основание за създаването на ENISA с цел постигане на вътрешния пазар бе потвърдено от Съда на Европейския съюз (дело C-217/04, *Обединеното кралство срещу Европейския парламент и Съвета*), както и от регламента от 2013 г., с който бе определен настоящият мандат на Агенцията. В допълнение, дейности, които съответстват на целите за разширяване на сътрудничеството и засилване на координацията между държавите членки и за развиване на равнище ЕС на способности за допълване на действията на държавите членки, биха попаднали в категорията на „оперативно сътрудничество“. Това изрично се определя в Директивата за МИС (чието

[17] Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО.

[18] Директива 2014/53/ЕС на Европейския парламент и на Съвета от 16 април 2014 г. за хармонизирането на законодателствата на държавите членки във връзка с предоставянето на пазара на радиосъоръжения и за отмяна на Директива 1999/5/ЕО.

[19] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1—88).

[20] Регламент (ЕО) № 765/2008 за определяне на изискванията за акредитация и надзор на пазара във връзка с предлагането на пазара на продукти и за отмяна на Регламент (ЕИО) № 339/93.

правно основание е член 114 от ДФЕС) като цел, която трябва да бъде преследвана в рамките на мрежата на CSIRT, при което „ENISA осигурява административното обслужване и активно подкрепя сътрудничеството“ (член 12, параграф 2). По-специално, в член 12, параграф 3, буква е) се подчертава отново, че набелязването на допълнителни форми на оперативно сътрудничество е задача на мрежата на CSIRT, включително по отношение на: i) категориите рискове и инциденти; ii) ранните предупреждения; iii) взаимопомощта; и iv) принципите и условията за координация на реакцията на държавите членки при трансгранични рискове и инциденти.

- Настоящата разпокъсаност на схемите за сертифициране на ИКТ продукти и услуги се дължи също на липсата на общ правно обвързващ и ефективен рамков процес, приложим за държавите членки. Това възпрепятства създаването на вътрешен пазар за ИКТ продукти и услуги и накърнява конкурентоспособността на промишлеността на ЕС в този сектор. Целта на настоящото предложение е да се преодолеят съществуващата разпокъсаност и сродните пречки пред вътрешния пазар, като се предостави обща рамка за създаване на схеми за сертифициране на киберсигурността, валидни в целия ЕС.

Субсидиарност (при неизключителна компетентност)

Принципът на субсидиарност изисква оценка на необходимостта от действия на ЕС и на тяхната добавена стойност. Валидността на принципа на субсидиарност в тази област вече е била призната при приемането на действащия регламент за ENISA[21].

Киберсигурността е въпрос от общ интерес за Съюза. Взаимовръзките между мрежите и информационните системи са такива, че отделните участници (публични и частни, включително гражданите) много често не са в състояние да се справят поотделно със заплахите, рисковете и възможните въздействия на киберинциденти. От една страна, взаимозависимостите между държавите членки, включително по отношение на дейността на критичните инфраструктури (енергетиката, транспортът, водоснабдяването са само няколко примера за такива инфраструктури) правят публичната намеса на европейско равнище не само полезна, но и необходима. От друга страна, намесата на ЕС може да има допълнителен положителен ефект като следствие на обмена на добри практики между държавите членки, което може да доведе до повишаване на киберсигурността в Съюза.

Като цяло изглежда, че в настоящия контекст и с оглед на възможните бъдещи сценарии, за **увеличаването на колективната киберустойчивост** на Съюза няма да са достатъчни **индивидуални действия на държавите — членки на ЕС, нито пък индивидуален подход към киберсигурността**.

Счита се, освен това, че действия на равнището на ЕС са необходими и за преодоляването на разпокъсаността на настоящите схеми за сертифициране на киберсигурността. Това би позволило на производителите да се възползват изцяло от вътрешния пазар и би донесло значителни икономии по отношение на разходите за изпитвания и преработки. Въпреки че настоящото споразумение за взаимно признаване (СВП) на Групата на висшите служители по сигурността на информационните системи

[21] Регламент (ЕС) № 526/2013 на Европейския парламент и на Съвета от 21 май 2013 година относно Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) и за отмяна на Регламент (ЕО) № 460/2004.

(SOG-IS) е постигнало значителни резултати в това отношение, при него са налице също така съществени ограничения, които му пречат да бъде подходящ инструмент за постигане на дългосрочни устойчиви решения за разгръщането на пълния потенциал на вътрешния пазар.

Добавената стойност на действията на равнището на ЕС, по-специално на тези от тях, насочени към засилване на сътрудничеството между държавите членки, както и между общностите в областта на мрежовата и информационната сигурност, бе призната в заключенията на Съвета от 2016 г.[22] и проличава също така ясно в оценката на ENISA.

- **Пропорционалност**

Предложените мерки не надхвърлят необходимото за постигане на поставените цели. Освен това обхватът на намесата на ЕС не е пречка за допълнителни действия на национално равнище в областта на националната сигурност. Поради това действията на равнище ЕС са оправдани от гледна точка на субсидиарността и пропорционалността.

- **Избор на инструмент**

С настоящото предложение се преразглежда Регламент (ЕС) № 526/2013, който определя понастоящем мандата и задачите на ENISA. Освен това, като се има предвид важната роля на ENISA за създаването и управлението на рамка на ЕС за сертифициране на киберсигурността, ще бъде най-добре новият мандат на ENISA и посочената рамка да бъдат установени с помощта на един-единствен правен инструмент, а именно — регламент.

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

Последващи оценки/проверки за пригодност на действащото законодателство

Комисията оцени в съответствие с пътната карта за оценката[23] **значимостта, въздействието, ефективността, ефикасността, съгласуваността и добавената стойност** на Агенцията с оглед на нейното функциониране, управление, вътрешна организационна структура и работни практики през периода 2013—2016 г. Основните констатации могат да бъдат обобщени, както следва (за повече информация вж. работния документ на службите на Комисията по темата, придружаващ оценката на въздействието).

- **Значимост:** Целите на ENISA доказаха своята значимост в контекста на технологичното развитие и променящите се заплахи, както и предвид значителната необходимост от повишаване на киберсигурността в ЕС. Действително, държавите членки и органите на ЕС разчитат на значителния експертен опит на Агенцията по въпросите на киберсигурността. Освен това в държавите членки трябва да се изгради капацитет за по-добро разбиране на заплахите и съответно реагиране, а заинтересованите страни трябва да си

[22] Заключения на Съвета относно укрепването на отбранителната способност на Европа срещу кибератаки и изграждането на конкурентен и иновативен сектор на киберсигурността – 15 ноември 2016 г.

[23] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

сътрудничат отвъд границите на конкретни тематични области и конкретни институции. Киберсигурността продължава да бъде основен политически приоритет на ЕС, по който се очаква ENISA да даде отговор. Обаче структурата на ENISA като агенция на ЕС с мандат за ограничен срок: i) не дава възможност за дългосрочно планиране и трайна подкрепа за държавите членки и институциите на ЕС; ii) може да доведе до правен вакуум, тъй като разпоредбите на Директивата за МИС, с които се възлагат задачи на ENISA, са с постоянен характер[24]; iii) не е съвместима с идеята за свързване на ENISA с една усъвършенствана екосистема на киберсигурността в ЕС.

- **Ефективност**: Като цяло ENISA постигна целите си и изпълни задачите си. Тя допринесе за повишаването на мрежовата и информационната сигурност в Европа чрез своите основни дейности (изграждане на капацитет, предоставяне на експертен опит, изграждане на общности и подкрепа на политики). Във всяка от тези дейности обаче пролича потенциал за подобрение. В оценката се прави заключението, че ENISA ефективно е изградила стабилни отношения на доверие с някои от заинтересованите страни, по-специално с държавите членки и общността на CSIRT. Смята се, че намесите ѝ в областта на изграждането на капацитет са били ефективни, по-специално за държавите членки с по-малко ресурси. Насърчаването на широкото сътрудничество е един от основните акценти в дейността на ENISA, като заинтересованите страни в голяма степен споделят мнението, че тя играе положителна роля при изграждането на контакти с цел сътрудничество. ENISA обаче изпитва трудности да увеличи своето влияние в областта на мрежовата и информационната сигурност. Това се дължи също и на факта, че тя трябва да изпълнява мандат със значителен обхват с доста ограничени човешки и финансови ресурси. Също така, при оценката бе направено заключението, че ENISA е постигнала целта за осигуряване на експертен опит частично, което се отдава на трудностите при набирането на експерти (вж. също раздела за ефикасността по-долу).
- **Ефикасност**: Въпреки малкия си бюджет — един от най-ниските сред агенциите на ЕС — Агенцията успя да даде своя принос за постигането на поставените цели, като демонстрира като цяло ефикасно използване на ресурсите си. В оценката се прави заключението, че процесите като цяло са били ефикасни, а ясното разграничаване на отговорностите в рамките на организацията е довело до доброто изпълнение на задачите. Едно от основните предизвикателства по отношение на ефективността на Агенцията е свързано с трудностите на ENISA при набирането и задържането на висококвалифицирани експерти. Констатациите показват, че това може да се обясни с комбинация от фактори, включително с общите трудности на публичния сектор да се пребори с конкуренцията на частния сектор за привличането на високоспециализирани експерти, с вида договори (срочни), които Агенцията бе в състояние да предложи в повечето случаи, и най-вече със сравнително ниската степен на привлекателност на местоположението на ENISA, дължаща се например на трудностите, които срещат съпрузите на служителите при намирането на работа. Разделянето на Агенцията между Атина и Ираклион изискваше допълнителни усилия за координация и доведе до допълнителни разходи, но

[24] Позоваване на членове 7, 9, 11, 12 и 19 от директивата относно сигурността на мрежите и информационните системи (Директива за МИС).

преместването на основните дейности в Атина през 2013 г. повиши оперативната ефективност на Агенцията.

- **Съгласуваност**: Дейностите на ENISA като цяло бяха съгласувани с политиките и дейностите на заинтересованите страни на национално равнище и на равнище ЕС, но съществува необходимост от по-координиран подход по отношение на киберсигурността на равнище ЕС. Потенциалът за сътрудничество между ENISA и други органи на ЕС не беше напълно изчерпан. С развитието на правните и политически условия в ЕС обаче съгласуваността на настоящия мандат започва да намалява.

- **Добавена стойност за ЕС**: Добавената стойност на ENISA се състои предимно в способността на Агенцията да подобрява сътрудничеството, основно между държавите членки, но също и между общностите в областта на мрежовата и информационната сигурност. Няма друг участник на равнище ЕС, който да подкрепя сътрудничеството между толкова различни заинтересовани страни в областта на мрежовата и информационната сигурност. Добавената от Агенцията стойност бе различна и зависеше от различните потребности и ресурси на нейните заинтересовани страни (напр. големи срещу малки държави членки; държави членки срещу промишлеността), както и от необходимостта Агенцията да съобразява дейностите си с приоритетите на своята работна програма. В оценката се прави заключението, че евентуално закриване на ENISA би било пропусната възможност за всички държави членки. Няма да бъде възможно да се гарантира същата степен на изграждане на общности и на сътрудничеството между държавите членки в областта на киберсигурността. Без по-централизирана агенция на ЕС картината би била още по-разпокъсана, като празнотата, оставена от ENISA, ще бъде запълнена от двустранно и регионално сътрудничество.

Що се отнася конкретно до извършената работа и до бъдещето на ENISA, основните тенденции, произтичащи от консултацията през 2017 г., са следните[25]:

- Цялостното функциониране на ENISA през периода 2013—2016 г. бе оценено положително от по-голямата част от отговорилите (74 %). Повечето от отговорилите също така считат, че ENISA постига различните поставени ѝ цели (най-малко 63 % за всяка от целите). Услугите и продуктите на ENISA се ползват редовно (веднъж месечно или по-често) от почти половината от отговорилите (46 %) и се ценят поради факта, че са предоставени от орган на равнище ЕС (83 %), както и заради качеството им (62 %).

- Отговорилите посочиха редица пропуски и предизвикателства за бъдещето на киберсигурността в ЕС, като петте най-често посочвани (от общо 16) бяха: сътрудничество между държавите членки; капацитет за предотвратяване,

[25] 90 заинтересовани страни от 19 държави членки отговориха на консултацията (88 отговора и 2 документа за изразяване на позиция), в това число национални органи от 15 държави членки, включително от Франция, Италия, Ирландия и Гърция, и 8 обединения, представляващи значителен брой европейски организации, например Европейската банкова федерация, организацията „Digital Europe“ (представляваща производителите на цифрови технологии в Европа), Асоциацията на европейските оператори на телекомуникационни мрежи (ETNO). Обществената консултация за ENISA бе допълнена от редица други източници, включително: i) задълбочени интервюта с около 50 основни участници в сектора на киберсигурността; ii) проучване на мрежата на CSIRT; iii) проучване на управителния съвет, изпълнителния съвет и Постоянната група на заинтересовани страни на ENISA.

откриване и отблъскване на широкомащабни кибератаки; сътрудничество между държавите членки по въпроси, свързани с киберсигурността; сътрудничество и обмен на информация между различните заинтересовани страни, включително сътрудничеството между публичния и частния сектор; защита на критичната инфраструктура от кибератаки.

- Голямо мнозинство от отговорилите (88 %) счита, че инструментите и механизмите, които понастоящем са на разположение на равнището на ЕС, са недостатъчни или само частично адекватни за преодоляването на гореизброените предизвикателства. Голямо мнозинство от отговорилите (98 %) посочва, че отговор на тези потребности трябва да бъде даден от орган на ЕС, като 99 % от тях считат, че подходящата за целта организация е ENISA.

Консултации със заинтересованите страни

- По повод прегледа на ENISA Комисията организира обществена консултация в периода между 12 април и 5 юли 2016 г. и получи 421 отговора[26]. Според нейните резултати 67,5 % от отговорилите са на мнение, че ENISA може да има роля при създаването на хармонизирана рамка за сертифициране на сигурността на ИКТ продукти и услуги.

Резултатите в раздела за сертифицирането на проведената през 2016 г. консултация относно киберсигурността сРРР[27] показват, че:

- 50,4 % (121 от 240) от отговорилите не знаят дали националните схеми за сертифициране се признават взаимно в отделните държави — членки на ЕС. 25,8 % (62 от 240) са отговорили с „не“, докато 23,8 % (57 от 240) са отговорили с „да“.
- 37,9 % от отговорилите (91 от 240) смятат, че съществуващите схеми за сертифициране не задоволяват потребностите на европейската промишленост. От друга страна, 17,5 % от отговорилите (42 от 240) — предимно действащи глобално предприятия, които осъществяват дейност на европейския пазар, са на противоположното мнение.
- 49,6 % (119 от 240) от отговорилите заявяват, че не е лесно да се докаже еквивалентност между стандарти, схеми за сертифициране и етикети. 37,9 % (91 от 240) са отговорили с „не зная“, докато 12,5 % (30 от 240) са отговорили с „да“.

Събиране и използване на експертен опит

Комисията е използвала следните становища на външни експерти:

---

[26] 162 предложения и коментари от граждани, 33 — от организации на гражданското общество и организации на потребителите; 186 — от промишлеността и 40 — от публични органи, включително компетентните органи за прилагане на Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

[27] 240 заинтересовани страни от националните публични администрации, големите предприятия, МСП, микропредприятията и научноизследователските организации са отговорили на въпросите в раздела за сертифицирането.

- Проучване относно оценката на ENISA (Ramboll/Carsa 2017; SMART № 2016/0077),
- Проучване относно сертифицирането на сигурността и етикетирането на ИКТ — Събиране на доказателства и оценка на въздействието (PriceWaterhouseCoopers 2017; SMART № 2016/0029).

Оценка на въздействието

- В доклада за оценката на въздействието на настоящата инициатива са набелязани следните основни проблеми, които трябва да бъдат решени:
- разпокъсаност на политиките и подходите към киберсигурността в различните държави членки;
- разпръснати ресурси и разпокъсаност на подходите към киберсигурността в различните институции, агенции и органи на ЕС; и
- недостатъчна осведоменост и информираност на гражданите и предприятията, както и нарастване на броя на новосъздадените национални и секторни схеми за сертифициране.

В доклада бяха разгледани следните варианти по отношение на мандата на ENISA:

- запазване на статуквото, т.е. разширяване на мандата, но все още за ограничен срок (базов вариант);
- неподновяване на сегашния мандат на ENISA след изтичането му и закриване на ENISA (без политическа намеса);
- реформиране на ENISA; и
- създаване на агенция на ЕС за кирберсигурност с пълна оперативна способност.

В доклада бяха разгледани следните варианти по отношение на сертифицирането на киберсигурността:

- без политическа намеса (базов вариант);
- незаконодателни мерки (актове с незадължителна юридическа сила);
- законодателен акт на ЕС за създаване на задължителна система за всички държави членки въз основа на системата SOG-IS; и
- обща рамка на ЕС за сертифициране на киберсигурността в сектора на ИКТ.

Анализът доведе до заключението, че предпочитаният вариант е реформирането на ENISA в съчетание със създаването на обща рамка на ЕС за сертифициране на киберсигурността в сектора на ИКТ.

Предпочитаният вариант се смята за най-ефективен за ЕС за постигането на набелязаните цели, а именно: подобряване на способностите, подготвеността, сътрудничеството, осведомеността и прозрачността в областта на киберсигурността, както и избягване на разпокъсаността на пазара. Смята се също, че той е най-добре съгласуван с политическите приоритети на стратегията на ЕС за киберсигурност и свързаните с нея политики (например Директивата за МИС), както и със стратегията за цифровия единен пазар. В допълнение, процесът на консултации показа, че

предпочитаният вариант се ползва с подкрепата на мнозинството от заинтересованите страни. Освен това анализът, направен в рамките на оценката на въздействието, показа, че при предпочитания вариант целите ще бъдат постигнати чрез разумно използване на ресурси.

Първоначалното Комитетът за регулаторен контрол към Комисията издаде отрицателно становище на 24 юли, което беше последвано от второ, положително, на 25 август 2017 г., след повторното подаване на заявлението. В изменения доклад за оценка на въздействието бяха включени допълнителни подкрепящи доказателства, окончателните заключения от оценката на ENISA и допълнителни обяснения относно вариантите на политиката и тяхното въздействие. В приложение 1 към окончателния доклад за оценка на въздействието е обобщено по какъв начин са взети предвид коментарите на комитета от второто му становище. По-специално, в актуализирания доклад беше представен в повече подробности контекстът на киберсигурността в ЕС, като бяха включени мерките, изброени в съвместното съобщение „Устойчивост, възпиране и отбрана: изграждане на устойчива киберсигурност за ЕС“, (JOIN(2017) 450) и имащи специално значение за ENISA: концепцията на ЕС за киберсигурността и Европейският експертен център за научни изследвания в областта на киберсигурността, които ще бъдат в основата на инструкциите на Агенцията относно потребностите от научни изследвания в ЕС.

В доклада се разяснява как реформата на Агенцията, включително новите задачи, по-добрите условия на работа и структурното сътрудничество с органите на ЕС в тази област, ще повиши нейната привлекателност като работодател и ще спомогне за решаването на проблемите, свързани с набирането на експерти. В приложение 6 към доклада е представена също така преразгледана оценка на разходите, свързани с вариантите на политиката за ENISA. Що се отнася до сертифицирането, докладът бе преработен, така че да включва по-подробно обяснение, включително графично представяне, на предпочитания вариант, и да предоставя оценки за разходите на държавите членки и на Комисията във връзка с новата рамка за сертифициране. Разяснява се допълнително причината за избора на ENISA като основен фактор в контекста на рамката, като се посочва нейният експертен опит в тази област и фактът, че тя е единствената агенция на равнището на ЕС в областта на киберсигурността. Освен това са преработени разделите за сертифицирането, с цел да се изяснят аспектите, свързани с разликите спрямо настоящата система SOG-IS, ползите, свързани с различните варианти на политиката, както и с цел да се обясни фактът, че видът на обхванатите от дадена европейска схема за сертифициране ИКТ продукти и услуги ще бъде определян в самата одобрена схема.

Пригодност и опростяване на законодателството

Не е приложимо

Въздействие върху основните права

Киберсигурността играе съществена роля за защитата на неприкосновеността на личния живот и личните данни на гражданите в съответствие с членове 7 и 8 от Хартата на основните права на ЕС. В случай на киберинциденти неприкосновеността на личния ни живот и нашите лични данни очевидно са изложени на опасност. Поради това киберсигурността е необходимо условие, за да бъдат зачитани неприкосновеността на

личния ни живот и поверителността на личните ни данни. От тази гледна точка, като допринася за укрепването на киберсигурността в Европа, предложението се явява важно допълнение към съществуващото законодателство за защита на основното право на неприкосновеност на личния живот и личните данни. Киберсигурността е от съществено значение и за опазването на поверителността на нашите електронни съобщения и следователно за упражняването на правото на свободно мнение и на информация, както и на други свързани права като правото на свобода на мисълта, съвестта и религията.

4. ОТРАЖЕНИЕ ВЪРХУ БЮДЖЕТА

Вж. финансовия фиш

5. ДРУГИ ЕЛЕМЕНТИ

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

Комисията ще наблюдава прилагането на регламента и ще представя доклад с оценката си на Европейския парламент, на Съвета и на Европейския икономически и социален комитет на всеки пет години. Тези доклади ще бъдат публично достъпни и ще разглеждат подробно ефективното изпълнение и правоприлагане на настоящия регламент.

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

Дял I от регламента съдържа общите разпоредби: предмета (член 1) и определенията (член 2), включително препратки към съответни определения от други инструменти на ЕС, като например Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (Директива за МИС), Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета за определяне на изискванията за акредитация и надзор на пазара във връзка с предлагането на пазара на продукти и за отмяна на Регламент (ЕИО) № 339/93, както и Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета относно европейската стандартизация.

Дял II от регламента съдържа основните разпоредби във връзка с ENISA — агенцията на ЕС за киберсигурност.

В глава I от този дял се описват мандатът (член 3), целите (член 4) и задачите на Агенцията (членове 5—11).

В глава II се описва организацията на ENISA и се посочват основните разпоредби относно нейната структура (член 12). В нея се разглеждат съставът, правилата за гласуване и функциите на управителния съвет (раздел 1, членове 13—17), на изпълнителния съвет (раздел 2, член 18) и на изпълнителния директор (раздел 3, член 19). Тя включва също така разпоредби относно състава и ролята на Постоянната група на заинтересованите страни (раздел 4, член 20). Също така, раздел 5 от тази глава съдържа подробно описание на оперативните правила на Агенцията, включително по отношение на планирането на нейните действия, конфликтите на интереси, прозрачността, поверителността и публичния достъп до документи (членове 21—25).

В глава III се разглеждат установяването и структурата на бюджета на Агенцията (членове 26 и 27), както и правилата, ръководещи неговото изпълнение (членове 28 и 29). В нея са включени и разпоредбите, подпомагащи борбата с измамите, корупцията и други незаконни дейности (член 30).

В глава IV се разглеждат въпроси във връзка с персонала на Агенцията. Тя съдържа общи разпоредби относно Правилника за длъжностните лица и Условията за работа на другите служители и правилата относно привилегиите и имунитета (членове 31 и 32). В нея се описват подробно и правилата за избиране и назначаване на изпълнителния директор на агенцията (член 33). Освен това тя включва разпоредби, ръководещи използването на командировани национални експерти или друг персонал, който не е нает от Агенцията (член 34).

И накрая, в глава V се съдържат общите разпоредби във връзка с Агенцията. В нея е описан правният статут (член 35) и са включени разпоредби, уреждащи въпросите за отговорността, езиковия режим, защитата на личните данни (членове 36—38), както и правила за сигурност относно защитата на класифицирана информация и некласифицирана чувствителна информация (член 40). В нея са описани също правилата за сътрудничеството на Агенцията с трети държави и международни организации (член 39). Освен това тя съдържа също разпоредби относно седалището на Агенцията и условията на работа, както и относно административния контрол от страна на Европейския омбудсман (членове 41 и 42).

С дял III от регламента се създава Европейска рамка на сертифициране на киберсигурността за ИКТ продукти и услуги („**Рамката**“) като *lex generalis* (член 1). В същия дял се определя общата цел на европейските схеми за сертифициране на киберсигурността, т.е. да се гарантира, че ИКТ продуктите и услугите отговарят на специалните изисквания за киберсигурност по отношение на способността им да устояват — при дадено ниво на обезпеченост — на действия, нарушаващи наличността, автентичността, целостта или поверителността на съхранявани, предавани или обработвани данни, на свързаните с тях функции, или на услуги (член 43). Освен това в посочения дял са изброени целите в областта на сигурността, които трябва да бъдат постигнати чрез европейските схеми за сертифициране на киберсигурността (член 45), като например способността да бъдат защитени данните от случаен или неправомерен достъп или разкриване, промяна или унищожаване, и е описано съдържанието (т.е. елементите) на европейските схеми за сертифициране на киберсигурността, например подробно описание на техния обхват, техните цели, критерии за оценка и т.н. (член 47).

В дял III се определят също основните правни последици на европейските схеми за сертифициране на киберсигурността, а именно i) задължението за прилагане на схемата на национално равнище и доброволният характер на сертифицирането; ii) автоматичното анулиране на националните схеми при наличието на европейски схеми за сертифициране на киберсигурността за същите продукти или услуги (членове 48 и 49).

В същия дял се определят процедурата за приемане на европейски схеми за сертифициране на киберсигурността и съответните роли на Комисията, ENISA и Европейската група по сертифициране на киберсигурността — „групата“ (член 44). И накрая, същият този дял съдържа разпоредби във връзка с регулирането на органите за оценяване на съответствието, включително изискванията към тях, техните правомощия и задачи, националните надзорни органи за сертифицирането, както и санкции.

В същия дял се създава и горепосочената група като важен орган, състоящ се от представители на националните надзорни органи за сертифицирането, чиято основна функция е да работи заедно с ENISA за изготвянето на европейските схеми за сертифициране на киберсигурността и да съветва Комисията по общи или специфични въпроси, свързани с политиката за сертифициране на киберсигурността.

Дял IV от регламента съдържа заключителните разпоредби, които описват упражняването на делегиране, изискванията за оценяване, отмяната и правоприемството, както и влизането в сила.

2017/0225 (COD)

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно ENISA — Агенцията на ЕС за киберсигурност, и за отмяна на Регламент (ЕС) № 526/2013, както и относно сертифицирането на киберсигурността на информационните и комуникационните технологии („Акт за киберсигурността“)

(текст от значение за ЕИП)

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз, и по-специално член 114 от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейския икономически и социален комитет[28],

като взеха предвид становището на Комитета на регионите[29],

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

(1) Мрежовите и информационните системи и далекосъобщителните мрежи и услуги играят жизненоважна роля за обществото и са се превърнали в основата на икономическия растеж. Информационните и комуникационните технологии са в основата на сложните системи, които поддържат обществената активност, правят възможно функционирането на нашите икономики в основни сектори като здравеопазване, енергетика, финанси и транспорт, и по-специално поддържат функционирането на вътрешния пазар.

(2) Използването на мрежовите и информационните системи от гражданите, предприятията и правителствата в целия Европейския съюз е вече повсеместно. Цифровизацията и свързаността се превръщат в основни характеристики на все по-голям брой продукти и услуги и с навлизането на „интернет на нещата“ се очаква на територията на ЕС през следващото десетилетие да има милиони, дори милиарди, свързани цифрови устройства. Въпреки нарастващия брой на устройствата, свързани към интернет, вграждането на сигурност и устойчивост в тях „още при проектирането“ все още не се извършва в задоволителен мащаб, което води до недостатъчно ниво на киберсигурността. В този контекст, ограниченото използване на сертифицирането води до недостиг на информация за потребителите (организации и частни лица) относно характеристиките на ИКТ продукти и услуги в областта на киберсигурността, като подкопава доверието в цифровите решения.

[28] ОВ С […], […] г., стр. […].
[29] ОВ С […], […] г., стр. […].

(3) Нарастването на цифровизацията и свързаността доведе до увеличаване на рисковете, свързани с киберсигурността, като по този начин обществото като цяло стана по-уязвимо за киберзаплахи и се изостриха опасностите за физически лица, включително уязвими лица, като например деца. С цел да се смекчи този риск за обществото, трябва да бъдат предприети всички необходими действия за подобряване на киберсигурността в ЕС, за по-добра защита срещу киберзаплахи на мрежовите и информационните системи, далекосъобщителните мрежи, цифровите продукти, услуги и устройства, използвани от гражданите, правителствата и предприятията — от МСП до операторите на критични инфраструктури.

(4) Броят на кибератаките нараства, а икономиката и обществото, които са свързани с интернет, са по-уязвими за киберзаплахи и кибератаки и имат нужда от засилени защитни механизми. Независимо от факта обаче, че кибератаките често са трансгранични, политическият отговор на органите по киберсигурността и правоприлагащите правомощия са основно национални. Широкомащабните киберинциденти могат да нарушат предоставянето на важни услуги в целия ЕС. Това изисква ефективен отговор и ефективно управление на кризи на равнището на ЕС, които да се основават на специални политики и по-широкообхватни инструменти за европейска солидарност и взаимопомощ. Освен това редовното оценяване на състоянието на киберсигурността и устойчивостта в Съюза въз основа на надеждни данни на Съюза, както и систематичното прогнозиране на бъдещи развития, предизвикателства и заплахи както на равнище на Съюза, така и на световно равнище, е важно за разработчиците на политики, за промишлеността и потребителите.

(5) В светлината на предизвикателствата, пред които е изправен Съюзът в областта на киберсигурността, е необходим всеобхватен набор от мерки, който ще се основава на предходни действия на Съюза и ще насърчава взаимно подкрепящите се цели. Това включва необходимостта от допълнително подобряване на способностите и подготвеността на държавите членки и на предприятията, както и от подобряване на сътрудничеството и координацията между държавите членки и институциите, агенциите и органите на ЕС. Освен това, предвид трансграничния характер на киберзаплахите е необходимо да се доразвият способностите на равнището на Съюза, чрез които могат да се допълват действията на държавите членки, по-специално в случаите на мащабни трансгранични киберинциденти и киберкризи. Също така са необходими допълнителни усилия, за да се повиши информираността на гражданите и на предприятията по въпроси, свързани с киберсигурността. Освен това доверието в цифровия единен пазар следва да бъде допълнително подобрено, като се предоставя прозрачна информация за нивото на сигурност на ИКТ продукти и услуги. Това може да бъде улеснено чрез сертифициране на равнище ЕС, като се предоставят общи изисквания относно киберсигурността и общи критерии за оценка, независещи от националните пазари и секторите.

(6) През 2004 г. Европейският парламент и Съветът приеха Регламент (ЕО) № 460/2004[30] относно създаването на ENISA, предназначен да подпомогне целите за осигуряване на високо ниво на мрежова и информационна сигурност в

[30] Регламент (ЕО) № 460/2004 на Европейския парламент и на Съвета от 10 март 2004 г. относно създаване на Европейската агенция за мрежова и информационна сигурност (ОВ L 77, 13.3.2004 г., стр. 1).

рамките на Съюза и създаване на култура на мрежова и информационна сигурност в полза на гражданите, потребителите, предприятията и държавните администрации. През 2008 г. Европейският парламент и Съветът приеха Регламент (ЕО) № 1007/2008[31] за удължаване на мандата на Агенцията до март 2012 г. С Регламент (ЕС) № 580/2011[32] мандатът на Агенцията беше удължен допълнително до 13 септември 2013 г. През 2013 г. Европейският парламент и Съветът приеха Регламент (ЕС) № 526/2013[33] относно ENISA и за отмяна на Регламент (ЕО) № 460/2004, с който мандатът на Агенцията беше удължен до юни 2020 г.

(7) Съюзът вече предприе важни стъпки за гарантиране на киберсигурността и за повишаване на доверието в цифровите технологии. През 2013 г. беше приета стратегия на ЕС за киберсигурност, която да направлява политиката на Съюза в отговор на заплахите и рисковете в областта на киберсигурността. В усилията си да защити по-добре европейските граждани в онлайн средата, през 2016 г. Съюзът прие първия законодателен акт в областта на киберсигурността — Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза („Директива за МИС“). С Директивата за МИС бяха въведени изисквания по отношение на националните способности в областта на киберсигурността, бяха създадени първите механизми за засилване на стратегическото и оперативното сътрудничество между държавите членки и бяха въведени задължения относно мерките за сигурност и уведомяването за инциденти отвъд границите на отделните сектори, които са жизненоважни за икономиката и обществото, като например енергетиката, транспорта, водните ресурси, банковото дело, инфраструктурите на финансовия пазар, здравеопазването, цифровата инфраструктура, както и доставчиците на основни цифрови услуги (интернет търсачки, услуги за изчисления в облак и платформи за онлайн търговия). ENISA получи основна роля в областта на подпомагането на изпълнението на директивата. В допълнение, ефективна борба срещу киберпрестъпността е важен приоритет в Европейската програма за сигурност, като допринася за общата цел за постигане на високо равнище на киберсигурността.

(8) Отчита се, че след приемането на Стратегията на ЕС за киберсигурност от 2013 г. и след последното преразглеждане на мандата на Агенцията общият контекст на политиката се е променил значително, също и във връзка с по-нестабилната и по-несигурна глобална среда. В този смисъл и в рамките на новата политика в областта на киберсигурността на Съюза е необходимо да се направи преглед на мандата на ENISA, за да се определи нейната роля в променената екосистема на киберсигурността и да се гарантира нейният

---

31 Регламент (ЕО) № 1007/2008 на Европейския парламент и на Съвета от 24 септември 2008 г. за изменение на Регламент (ЕО) № 460/2004 относно създаване на Европейска агенция за мрежова и информационна сигурност по отношение на срока на съществуване на агенцията (ОВ L 293, 31.10.2008 г., стр. 1).

32 Регламент (ЕС) № 580/2011 на Европейския парламент и на Съвета от 8 юни 2011 г. за изменение на Регламент (ЕО) № 460/2004 относно създаване на Европейската агенция за мрежова и информационна сигурност по отношение на срока на съществуване на агенцията (ОВ L 165, 24.6.2011 г., стр. 3).

33 Регламент (ЕС) № 526/2013 на Европейския парламент и на Съвета от 21 май 2013 година относно Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) и за отмяна на Регламент (ЕО) № 460/2004 (ОВ L 165, 18.6.2013 г., стр. 41).

ефективен принос към борбата с предизвикателствата за киберсигурността в Съюза, произтичащи от тази коренно променена картина на заплахите, за които настоящият мандат не е достатъчен, както беше констатирано в оценката на Агенцията.

(9) Агенцията, която се създава с настоящия регламент, следва да бъде правоприемник на агенцията ENISA, създадена с Регламент (ЕС) № 526/2013. Агенцията следва да изпълнява задачите, възложени ѝ с настоящия регламент и правните актове на Съюза в областта на киберсигурността, като, наред с другото, предоставя експертен опит и консултации и действа като център на Съюза за информация и знания. Тя следва да насърчава обмена на добри практики между държавите членки и заинтересовани страни от частния сектор, да предоставя предложения за политики на Европейската комисия и държавите членки, да действа като отправна точка за секторни политически инициативи на Съюза по въпросите на киберсигурността, да насърчава оперативното сътрудничество между държавите членки, както и между тях и институциите, агенциите и органите на ЕС.

(10) В рамките на Решение № 2004/97/ЕО, Евратом, прието на заседанието на Европейския съвет на 13 декември 2003 г., представителите на държавите членки решиха, че седалището на ENISA ще бъде в град в Гърция, който ще бъде определен от гръцкото правителство. Приемащата Агенцията държава членка следва да осигури възможно най-добрите условия за безпроблемното и ефективно функциониране на Агенцията. За правилното и ефикасно изпълнение на задачите на Агенцията, за целите на набирането на персонал и задържането му и за подобряване на ефикасността на дейностите за осъществяване на връзки е наложително Агенцията да се установи в подходящо местоположение, което наред с другото да предоставя подходящи транспортни връзки и съоръжения за съпрузите и децата, придружаващи членовете на персонала на Агенцията. Необходимите разпоредби следва да бъдат определени в споразумение между Агенцията и приемащата държава членка, което се сключва след получаване на одобрението на управителния съвет на Агенцията.

(11) Като се има предвид нарастващият брой на предизвикателствата в областта на киберсигурността, пред които е изправен Съюзът, предоставените на Агенцията финансови и човешки ресурси следва да бъдат увеличени, така че да отразяват нейната разширена роля, нейните задачи, както и нейната ключова позиция в екосистемата на организациите, които защитават европейската цифрова екосистема.

(12) Агенцията следва да постигне и запази високо равнище на експертен опит и да функционира като отправна точка, създавайки условия за увереност и доверие в единния пазар благодарение на своята независимост, качеството на предоставяните от нея консултации и разпространяваната от нея информация, на прозрачността на своите процедури и методи на работа, както и на добросъвестното изпълнение на възложените ѝ задачи. Агенцията следва да дава активен принос към усилията на национално равнище и на равнището на Съюза, като същевременно изпълнява своите задачи в пълно сътрудничество с институциите, органите, службите и агенциите на Съюза, както и с държавите членки. Освен това работата на Агенцията следва да се основава на приноса и на сътрудничеството с частния сектор и с други заинтересовани страни. В набор от задачи следва да се формулира как Агенцията трябва да постига своите цели и същевременно да ѝ се предоставя възможност за гъвкаво функциониране.

(13) Агенцията следва да подпомага Комисията чрез консултации, становища и анализи по всички въпроси на Съюза, свързани с разработването, актуализирането и преразглеждането на политиката и законодателството в областта на киберсигурността, включително защитата на критичната инфраструктура и киберустойчивостта. Агенцията следва да служи като отправна точка за консултации и експертен опит за специфичните секторни политики и правни инициативи на Съюза, когато те включват въпроси, свързани с киберсигурността.

(14) Основната задача на Агенцията е да насърчава последователното прилагане на съответната правна рамка, по-конкретно на ефективното изпълнение на Директивата за МИС, която е от съществено значение за повишаване на киберустойчивостта. С оглед на бързо развиващата се картина на заплахите за киберсигурността е ясно, че държавите членки трябва да бъдат подкрепяни чрез по-широкообхватен подход, надхвърлящ границите на отделните политики, за изграждането на киберустойчивост.

(15) Агенцията следва да подпомага държавите членки и институциите, органите, службите и агенциите на Съюза в усилията им да изградят и подобрят способностите си и подготвеността си за предотвратяване, откриване и реагиране на проблеми и инциденти в областта на киберсигурността, както и във връзка със сигурността на мрежовите и информационните системи. По-специално, Агенцията следва да подкрепя развитието и укрепването на националните екипи CSIRT с оглед постигане на високо общо равнище на тяхната зрелост в Съюза. Агенцията следва също да съдейства за разработването и актуализирането стратегиите на Съюза и държавите членки относно сигурността на мрежовите и информационните системи, по-специално в областта на киберсигурността, да насърчава тяхното разпространение и да следи напредъка при изпълнението им. Също така, Агенцията следва да предлага обучения и образователни материали за публичните органи и, когато е целесъобразно, да „обучава обучаващите“, с цел да подпомогне държавите членки при развитието на техни собствени способности за обучение.

(16) Агенцията следва да подпомага групата за сътрудничество, създадена с Директивата за МИС, в изпълнението на нейните задачи, по-специално чрез предоставяне на експертен опит и консултации, и да улеснява обмена на най-добри практики, по-специално по отношение на определянето на операторите на основни услуги от държавите членки, включително по отношение на трансграничната зависимост във връзка с рисковете и инцидентите.

(17) С оглед на насърчаването на сътрудничеството между обществения и частния сектор и в рамките на частния сектор, по-специално с цел да се подкрепи защитата на критичните инфраструктури, Агенцията следва да улеснява създаването на секторни центрове за споделяне и анализ на информация (ISAC) чрез предоставянето на най-добри практики и насоки относно наличните инструменти и процедури, както и да предоставя насоки как да се работи с регулаторни въпроси, свързани с обмена на информация.

(18) Агенцията следва да обобщава и анализира националните доклади от CSIRT и CERT-EU, въвеждащи общи правила, език и терминология за обмен на информация. Агенцията следва също така да включи частния сектор, в рамките на Директивата за МИС, с която бяха положени основите за доброволен обмен

на техническа информация на оперативно равнище, като бе създадена мрежата на CSIRT.

(19) Агенцията следва да допринася за реакцията на равнището на ЕС в случай на мащабни трансгранични инциденти и кризи в областта на киберсигурността. Тази функция следва да включва събирането на съответна информация и поемането на ролята на посредник между мрежата на CSIRT, техническата общност и отговорните за вземане на решения лица, натоварени с управлението на кризи. Освен това на Агенцията би могла да спомогне за справянето с инциденти в технически аспект, като улесни съответния технически обмен на решения между държавите членки и даде своя принос за публичното осведомяване. Агенцията следва да подкрепя процеса, като проверява как функционира това сътрудничество чрез ежегодни учения в областта на киберсигурността.

(20) За изпълнението на оперативните си задачи Агенцията следва да използва наличния експертен опит на CERT-EU чрез структурирано сътрудничество в непосредствена географска близост. Структурираното сътрудничество ще улесни възникването на необходимите полезни взаимодействия и натрупването на експертен опит в ENISA. При необходимост следва да бъдат сключени специални договорености между двете организации, за да се определи практическото изражение на такова едно сътрудничество.

(21) В съответствие с оперативните си задачи, Агенцията следва да е в състояние да оказва подкрепа на държавите членки, например като предоставя консултации или техническа помощ или като осигурява анализи на заплахите и инцидентите. В препоръката на Комисията за координирана реакция при мащабни инциденти и кризи в областта на киберсигурността се препоръчва държавите членки да си сътрудничат добросъвестно и да обменят информация помежду си и с ENISA относно мащабни инциденти и кризи в областта на киберсигурността без излишно забавяне. Тази информация ще помогне допълнително на ENISA при изпълнението на нейните оперативни задачи.

(22) Като част от редовното сътрудничество на техническо равнище за подпомагане на ситуационната осведоменост на Съюза, Агенцията следва редовно да изготвя технически доклади за състоянието на киберсигурността в ЕС във връзка с инциденти и заплахи въз основа на публично достъпна информация, свои собствени анализи, както и доклади, подадени (доброволно) от CSIRT на държавите членки или от единните звена за контакт съгласно Директивата за МИС, Европейския център за борба с киберпрестъпността към Европол (EC3 към Европол), CERT-EU, и когато е целесъобразно — от Центъра на ЕС за анализ на информация (INTCEN) към Европейската служба за външна дейност (ЕСВД). Докладите следва да се предоставят на съответните служби на Съвета, Комисията, върховния представител на Съюза по въпросите на външните работи и политиката на сигурност и мрежата на CSIRT.

(23) Последващите технически разследвания на инциденти със значително въздействие в повече от една държава членка, извършвани от Агенцията или с нейната подкрепа, по искане или със съгласието на заинтересованите държави членки, следва да бъдат насочени към предотвратяване на бъдещи инциденти и да се осъществяват, без това да засяга евентуални съдебни или административни производства за определяне на вина или отговорност.

(24) Засегнатите държави членки следва да предоставят необходимата информация и съдействие на Агенцията за целите на разследването, без това да засяга разпоредбите на член 346 от Договора за функционирането на Европейския съюз или други съображения във връзка с публичната политика.

(25) Държавите членки могат да приканят засегнати от инцидента предприятия да сътрудничат, като предоставят необходимата информация и съдействие на Агенцията, без да се накърнява правото им на защита на поверителната търговска информация.

(26) С оглед да се разберат по-добре предизвикателствата в областта на киберсигурността и да се предоставят стратегически дългосрочни препоръки на държавите членки и институциите на Съюза, Агенцията трябва да анализира текущите и нововъзникващи рискове. За тази цел Агенцията, в сътрудничество с държавите членки и, по целесъобразност, със статистически органи и други организации, следва да събира съответна информация, да извършва анализи на нововъзникващите технологии и да предоставя тематични оценки на очаквани социални, правни, икономически и регулаторни въздействия на дадени технологични иновации в областта на мрежовата и информационната сигурност, по-специално в областта на киберсигурността. Освен това Агенцията следва да подпомага държавите членки и институциите, агенциите и органите на Съюза при установяването на възникващите тенденции и предотвратяването на проблеми, свързани с киберсигурността, като извършва анализи на заплахите и инцидентите.

(27) С цел да се повиши киберустойчивостта на Съюза, Агенцията следва да развие върхов капацитет в областта на сигурността на инфраструктурата на интернет и на критичните инфраструктури, като предоставя съвети, насоки и най-добри практики. С оглед да се осигури по-лесен достъп до по-добре структурирана информация относно рисковете за киберсигурността и потенциалните средства за защита, Агенцията следва да разработи и поддържа „информационен център“ на Съюза — един вид портал за „обслужване на едно гише“, който осигурява на обществеността информация относно киберсигурността, получена от европейските и националните институции, агенции и органи.

(28) Агенцията следва да допринася за повишаването на обществената осведоменост относно рисковете, свързани с киберсигурността, и да предлага насоки и добри практики за отделните потребители, насочени към гражданите и организациите. Агенцията следва също така да допринася за насърчаване на най-добрите практики и решения на равнището на отделни лица и организации, като събира и анализира обществено достъпна информация относно значителни инциденти и изготвя доклади, с цел да се предоставят насоки за предприятията и гражданите и да се подобри цялостното ниво на подготвеност и устойчивост. Освен това Агенцията следва да организира, в сътрудничество с институциите, органите, службите и агенциите на Съюза и държавите членки, редовни разяснителни и обществени образователни кампании за крайните потребители, насочени към насърчаването на по-безопасно индивидуално поведение онлайн и повишаване на осведомеността относно потенциалните заплахи в киберпространството, включително относно киберпрестъпления като фишинг, ботмрежи, финансови и данъчни измами, а също така насочени към разпространението на основни съвети относно автентификацията и защитата на данните. Агенцията следва да играе централна роля за по-бързото осведомяване на крайните ползватели относно сигурността на изделията.

(29) За да се подпомогнат предприятията, извършващи дейност в сектора на киберсигурността, както и ползвателите на решения в областта на киберсигурността, Агенцията следва да разработи и поддържа „обсерватория на пазара“, като извършва редовни анализи и разпространява информация за основните тенденции на пазара на киберсигурността, както по отношение на търсенето, така и по отношение на предлагането.

(30) С цел да се гарантира, че Агенцията ще постигне напълно своите цели, тя следва да си сътрудничи със съответните институции, агенции и органи, в това число CERT-EU, Европейския център за борба с киберпрестъпността към Европол (EC3 към Европол), Европейската агенция по отбрана (EDA), Европейската агенция за оперативното управление на широкомащабни информационни системи (eu-LISA), Европейската агенция за авиационна безопасност (ЕААБ) и всяка друга агенция на ЕС, която действа в областта на киберсигурността. Тя следва също така да поддържа връзка с органите, които работят в областта на защитата на данните, с цел да обменя с тях ноу-хау и най-добри практики и да предоставя консултации относно аспекти на киберсигурността, които биха могли да окажат влияние върху тяхната работа. Правоприлагащите органи на национално равнище и на равнището на Съюза и органите за защита на данните следва да имат правото да бъдат представлявани в Постоянната група на заинтересованите страни на Агенцията. При сътрудничеството си с правоприлагащите органи по въпроси на мрежовата и информационната сигурност, които биха могли да окажат влияние върху тяхната работа, Агенцията следва да спазва съществуващите информационни канали и изградени мрежи.

(31) Агенцията, като член на мрежата на CSIRT, който наред с другото осигурява секретариата на мрежата, следва да подкрепя екипите CSIRT на държавите членки и екипите CERT-EU при оперативното сътрудничество в допълнение към всички съответни задачи на мрежата на CSIRT, както е определено в Директивата за МИС. Наред с това Агенцията следва да насърчава и подкрепя сътрудничеството между съответните екипи CSIRT в случай на инциденти, атаки или нарушения в работата на мрежите или инфраструктурата, управлявани или защитавани от екипите CSIRT, които включват, действително или потенциално, най-малко два екипа CERT, като същевременно взема предвид надлежно стандартните оперативни процедури на мрежата на CSIRT.

(32) С оглед повишаване на подготвеността на Съюза за реагиране на киберинциденти, Агенцията следва да организира ежегодни учения в областта на киберсигурността на равнището на Съюза и да помага на държавите членки и на институциите, агенциите и органите на ЕС, по тяхно искане, при организирането на учения.

(33) Агенцията следва да продължава да развива и поддържа своя експертен опит в областта на сертифицирането на киберсигурността, с цел да подпомага политиките на Съюза в тази област. Агенцията следва да насърчава внедряването на сертифицирането на киберсигурността, включително като допринася за създаването и поддържането на мрежа за сертифициране на киберсигурността на равнище ЕС, с цел повишаване на прозрачността при обезпечаването на ИКТ продукти и услуги и, в крайна сметка, укрепване на доверието в цифровия вътрешен пазар.

(34) Ефективните политики за киберсигурност следва да се основават на добре разработени методи за оценяване на риска както в публичния, така и в частния сектор. Методите за оценка на риска се използват на различни нива, без да има обща практика относно най-добрия начин за тяхното ефикасно прилагане. Популяризирането и развитието на най-добри практики за оценяване на риска и за оперативно съвместими решения за управление на риска в организациите от публичния и частния сектор ще повиши нивото на киберсигурността в Съюза. За целта Агенцията следва да подкрепя сътрудничеството между заинтересовани страни на равнището на Съюза, като улеснява техните усилия, свързани с въвеждането и използването на европейски и международни стандарти за управление на риска и за измерима сигурност на електронните продукти, системи, мрежи и услуги, които заедно със софтуера са елементите, образуващи мрежовите и информационните системи.

(35) Агенцията следва да насърчава държавите членки и доставчиците на услуги да повишават общите си стандарти за сигурност, така че всички потребители на интернет да вземат необходимите мерки за гарантиране на собствената си киберсигурност. По-специално, доставчиците на услуги и създателите на продукти следва да оттеглят или рециклират продукти и услуги, които не отговарят на стандартите за киберсигурност. В сътрудничество с компетентните органи, ENISA може да разпространява информация относно равнището на киберсигурността на продуктите и услугите, предлагани на вътрешния пазар, и да отправя предупреждения по отношение на доставчиците и производителите и да изисква от тях да подобрят сигурността, включително киберсигурността, на своите продукти и услуги.

(36) Агенцията следва да взема под внимание в пълна степен текущата научноизследователска и развойна дейност и дейностите за оценка на технологиите, по-специално тези, провеждани от различните научноизследователски инициативи на Съюза, за да съветва институциите, органите, службите и агенциите на Съюза и, когато е необходимо, държавите членки, по тяхно искане, относно необходимостта от научни изследвания в областта на мрежовата и информационната сигурност, по-специално в областта на киберсигурността.

(37) Проблемите на киберсигурността са глобални. Необходимо е по-тясно международно сътрудничество с цел подобряване на стандартите за сигурност, включително определяне на общи норми за поведение, обмен на информация, насърчаване на по-бързи форми на международно сътрудничество при реагиране на проблеми на мрежовата и информационната сигурност, както и общ глобален подход към такива проблеми. За тази цел Агенцията следва да подкрепя по-задълбоченото ангажиране на Съюза и сътрудничеството с трети държави и международни организации, като предоставя, където е уместно, необходимия експертен опит и анализи на съответните институции, органи, служби и агенции на Съюза.

(38) Агенцията следва да бъде в състояние да реагира на ad hoc искания за консултации и помощ от страна на държавите членки и институциите, агенциите и органите на ЕС, попадащи в обхвата на нейните цели.

(39) Необходимо е да се прилагат определени принципи по отношение на управлението на Агенцията с цел спазване на съвместното изявление и общия подход, договорени от междуинституционалната работна група за

децентрализираните агенции на ЕС през юли 2012 г., чиято цел е усъвършенстването на дейността на агенциите и подобряването на техните резултати. Съвместното изявление и общият подход следва да се отчитат, когато е уместно, в работните програми на Агенцията, нейните оценки, както и в докладването и административната практика на Агенцията.

(40) Управителният съвет, състоящ се от държавите членки и Комисията, следва да определя общата насока на дейността на Агенцията и да гарантира, че тя изпълнява своите задачи в съответствие с настоящия регламент. Управителният съвет следва да получи правомощията, необходими за определяне на бюджета, проверка на неговото изпълнение, приемане на подходящи финансови правила, установяване на прозрачни работни процедури за вземане на решения от страна на Агенцията, приемане на единния програмен документ на Агенцията, приемане на собствен правилник за дейността на Агенцията, назначаване на изпълнителния директор и вземане на решения за удължаване или прекратяване на неговия мандат.

(41) С оглед на правилното и ефективно функциониране на Агенцията Комисията и държавите членки следва да гарантират, че лицата, назначени в управителния съвет, притежават подходяща професионална компетентност, както и опит в областите на работа. Държавите членки и Комисията следва също да положат усилия да намалят текучеството на своите съответни представители в управителния съвет, за да се гарантира непрекъснатост на работата му.

(42) Гладкото функциониране на Агенцията налага нейният изпълнителен директор да се назначава въз основа на неговите заслуги и документирани административни и управленски умения, както и въз основа на неговите компетентност и опит, свързани с киберсигурността, като той трябва да изпълнява задълженията си в условия на пълна независимост. Изпълнителният директор следва да изготви предложение за работна програма на Агенцията след предварителни консултации с Комисията и да предприеме всички необходими стъпки за гарантиране на правилното изпълнение на работната програма на Агенцията. Изпълнителният директор следва да изготвя ежегоден доклад, който да бъде представян на управителния съвет, да съставя проект на разчета за предвидените приходи и разходи на Агенцията, както и да изпълнява бюджета. Освен това, изпълнителният директор следва да разполага с възможността да сформира ad hoc работни групи за решаване на специфични въпроси, по-специално с научен, технически, правен или социално-икономически характер. Изпълнителният директор следва да гарантира, че членовете на ad hoc работните групи се избират съобразно най-високите стандарти за експертни знания, като надлежно се отчита балансът при представянето, в зависимост от конкретния въпрос, между държавните администрации на държавите членки, институциите на Съюза и частния сектор, включително индустрията, потребителите и академични експерти в областта на мрежовата и информационната сигурност.

(43) Изпълнителният съвет следва да допринася за ефективното функциониране на управителния съвет. Като част от подготвителната си работа във връзка с решенията на управителния съвет той следва да разглежда подробно съответната информация, да проучва възможните варианти и да предлага консултации и решения за изготвяне на съответните решения на управителния съвет.

(44) Агенцията следва да разполага с Постоянна група на заинтересованите страни в ролята на консултативен орган, за да се гарантира редовен диалог с частния

сектор, потребителските организации и други подходящи заинтересовани страни. Постоянната група на заинтересованите страни, сформирана от управителния съвет по предложение на изпълнителния директор, следва да се съсредоточи върху въпроси, засягащи заинтересованите страни, и да насочва вниманието на Агенцията към тях. Съставът на Постоянната група на заинтересованите страни и задачите, които ѝ се възлагат — по-конкретно предоставянето на консултации относно проекта на работната програма — следва да гарантират достатъчна степен на представяне на заинтересованите страни в работата на Агенцията.

(45) Агенцията следва да има правила за предотвратяването и управлението на конфликти на интереси. Агенцията следва също така да прилага съответните разпоредби на Съюза относно публичния достъп до документи, както е посочено в Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета[34]. Агенцията следва да обработва лични данни в съответствие с Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни[35]. Агенцията следва да съблюдава разпоредбите, приложими за институциите на Съюза, както и националното законодателство относно обработката на информация, по-специално на чувствителната некласифицирана информация и на класифицирана информация на ЕС.

(46) За да се гарантира пълната автономност и независимост на Агенцията и за да може тя да изпълнява допълнителни и нови задачи, включително непредвидени задачи в спешни случаи, на Агенцията следва да бъде предоставен достатъчен и автономен бюджет, чиито приходи се набавят най-вече чрез вноска на Съюза и вноски на трети държави, вземащи участие в работата на Агенцията. По-голямата част от персонала на Агенцията следва да е пряко ангажирана с оперативното изпълнение на мандата на Агенцията. Приемащата държава членка или всяка друга държава членка следва да могат да правят доброволни вноски към приходите на Агенцията. Бюджетната процедура на Съюза следва да остане приложима по отношение на всякакви субсидии, платими от общия бюджет на Съюза. Освен това Сметната палата следва да одитира финансовите отчети на Агенцията, за да се гарантират прозрачност и отчетност.

(47) Оценяването на съответствието е процесът, който показва дали са били изпълнени конкретните изисквания, свързани с продукта, процеса, услугата, подсистемата, физическото или юридическото лице. За целите на настоящия регламент сертифицирането следва да се счита за един вид оценяване на съответствието по отношение на свързаните с киберсигурността характеристики на даден продукт, процес, услуга, система, или комбинация от тях („ИКТ продукти и услуги“) от независима трета страна, различна от създателя на продукта или услугата. Сертифицирането само по себе си не може да гарантира, че сертифицираните ИКТ продукти и услуги са сигурни по отношение на киберзаплахите. То е само процедура и техническа методика за удостоверяване, че ИКТ продуктите и услугите са изследвани и отговарят на определени

[34] 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).

[35] ОВ L 8, 12.1.2001 г., стр. 1.

изисквания, свързани с киберсигурността, които са определени другаде, например в технически стандарти.

(48) Сертифицирането на киберсигурността играе важна роля за повишаването на доверието в ИКТ продуктите и услугите и на тяхната сигурност. Цифровият единен пазар, и по-конкретно основаващата се на данни икономика и „интернет на нещата“, могат да функционират успешно само ако обществото като цяло е уверено, че тези продукти и услуги предоставят определено ниво на обезпеченост в областта на киберсигурността. Свързаните автомобили и автомобилите с автоматично управление, електронните медицински устройства, системите за управление на промишлената автоматизация или интелигентните енергийни мрежи са само някои от примерите за сектори, в които сертифицирането вече широко се използва или е вероятно да бъде използвано в близко бъдеще. Секторите, регулирани от Директивата за МИС, са също така сектори, в които сертифицирането на киберсигурността е от ключово значение.

(49) В съобщението от 2016 г., озаглавено „Укрепване на отбранителната способност на Европа срещу кибератаки и изграждане на конкурентен и иновативен сектор на киберсигурността“, Комисията описа необходимостта от висококачествени, достъпни и оперативно съвместими продукти и решения, свързани с киберсигурността. Предлагането на ИКТ продукти и услуги в рамките на единния пазар остава обаче силно разпокъсано географски. Това е така, защото развитието на сектора на киберсигурността в Европа се основава главно на търсене от страна на националните правителства. Освен това, липсата на оперативно съвместими решения (технически стандарти), практики и прилагани в целия ЕС механизми за сертифициране е част от другите пропуски, които оказват влияние върху единния пазар на киберсигурността. От една страна, това влошава конкурентоспособността на европейските компании в национален, европейски и световен мащаб. От друга, то ограничава избора на надеждни и приложими технологии за киберсигурност, до които лицата и предприятията имат достъп. Аналогично, в междинния преглед на изпълнението на стратегията за цифровия единен пазар Комисията подчерта необходимостта от безопасни свързани продукти и системи и посочи, че създаването на Европейска рамка за ИКТ сигурност, определяща правила относно организацията на сертифицирането на сигурността на ИКТ в ЕС, би могло да помогне както за запазването на доверието в интернет, така и за преодоляването на настоящата разпокъсаност на пазара за киберсигурност.

(50) Понастоящем сертифицирането на киберсигурността на ИКТ продукти и услуги се използва само в ограничена степен. Ако има такова, то се осъществява предимно на равнището на държавите членки или в рамките на секторно обусловени схеми. В тези условия сертификат, издаден от един национален орган в областта на киберсигурността, по принцип не се признава от другите държави членки. Поради това може да се наложи предприятията да сертифицират своите продукти и услуги в няколко държави членки, в които развиват дейност, например с цел да участват в националните процедури за възлагане на обществени поръчки. Освен това, въпреки че се появяват нови схеми, изглежда няма съгласуван и цялостен подход по отношение на хоризонталните въпроси, свързани с киберсигурността, например в сферата на „интернет на нещата“. Действащите схеми проявяват съществени недостатъци и различия по отношение на продуктовия обхват, нивата на обезпеченост, съществените критерии и фактическото използване.

(51) В миналото бяха положени известни усилия за постигането на взаимно признаване на сертификати в Европа. Те обаче имаха само частичен успех. Най-важният пример в това отношение е споразумението за взаимно признаване (СВП) на Групата на висшите служители по сигурността на информационните системи (SOG-IS). Макар да представлява най-важният модел за сътрудничество и взаимно признаване в областта на сертифицирането на сигурността, СВП на SOG-IS показва някои съществени недостатъци, свързани с неговите високи разходи и ограничен обхват. Досега са разработени само няколко защитни профила за цифрови продукти, като например за цифров подпис, цифров тахограф и карти с чип. Но най-важното е, че SOG-IS включва само част от държавите — членки на Съюза. Това ограничава ефективността на СВП на SOG-IS от гледна точка на вътрешния пазар.

(52) С оглед на посоченото по-горе е необходимо да се въведе Европейска рамка на сертифициране на киберсигурността, която да определя основните хоризонтални изисквания за европейските схеми за сертифициране на киберсигурност, които ще бъдат разработени, и да дава възможност сертификатите за ИКТ продукти и услуги да бъдат признавани и използвани във всички държави членки. Европейската рамка следва да има две цели: от една страна, тя следва да спомогне за повишаване на доверието в ИКТ продуктите и услугите, които са били сертифицирани по такива схеми. От друга страна тя следва да предотврати увеличаването на броя на противоречащи си или припокриващи се национални сертификати за киберсигурност и по този начин да намали разходите за предприятията, упражняващи дейност на единния цифров пазар. Схемите следва да бъдат недискриминационни и да се основават на международни стандарти и/или стандарти на Съюза, освен ако тези стандарти са неефективни или неподходящи за изпълнението на легитимните цели на ЕС в това отношение.

(53) Комисията следва да бъде оправомощена да приема европейски схеми за сертифициране на киберсигурност за специфични групи ИКТ продукти и услуги. Тези схеми следва да се прилагат и контролират от национални надзорни органи за сертифициране, а сертификатите, издадени в рамките на тези схеми, следва да са валидни и да се признават на цялата територия на Съюза. Схемите за сертифициране, управлявани от промишлеността или от други частни организации, следва да не попадат в обхвата на регламента. Въпреки това, управляващите такива схеми органи могат да предлагат на Комисията да ги разгледа като основа за схеми, които да бъдат одобрени като европейска схема.

(54) Разпоредбите на настоящия регламент не следва да засягат законодателство на Съюза, с което се определят специфични правила за сертифициране на ИКТ продукти и услуги. По-конкретно с Общия регламент относно защитата на данните (ОРЗД) се установяват разпоредби за създаване на механизми за сертифициране и на печати и маркировки за защита на данните, чрез които се доказва съответствието с посочения регламент на операциите по обработката на данни от страна на контрольорите и обработващите тези данни. Тези механизми за сертифициране и тези печати и маркировки за защита на данните следва да позволяват на субектите, предоставящи своите данни, бързо да оценяват нивото на защита на данните на съответните продукти и услуги. Настоящият регламент не засяга сертифицирането на операции по обработката на данни съгласно ОРЗД, включително когато тези операции са включени в продукти и услуги.

(55) Целта на европейските схеми за сертифициране на киберсигурността следва да бъде да се гарантира, че ИКТ продуктите и услугите, сертифицирани по такава

схема, съответстват на специфицираните изисквания. Тези изисквания засягат тяхната способност да устояват — при определено ниво на обезпеченост — на действия, които имат за цел да нарушат наличността, автентичността, целостта и поверителността на съхраняваните, предавани или обработвани данни, или на свързаните с тях функции или услуги, предлагани непосредствено от тези продукти, процеси, услуги и системи или достъпни чрез тях, по смисъла на настоящия регламент. Не е възможно в настоящия регламент да се определят подробно изискванията във връзка с киберсигурността на всички ИКТ продукти и услуги. ИКТ продуктите и услугите и техните потребности във връзка с киберсигурността са толкова разнообразни, че е много трудно да се формулират общи изисквания в областта на киберсигурността, които да са общовалидни. Поради това е необходимо да се приеме широко и общо понятие за киберсигурността за целите на сертифицирането, което да се допълва от набор от конкретни цели, свързани с киберсигурността, които трябва да бъдат вземани предвид при разработването на европейските схеми за сертифициране на киберсигурността. Условията, при които тези цели ще бъдат постигани при конкретни ИКТ продукти и услуги, следва да бъдат допълнително уточнявани в подробности на нивото на всяка отделна схема за сертифициране, приемана от Комисията, например чрез позоваване на стандарти или технически спецификации.

(56) На Комисията следва да бъде предоставено правомощието да изисква от ENISA да подготвя проекти за схеми за отделни ИКТ продукти или услуги. Комисията следва да бъде оправомощена да приема посредством актове за изпълнение европейски схеми за сертифициране на киберсигурността въз основава на проекти за схеми, предложени от ENISA. Като се вземат предвид общата цел и целите, свързани със сигурността, определени в настоящия регламент, в европейските схеми за сертифициране на киберсигурността, приемани от Комисията, следва да бъде определен минимален набор от елементи по отношение на предмета, обхвата и функционирането на дадена схема. Те следва да включват, наред с другото, обхвата и предмета на сертифицирането на киберсигурността, включително обхванатите категории ИКТ продукти и услуги, подробна спецификация на изискванията в областта на киберсигурността, например чрез позоваване на стандарти или технически спецификации, конкретните критерии и методи за оценка, както и желаното ниво на обезпеченост: основно, значително и/или високо.

(57) Използването на европейското сертифициране за киберсигурност следва да остане доброволно, освен ако не е предвидено друго в законодателството на Съюза или в националното законодателство. Въпреки това, за да бъдат постигнати целите на настоящия регламент и да се избегне разпокъсване на вътрешния пазар, националните схеми или процедури за сертифициране на киберсигурността за ИКТ продукти и услуги, обхванати от европейска схема за сертифициране на киберсигурността, следва да престанат да пораждат правно действие от датата, определена от Комисията в акта за изпълнение. Освен това държавите членки следва да не въвеждат нови национални схеми за сертифициране на киберсигурността на ИКТ продукти и услуги, които са вече обхванати от съществуваща европейска схема за сертифициране на киберсигурността.

(58) След като дадена европейски схема за сертифициране на киберсигурността бъде приета, производителите на ИКТ продукти или доставчиците на ИКТ услуги

следва да могат да подават заявления за сертифициране на своите продукти или услуги до орган за оценяване на съответствието по техен избор. Органите за оценяване на съответствието следва да се акредитират от орган по акредитация, ако отговарят на конкретни изисквания, определени в настоящия регламент. Акредитацията следва да се издава за максимален срок от пет години и може да бъде подновявана при същите условия, ако органът за оценяване на съответствието отговаря на изискванията. Органите по акредитация следва да отнемат акредитацията на органа за оценяване на съответствието, ако условията за акредитация не са били спазени или вече не се спазват, или ако органът за оценяване на съответствието е предприел действия, които нарушават разпоредбите на настоящия регламент.

(59) Трябва да се изиска от всички държави членки да определят по един надзорен орган за сертифицирането на киберсигурността, който да упражнява надзор дали органите за оценяване на съответствието и сертификатите, издавани от такива органи, установени на тяхната територия, отговарят на изискванията на настоящия регламент и на съответните схеми за сертифициране на киберсигурността. Националните надзорни органи за сертифициране следва да разглеждат жалбите, подадени от физически или юридически лица по отношение на сертификатите, издадени от органите за оценяване на съответствието, установени на тяхна територия, да разследват в необходимата степен предмета на жалбата и информират жалбоподателя за напредъка и резултатите от разследването в разумен срок. Освен това те следва да си сътрудничат с други национални надзорни органи за сертифицирането или други публични органи, включително чрез споделяне на информация за възможни несъответствия на ИКТ продукти и услуги с изискванията на настоящия регламент или на конкретни европейски схеми за сертифициране на киберсигурността.

(60) За да се гарантира последователно прилагане на Европейската рамка за сертифициране на киберсигурността, следва да се създаде Европейска група за сертифициране на киберсигурността („групата“), състояща се от национални надзорни органи за сертифицирането. Основните задачи на групата следва да са да съветва и подпомага Комисията при работата ѝ за гарантиране на последователното изпълнение и прилагане на Европейската рамка за сертифициране на киберсигурността; да подпомага Агенцията и да си сътрудничи тясно с нея при изготвянето на проекти на схеми за сертифициране на киберсигурността; да препоръчва на Комисията да изиска от Агенцията подготовката на конкретен проект на европейска схема за сертифициране на киберсигурността; и да приема становища, адресирани до Комисията, свързани с поддръжката и преразглеждането на съществуващите европейски схеми за сертифициране на киберсигурността.

(61) С цел да се повиши осведомеността и да се улесни приемането на бъдещи схеми на ЕС за киберсигурност, Европейската комисия може да издава общи или специфични за сектора на насоки за киберсигурност, например относно добри практики в областта на киберсигурността или отговорно поведение по отношение на киберсигурността, които да подчертават положителните ефекти от използването на сертифицирани ИКТ продукти и услуги.

(62) Подкрепата на Агенцията за сертифицирането на киберсигурността следва да включва и координация с Комитета по сигурността на Съвета и съответния

национален орган относно одобряването на криптографските характеристики на продукти, които се използват в мрежи за класифицирана информация.

(63) За целите на допълнителното конкретизиране на критериите за акредитиране на органите за оценяване на съответствието, на Комисията следва да се делегира правомощието да приема актове в съответствие с член 290 от Договора за функционирането на Европейския съюз. Комисията следва да провежда подходящи консултации, включително на експертно равнище, по време на подготвителната си работа. Тези консултации следва да се провеждат в съответствие с принципите, заложени в Междуинституционалното споразумение за по-добро законотворчество от 13 април 2016 г. По-специално, с цел осигуряване на равно участие при подготовката на делегирани актове, Европейският парламент и Съветът следва да получават всички документи едновременно с експертите от държавите членки, като техните експерти получават систематично достъп до заседанията на експертните групи на Комисията, занимаващи се с подготовката на делегираните актове.

(64) За да се гарантират еднакви условия за прилагане на настоящия регламент, на Комисията следва да се предоставят изпълнителни правомощия, когато това е предвидено в настоящия регламент. Тези правомощия следва да се упражняват в съответствие с Регламент (ЕС) № 182/2011.

(65) За приемането на актове за изпълнение относно европейските схеми за сертифициране на киберсигурността на ИКТ продукти и услуги следва да се използва процедурата по разглеждане; по отношение на условията за провеждане на разследвания от страна на Агенцията; както и по отношение на обстоятелствата, форматите и процедурите за уведомяване на Комисията относно органи за оценяване на съответствието от националните надзорни органи за сертифицирането.

(66) Дейностите на Агенцията следва да бъдат оценявани от независим орган. При оценката следва да се има предвид постигането на целите от страна на Агенцията, нейните работни практики и значимостта на задачите ѝ. В оценката следва също така да се разглеждат въздействието, ефективността и ефикасността на Европейската рамка за сертифициране на киберсигурността.

(67) Регламент (ЕС) № 526/2013 следва да бъде отменен.

(68) Тъй като целите на настоящия регламент не могат да бъдат постигнати в достатъчна степен от държавите членки и могат да бъдат постигнати по-добре на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от Договора за Европейския съюз. В съответствие с принципа на пропорционалност, както е определено в споменатия член, настоящият регламент не надхвърля необходимото за постигането на тази цел,

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

ДЯЛ I

ОБЩИ РАЗПОРЕДБИ

Член 1
Предмет и обхват

С оглед да се гарантира правилното функциониране на вътрешния пазар, като същевременно се постигне висока степен на киберсигурност, киберустойчивост и доверие в киберпространството в рамките на Съюза, с настоящия регламент се определят:

а) целите, задачите и организационните аспекти на ENISA — Агенцията на ЕС за киберсигурност, наричана по-долу „Агенцията“; и

б) рамка за създаването на европейски схеми за сертифициране на киберсигурността, с цел да се гарантира подходящо ниво на киберсигурността на ИКТ продукти и услуги в Съюза. Тази рамка се прилага, без да се засягат специфичните разпоредби за доброволно или задължително сертифициране, предвидени в други правни актове на Съюза.

Член 2
Определения

За целите на настоящия регламент се прилагат следните определения:

1) „киберсигурност“ обхваща всички дейности, необходими за защита от киберзаплахи на мрежовите и информационните системи, на техните потребители и засегнати лица;

2) „мрежова и информационна система“ означава система по смисъла на член 4, точка 1 от Директива (ЕС) 2016/1148;

3) „национална стратегия относно сигурността на мрежовите и информационните системи“ означава рамка по смисъла на член 4, точка 3 от Директива (ЕС) 2016/1148;

4) „оператор на основни услуги“ означава публичен или частен субект съгласно определението в член 4, точка 4 от Директива (ЕС) № 2016/1148;

5) „доставчик на цифрови услуги“ означава юридическо лице, предоставящо цифрова услуга, съгласно определението в член 4, точка 6 от Директива (ЕС) 2016/1148;

6) „инцидент“ означава събитие съгласно определението в член 4, точка 7 от Директива (ЕС) 2016/1148;

7) „действия при инцидент“ означава всяка процедура съгласно определението в член 4, точка 8 от Директива (ЕС) 2016/1148;

8) „киберзаплаха“ означава всяко потенциално обстоятелство или събитие, което може да има неблагоприятно въздействие върху мрежови и информационни системи, техните потребители и засегнати лица;

9) „европейска схема за сертифициране на киберсигурността“ означава цялостен набор от правила, технически изисквания, стандарти и процедури, определени на равнището на Съюза, които се прилагат за сертифициране на продукти и услуги на информационните и комуникационните технологии (ИКТ продукти и услуги), които попадат в обхвата на съответната конкретна схема;

10) „европейски сертификат за киберсигурност“ означава документ, издаден от орган за оценяване на съответствието, който удостоверява, че даден ИКТ продукт или дадена ИКТ услуга отговаря на специфичните изисквания, определени в съответната европейска схема за сертифициране на киберсигурността;

11) „ИКТ продукт и услуга“ означава елемент или група елементи на мрежовите и информационните системи;

12) „акредитация“ означава акредитация съгласно определението в член 2, точка 10 от Регламент (ЕО) № 765/2008;

13) „национален орган по акредитация“ означава национален орган по акредитация съгласно определението в член 2, точка 11 от Регламент (ЕО) № 765/2008;

14) „оценяване на съответствието“ означава оценяване на съответствието съгласно определението в член 2, точка 12 от Регламент (ЕО) № 765/2008;

15) „орган за оценяване на съответствието“ означава орган за оценяване на съответствието съгласно определението в член 2, точка 13 от Регламент (ЕО) № 765/2008;

16) „стандарт“ означава стандарт съгласно определението в член 2, точка 1 от Регламент (ЕС) № 1025/2012.

ДЯЛ II
ENISA — Агенцията на Европейския съюз за киберсигурност

ГЛАВА I
ОБХВАТ, ЦЕЛИ И ЗАДАЧИ

Член 3
Мандат

1. Агенцията поема задачите, възложени ѝ с настоящия регламент, с цел да допринесе за постигане на високо равнище на киберсигурността в Съюза.

2. Агенцията изпълнява задачи, поверени ѝ чрез законодателни актове на Съюза, с които се определят мерки за сближаване на законовите, подзаконовите и административните разпоредби на държавите членки, свързани с киберсигурността.

3. Целите и задачите на Агенцията не накърняват компетентността на държавите членки по въпросите на киберсигурността, нито дейностите, свързани с обществената сигурност, отбраната, националната сигурност и дейностите на държавата в областта на наказателното право.

Член 4
Цели

1. Агенцията функционира като експертен център по въпросите на киберсигурността благодарение на своята независимост, на научното и техническо качество на консултациите, които предоставя, на предлаганата от нея помощ и информация, на прозрачността на процедурите и методите ѝ на работа, както и на добросъвестното изпълнение на възложените ѝ задачи.

2. Агенцията подпомага институциите, агенциите и органите на Съюза, както и държавите членки, при разработването и прилагането на политиките, свързани с киберсигурността.

3. Агенцията подпомага изграждането на капацитет и подготвеността в целия Съюз, като съдейства на Съюза, държавите членки и заинтересованите страни от публичния и частния сектор, с цел засилване на защитата на техните мрежи и информационни системи, развитие на уменията и знанията в областта на киберсигурността, както и за постигане на киберустойчивост.

4. Агенцията насърчава сътрудничеството и координацията между държавите членки на равнището на Съюза, неговите институции, агенции и органи, и съответните заинтересовани страни, включително от частния сектор, по въпросите на киберсигурността.

5. Агенцията повишава способностите в областта на киберсигурността на равнището на Съюза, за да допълни дейността на държавите членки за предотвратяването на киберзаплахи и реакцията спрямо тях, особено в случаи на трансгранични инциденти.

6. Агенцията насърчава използването на сертифициране, включително като допринася за създаването и поддържането на мрежа за сертифициране на киберсигурността на равнище ЕС съгласно дял III от настоящия регламент, с цел постигане на повече прозрачност на обезпечаването на киберсигурността на ИКТ продукти и услуги и за укрепване на доверието в цифровия вътрешен пазар.

7. Агенцията насърчава високо равнище на осведоменост на гражданите и на предприятията по въпросите на киберсигурността.

Член 5

Задачи, свързани с разработването и прилагането на политиката и законодателството на Съюза

Агенцията дава своя принос за разработването и прилагането на политиката и законодателството на Съюза, като:

1. подпомага и консултира, особено посредством представяне на независими становища и подготвителна работа по разработването и прегледа на политиката и законодателството на Съюза в областта на киберсигурността, както и специфични за сектора политически и законодателни инициативи, засягащи въпросите на киберсигурността;

2. подпомага държавите членки в последователното прилагане на политиката и законодателството на Съюза по отношение на киберсигурността, особено във връзка с Директива (ЕС) 2016/1148, включително посредством становища, насоки, консултации и споделяне на най-добри практики по въпроси като управление на риска, докладване на инциденти и обмен на информация, както и чрез улесняване на обмена на най-добри практики между компетентните органи в това отношение;

3. дава своя принос за работата на групата за сътрудничество съгласно член 11 от Директива (ЕС) 2016/1148 чрез предоставяне на експертен опит и помощ;

4. подпомага:

    1) разработването и прилагането на политиката на Съюза в областта на електронната самоличност и удостоверителните услуги, по-специално чрез предоставяне на консултации и технически насоки, както и улесняване на обмена на най-добри практики между компетентните органи;

    2) насърчаването на повишено равнище на сигурност на електронните съобщения, включително чрез предоставяне на експертен опит и консултации и улесняване на обмена на най-добри практики между компетентните органи;

5. подпомага редовното преразглеждане на дейностите по политиката на ЕС и представянето на годишния доклад за напредъка на прилагането на съответната нормативна уредба относно:

    а) докладването на инциденти от държавите членки до единното звено за контакти на групата за сътрудничество съгласно член 10, параграф 3 от Директива (ЕС) 2016/1148;

б) докладването пред Агенцията от страна на надзорните органи на нарушения на сигурността и целостта на системите, засягащи доставчиците на удостоверителни услуги, както е предвидено в член 19, параграф 3 от Регламент (ЕС) № 910/2014;

в) докладването на нарушения на сигурността, осъществено от предприятията, осигуряващи обществени съобщителни мрежи или обществено достъпни електронни съобщителни услуги и предоставяно на Агенцията от компетентните органи съгласно член 40 от [Директива за създаване на Европейския кодекс за електронните съобщения].

Член 6

Задачи, свързани с изграждането на капацитет

1. Агенцията съдейства:

а) на държавите членки в усилията им да подобрят предотвратяването, откриването, анализа и способността за реагиране на проблеми и инциденти на киберсигурността, като им предоставя необходимите знания и експертен опит;

б) на институциите, органите, службите и агенциите на Съюза в усилията им да подобрят предотвратяването, установяването, анализа и способността за реагиране на проблеми и инциденти на киберсигурността чрез целесъобразна подкрепа за CERT на институциите, агенциите и органите на Съюза (CERT-EU);

в) на държавите членки, по тяхна молба, за създаване на екипи за реагиране при инциденти с компютърната сигурност (CSIRT) съгласно член 9, параграф 5 от Директива (ЕС) 2016/1148;

г) на държавите членки, по тяхна молба, за разработване на национални стратегии за мрежовите и информационните системи съгласно член 7, параграф 2 от Директива (ЕС) 2016/1148; Агенцията също така насърчава разпространението и следи напредъка на изпълнението на тези стратегии в целия Съюз, за да популяризира най-добрите практики;

д) на институциите на Съюза при изготвянето и прегледа на стратегиите на Съюза за киберсигурността, като насърчава тяхното разпространение и проследява напредъка в изпълнението им;

е) на националните CSIRT и CSIRT на Съюза, като увеличава техните способности, включително чрез насърчаване на диалога и обмена на информация, за да гарантира, че всеки CSIRT отговаря на общ набор от минимални способности и работи в съответствие с най-добрите практики съобразно актуалните технологични постижения;

ж) на държавите членки чрез организиране на широкомащабните ежегодни учения в областта на киберсигурността на равнището на Съюза, посочени в член 7, параграф 6, и чрез препоръки за политиката въз основа на процеса на оценка на ученията и направените от тях изводи;

з) на съответните публични органи чрез предлагане на обучения по киберсигурност, по целесъобразност съвместно със заинтересованите страни;

и) на групата за сътрудничество чрез обмен на най-добри практики, по-специално относно определянето на оператори на основни услуги от държавите членки, включително по отношение на трансграничните взаимовръзки, рисковете и инцидентите, съгласно член 11, параграф 3, буква л) от Директива (ЕС) 2016/1148.

2. Агенцията улеснява създаването и непрекъснато подпомага секторните центрове за споделяне и анализ на информация (ISAC), по-специално в секторите, изброени в приложение II към Директива (ЕС) 2016/1148, като им предоставя най-добри практики и насоки относно наличните инструменти и процедури, както и относно начините за преодоляване на нормативните проблеми във връзка с обмена на информация.

Член 7

Задачи, свързани с оперативното сътрудничество на равнището на Съюза

1. Агенцията подпомага оперативното сътрудничество между компетентните публични органи и между заинтересованите страни.

2. Агенцията съдейства на оперативно ниво и създава синергии с институциите, органите, службите и агенциите на Съюза, включително CERT-EU, службите, работещи в областта на киберпрестъпността и надзорните органи за защита на неприкосновеността на личния живот и на личните данни, с оглед решаване на въпроси от общ интерес, включително посредством:

   а) обмен на ноу-хау и най-добри практики;

   б) осигуряване на съвети и насоки по актуални въпроси, свързани с киберсигурността;

   в) определяне в консултация с Комисията на практически договорености за изпълнението на конкретни задачи.

3. Агенцията осигурява секретариата на мрежата на CSIRT съгласно член 12, параграф 2 от Директива (ЕС) 2016/1148 и активно улеснява споделянето на информация и сътрудничеството между своите членове.

4. Агенцията допринася за оперативно сътрудничество в рамките на мрежата на CSIRT, като предоставя подкрепа на държавите членки чрез:

   а) консултации за подобряване на способностите им за предотвратяване, откриване и реагиране на инциденти;

   б) предоставяне, по тяхно искане, на техническа помощ при инциденти със значително или съществено въздействие;

   в) анализи на уязвими точки, артефакти и инциденти.

В изпълнението на тези задачи Агенцията и CERT-EU си сътрудничат структурирано, за да се възползват от синергии, особено по отношение на оперативните аспекти.

5. По искане на две или повече заинтересовани държави членки и единствено с цел консултация за предотвратяване на бъдещи инциденти, Агенцията осигурява подпомагане или извършва последваща техническа проверка след уведомленията от засегнатите предприятия за инциденти със значително или съществено въздействие съгласно Директива (ЕС) 2016/1148. Агенцията също така осъществява такава проверка при надлежно обосновано искане от

Комисията със съгласието на засегнатите държави членки в случай на инциденти, засягащи интересите на повече от две държави членки.

Обхватът на проверката и процедурата за извършването ѝ се договарят между засегнатите държави членки и Агенцията и не засягат евентуални текущи криминални разследвания относно въпросния инцидент. Проверката завършва с окончателен технически доклад, съставен от Агенцията по-специално въз основа на информацията и коментарите, представени от съответните държави членки и предприятия, и съгласуван със съответните държави членки. В мрежата на CSIRT се представя резюме на доклада с акцент върху препоръките за предотвратяването на бъдещи инциденти.

6. Агенцията организира ежегодни учения в областта на киберсигурността на равнището на Съюза и подпомага държавите членки и институциите, агенциите и органите на Съюза, като организира учения по тяхно искане. Годишните учения на равнището на Съюза включват технически, оперативни и стратегически елементи и спомагат за подготовката на колективна реакция на равнище ЕС на широкомащабни трансгранични киберинциденти. По целесъобразност Агенцията също така участва и помага в организирането на секторни учения в областта на киберсигурността заедно със съответните ISAC, като позволява на ISAC да участват и в учения на равнището на Съюза.

7. Агенцията изготвя редовен доклад за техническото състояние на киберсигурността на ЕС, който разглежда инциденти и заплахи и се основава на информация от открити източници, собствените ѝ анализи и доклади, споделяни от, между другото: CSIRT на държавите членки (на доброволни начала) или единните звена за контакт по Директивата за МИС (съгласно член 14, параграф 5 от Директивата за МИС); Европейския център за борба с киберпрестъпността (EC3) към Европол, CERT-EU.

8. Агенцията допринася за разработването на колективна реакция на равнище ЕС и на равнище държави членки на широкомащабни трансгранични инциденти или кризи, свързани с киберсигурността, основно чрез:

   а) обобщаване на доклади от национални източници с цел да допринесе за общата ситуационна осведоменост;

   б) осигуряване на ефективен поток на информация и предоставяне на механизми за ескалация между мрежата на CSIRT и техническите и политическите фактори на равнището на Съюза;

   в) подпомагане на техническата работа по инциденти или кризи, включително улесняване на обмена на технически решения между държавите членки;

   г) съдействие за представянето пред обществеността, свързано с инциденти или кризи;

   д) изпитване на плановете за сътрудничество в отговор на такива инциденти или кризи.

Член 8

Задачи, свързани с пазара, сертифицирането на киберсигурността и стандартизацията

Агенцията:

а) насърчава разработването и изпълнението на политиката на Съюза за сертифициране на киберсигурността на ИКТ продукти и услуги, както е предвидено в дял III от настоящия регламент, като:

1) изготвя проекти за схеми за европейско сертифициране за киберсигурността на ИКТ продукти и услуги в съответствие с член 44 от настоящия регламент;

2) съдейства на Комисията с осигуряване на секретариата на Европейската група за сертифициране на киберсигурността съгласно член 53 от настоящия регламент;

3) съставя и публикува насоки и разработва добри практики относно изискванията за киберсигурност на ИКТ продукти и услуги съвместно с националните надзорни органи по сертифицирането и с отрасъла;

б) улеснява въвеждането и използването на европейски и международни стандарти за управление на риска и за сигурността на ИКТ продукти и услуги, и също така съвместно с държавите членки съставя препоръки и насоки по отношение на техническите области, свързани с изискванията за сигурност за операторите на основни услуги и доставчиците на цифрови услуги, както и по отношение на вече съществуващите стандарти, включително националните стандарти на държавите членки, съгласно член 19, параграф 2 от Директива (ЕС) 2016/1148;

в) извършва и разпространява редовни анализи на основните тенденции на пазара на киберсигурността по отношение както на търсенето, така и на предлагането, с цел да се развие пазарът за киберсигурност в Съюза.

Член 9

Задачи, свързани с познанията, информацията и повишаването на осведомеността

Агенцията:

а) анализира нововъзникващите технологии и предоставя тематични оценки за очакваните социални, правни, икономически и регулаторни въздействия на технологичните нововъведения върху киберсигурността;

б) извършва дългосрочни стратегически анализи на заплахите и инцидентите в областта на киберсигурността, за да установи възникващи тенденции и спомогне за предотвратяване на проблемите пред киберсигурността;

в) съвместно с експерти от компетентните органи на държавите членки предоставя съвети, насоки и най-добри практики за сигурността на мрежовите и информационните системи, по-специално за сигурността на интернет инфраструктурата и инфраструктурите, поддържащи изброените в приложение II от Директива (ЕС) 2016/1148 сектори;

г) събира, организира и предоставя на разположение на обществеността чрез специален портал осигурена от институциите, агенциите и органите на Съюза информация относно киберсигурността;

д) повишава обществената осведоменост относно рисковете за киберсигурността и предлага насоки и добри практики за отделните потребители, насочени към гражданите и организациите;

е) събира и анализира обществено достъпна информация за значителни инциденти и съставя доклади с цел предоставяне на насоки на предприятията и гражданите в целия Съюз;

ж) съвместно с държавите членки и институциите, органите, службите и агенциите на Съюза организира редовни информационни кампании за повишаване на киберсигурността и на присъствието си в Съюза.

Член 10

Задачи, свързани с научните изследвания и иновациите

Във връзка с научните изследвания и иновациите, Агенцията:

а) консултира Съюза и държавите членки относно нуждата от научни изследвания в областта на киберсигурността, с което съдейства за ефективна реакция на настоящите и нововъзникващите рискове и заплахи, както и относно нови и нововъзникващи информационни и комуникационни технологии и ефективното използване на технологиите за предотвратяване на риска;

б) участва, съобразно делегирани ѝ от Комисията правомощия, като изпълнител на програми за финансиране на научните изследвания и иновациите или като бенефициер.

Член 11

Задачи, свързани с международното сътрудничество

Агенцията дава своя принос в усилията на Съюза за сътрудничество с трети държави и международни организации с оглед насърчаване на международното сътрудничество в областта на киберсигурността, като:

а) участва по целесъобразност като наблюдател при организирането на международни учения, анализира и докладва на управителния съвет резултатите от такива учения;

б) по искане на Комисията улеснява обмена на най-добри практики между съответните международни организации;

в) по искане предоставя на Комисията експертни становища.

ГЛАВА II
ОРГАНИЗАЦИЯ НА АГЕНЦИЯТА

Член 12
Структура

Административната и управленска структура на Агенцията се състои от:

а) управителен съвет, който изпълнява функциите, определени в член 14;

б) изпълнителен съвет, който изпълнява функциите, определени в член 18;

в) изпълнителен директор, който изпълнява задълженията, определени в член 19; както и

г) постоянна група на заинтересованите страни, която изпълнява функциите, определени в член 20.

РАЗДЕЛ 1
УПРАВИТЕЛЕН СЪВЕТ

Член 13
Състав на управителния съвет

1. Съставът на управителния съвет включва по един представител на всяка държава членка и двама представители, назначени от Комисията. Всеки от представителите има право на глас.

2. Всеки член на управителния съвет има заместник, който го представлява при отсъствие.

3. Членовете на управителния съвет и техните заместници се назначават въз основа на познанията им в областта на киберсигурността, като се вземат предвид съответните им умения в областта на управлението, администрацията и бюджетирането. Комисията и държавите членки полагат усилия за ограничаване на текучеството на своите представители в управителния съвет, за да се осигури непрекъснатост на работата му. Комисията и държавите членки се стремят към постигането на балансирано представителство между мъже и жени в управителния съвет.

4. Мандатът на членовете на управителния съвет и на техните заместници е четири години. Този мандат подлежи на подновяване.

Член 14
Функции на управителния съвет

1. Управителният съвет:

   а) определя общата насока на дейността на Агенцията и гарантира, че тя работи в съответствие с правилата и принципите, заложени в настоящия регламент. Той също така гарантира съгласуваността на работата на Агенцията с дейностите, осъществявани от държавите членки, както и на нивото на Европейския съюз;

б) приема проекта на единен програмен документ, посочен в член 21, преди представянето му на Комисията за становище;

в) приема, съобразявайки се със становището на Комисията, единния програмен документ на Агенцията с мнозинство от две трети от членовете си и в съответствие с член 17;

г) приема с мнозинство от две трети от членовете годишния бюджет на Агенцията и упражнява други функции във връзка с бюджета на Агенцията в съответствие с глава III;

д) оценява и приема консолидирания годишен доклад за дейностите на Агенцията и изпраща доклада и неговата оценка най-късно до 1 юли на следващата година на Европейския парламент, Съвета, Комисията и Сметната палата. Годишният доклад включва отчетите и описва как Агенцията е изпълнила своите показатели за изпълнение. Годишният доклад е обществено достъпен;

е) приема финансовите правила, приложими за Агенцията, в съответствие с член 29;

ж) приема стратегия за борба с измамите, пропорционална на риска от измами, като взема предвид анализа на разходите и ползите от действията, които следва да бъдат предприети;

з) приема правила за предотвратяване и управление на конфликти на интереси по отношение на своите членове;

и) осигурява подходящи последващи действия във връзка с констатациите и препоръките, произтичащи от разследвания на Европейската служба за борба с измамите (OLAF) и на различни вътрешни или външни одитни доклади и оценки;

й) приема свой правилник за дейността;

к) в съответствие с параграф 2 упражнява по отношение на персонала на Агенцията правомощията, предоставени на органа по назначаването съгласно Правилника за длъжностните лица, както и правомощията, предоставени на органа, оправомощен да сключва трудови договори съгласно Условията за работа на другите служители на Съюза („правомощия на органа по назначаването“);

л) приема правила за прилагане на Правилника за длъжностните лица и Условията за работа на другите служители на Съюза в съответствие с процедурата, предвидена в член 110 от Правилника за длъжностните лица;

м) назначава изпълнителния директор и при необходимост удължава срока на мандата му или го отстранява от длъжност в съответствие с член 33 от настоящия регламент;

н) назначава счетоводител, който може да бъде счетоводителят на Комисията и който се ползва с пълна независимост при изпълнението на своите задължения;

о) взема всички решения относно създаването на вътрешната структура на Агенцията и при необходимост относно нейното

изменение, като взема под внимание нуждите за дейността на Агенцията, както и доброто бюджетно управление;

п) разрешава сключването на работни договорености в съответствие с членове 7 и 39.

2. Управителният съвет, в съответствие с член 110 от Правилника за длъжностните лица, приема на основание член 2, параграф 1 от същия правилник и член 6 от Условията за работа на другите служители решение за делегиране на съответните правомощия на орган по назначаването на изпълнителния директор и за определяне на условията, при които делегираните правомощия могат да бъдат оттеглени. Изпълнителният директор има правото от своя страна да делегира тези правомощия на други лица.

3. Когато изключителни обстоятелства налагат това, управителният съвет може с решение временно да оттегли правомощията на орган по назначаването, делегирани на изпълнителния директор, както и правомощията, които последният е делегирал на други лица, и да ги упражнява пряко или да ги делегира на някой от членовете си или на друг служител, различен от изпълнителния директор.

Член 15

Председател на управителния съвет

Управителният съвет избира с мнозинство от две трети от членовете си свой председател и заместник-председател измежду членовете си за срок от четири години, като този срок може да бъде подновяван еднократно. Ако обаче по време на мандата им те престанат да бъдат членове на управителния съвет, мандатът изтича автоматично на същата дата. Заместник-председателят замества служебно председателя, ако последният не е в състояние да изпълнява своите задължения.

Член 16

Заседания на управителния съвет

1. Заседанията на управителния съвет се свикват от неговия председател.

2. Управителният съвет провежда най-малко две редовни заседания годишно. Той провежда и извънредни заседания по искане на председателя, на Комисията или на най-малко една трета от членовете си.

3. Изпълнителният директор взема участие в събранията на управителния съвет без право на глас.

4. По покана на председателя членове на Постоянната група на заинтересованите страни могат да участват в заседанията на управителния съвет без право на глас.

5. По време на заседанията членовете на управителния съвет и техните заместници могат да бъдат подпомагани от съветници или експерти при спазване на правилника за дейността на управителния съвет.

6. Агенцията осигурява секретариата на управителния съвет.

Член 17

Правила за гласуване в управителния съвет

1. Управителният съвет взема решенията си с мнозинство на членовете си.
2. Мнозинство от две трети от всички членове на управителния съвет се изисква за единния програмен документ, годишния бюджет, назначаването, удължаването на мандата или освобождаването от длъжност на изпълнителния директор.
3. Всеки член има един глас. При отсъствие на даден член заместникът му упражнява неговото право на глас.
4. Председателят участва в гласуването.
5. Изпълнителният директор не участва в гласуването.
6. Правилникът за дейността на управителния съвет определя по-подробно условията и реда за гласуване, по-специално условията, при които даден член може да действа от името на друг член.

РАЗДЕЛ 2
ИЗПЪЛНИТЕЛЕН СЪВЕТ

Член 18

Изпълнителен съвет

1. Управителният съвет се подпомага от изпълнителен съвет.
2. Изпълнителният съвет:
   а) подготвя решенията, които трябва да бъдат приети от управителния съвет;
   б) заедно с управителния съвет осигурява подходящи мерки за съобразяване с резултатите и препоръките от разследванията на OLAF и различните вътрешни и външни одитни доклади и оценки;
   в) без да се засягат отговорностите на изпълнителния директор, определени в член 19, подпомага и съветва изпълнителния директор при изпълнението на решенията на управителния съвет по административни и бюджетни въпроси съгласно член 19.
3. Изпълнителният съвет се състои от петима членове, назначени измежду членовете на управителния съвет, като един от тях е председателят на управителния съвет, който може също така да бъде председател на изпълнителния съвет, и един от представителите на Комисията. Изпълнителният директор взима участие в заседанията на изпълнителния съвет, но няма право на глас.
4. Мандатът на членовете на изпълнителния съвет е четири години. Този мандат подлежи на подновяване.
5. Изпълнителният съвет заседава най-малко веднъж на всеки три месеца. Председателят на изпълнителния съвет свиква допълнителни заседания по искане на членовете на съвета.

6. Управителният съвет установява правилника за дейността на изпълнителния съвет.

7. Когато е необходимо при спешни случаи Изпълнителният съвет може да приема временни решения от името на Управителния съвет, особено по въпроси на административното управление, включително за оттегляне на делегираните правомощия на орган по назначаването и в областта на бюджета.

РАЗДЕЛ 3
ИЗПЪЛНИТЕЛЕН ДИРЕКТОР

Член 19

Отговорности на изпълнителния директор

1. Агенцията се ръководи от изпълнителен директор, който е независим при изпълнението на своите задължения. Изпълнителният директор отговаря пред управителния съвет.

2. Изпълнителният директор докладва на Европейския парламент относно изпълнението на своите задължения, когато бъде поканен да направи това. Съветът може да покани изпълнителния директор да докладва за изпълнението на своите задължения.

3. Изпълнителният директор отговаря за:

   а) текущото управление на Агенцията;

   б) изпълнението на решенията, приети от управителния съвет;

   в) изготвянето на проекта на единния програмен документ и предаването му на управителния съвет за одобрение преди представянето му на Комисията;

   г) изпълнението на единния програмен документ и докладването пред управителния съвет за неговото изпълнение;

   д) изготвянето на консолидирания годишен доклад за дейностите на Агенцията и представянето му на управителния съвет за оценка и приемане;

   е) изготвянето на план за действие за съобразяване със заключенията от оценки за изминал период, и докладване за напредъка на всеки две години пред Комисията;

   ж) изготвянето на план за последващи действия във връзка със заключенията от вътрешните или външните одитни доклади и оценки, както и от разследвания на Европейската служба за борба с измамите (OLAF), представянето на доклади за напредъка два пъти годишно на Комисията и редовно на управителния съвет;

   з) изготвянето на проект за финансовите правила, приложими по отношение на Агенцията;

   и) изготвянето на проекта на декларация за разчета на приходите и разходите на Агенцията и изпълнението на нейния бюджет;

й) защитата на финансовите интереси на Съюза чрез прилагането на превантивни мерки срещу измами, корупция и всякакви други незаконни дейности, посредством ефективни проверки и, при наличие на нередности, чрез събирането на недължимо платените суми, а също така, когато това е целесъобразно, чрез ефективни, съразмерни и възпиращи административни и финансови санкции;

к) изготвянето на стратегия на Агенцията за борба с измамите и представянето ѝ на управителния съвет за одобрение;

л) установяването и поддържането на контакт с бизнес общността и потребителските организации с цел осигуряване на редовен диалог със съответните заинтересовани страни;

м) други задачи, възложени на изпълнителния директор с настоящия регламент.

4. При необходимост, в рамките на мандата на Агенцията и в съответствие с нейните цели и задачи, изпълнителният директор може да сформира ad hoc работни групи, съставени от експерти, включително от компетентните органи на държавите членки. Управителният съвет се информира предварително за това. Процедурите, по-специално относно състава на работните групи, назначаването на експертите от изпълнителния директор и дейността на ad hoc работните групи, се определят във вътрешния правилник за дейността на Агенцията.

5. Изпълнителният директор решава дали за целите на ефективното и ефикасно изпълнение на задачите на Агенцията е необходимо нейни служители да бъдат разположени в една или повече държави членки. Преди да вземе решение за установяване на местен офис, изпълнителният директор получава предварителното съгласие на Комисията, управителния съвет и съответната(те) държава(и) членка(и). В решението се уточнява обхватът на дейностите, които ще се извършват в местния офис, така че да се избегнат ненужни разходи и дублиране на административни функции на Агенцията. Където е уместно или необходимо, се постига споразумение със съответните държави членки.

РАЗДЕЛ 4
ПОСТОЯННА ГРУПА НА ЗАИНТЕРЕСОВАНИТЕ СТРАНИ

Член 20

Постоянна група на заинтересованите страни

1. По предложение на изпълнителния директор управителният съвет учредява Постоянна група на заинтересовани страни, съставена от доказани експерти, представляващи съответните заинтересовани страни, например отрасъла на ИКТ, доставчиците на обществени електронни съобщителни мрежи или услуги, потребителски групи, академични експерти в областта на киберсигурността и представители на компетентните органи, нотифицирани съгласно [Директивата за установяване на Европейски кодекс за електронни съобщения], както и правоприлагащите органи и надзорните органи за защита на данните.

2. Процедурите за Постоянната група на заинтересованите страни, и по-специално тези относно броя, състава, назначаването на членовете от управителния съвет, предложението на изпълнителния директор и дейността на групата, се определят във вътрешния правилник за дейността на Агенцията и се публикуват.

3. Постоянната група на заинтересованите страни се председателства от изпълнителния директор или лице, определено от изпълнителния директор за всеки конкретен случай.

4. Мандатът на членовете на Постоянната група на заинтересованите страни е с продължителност две години и половина. Членовете на управителния съвет не могат да бъдат членове на Постоянната група на заинтересованите страни. Експертите на Комисията и от държавите членки имат право да присъстват на заседанията на Постоянната група на заинтересованите страни и да участват в нейната работа. Представители на други органи, които не са членове на Постоянната група на заинтересованите страни, но които изпълнителният директор счита за подходящи, могат да бъдат поканени да присъстват на заседанията на Постоянната група на заинтересованите страни и да участват в работата ѝ.

5. Постоянната група на заинтересованите страни консултира Агенцията при изпълнението на нейните дейности. По-специално тя консултира изпълнителния директор относно изготвянето на предложение за работна програма на Агенцията и гарантирането на диалог със съответните заинтересовани страни по всички въпроси, свързани с работната програма.

РАЗДЕЛ 5
ДЕЙНОСТ

Член 21
Единен програмен документ

1. Агенцията извършва дейността си в съответствие със единен програмен документ, който съдържа многогодишната и едногодишната програма, включващи всички планирани дейности.

2. Всяка година изпълнителният директор изготвя проект на единен програмен документ, който съдържа годишно и многогодишно програмиране на съответните човешки и финансови ресурси съгласно член 32 от Делегиран регламент (ЕС) № 1271/2013 на Комисията[36], като взема предвид насоките на Комисията.

3. До 30 ноември всяка година управителният съвет приема единния програмен документ, посочен в параграф 1, и го изпраща на Европейския парламент,

---

36 Делегиран регламент (ЕС) № 1271/2013 на Комисията от 30 септември 2013 г. относно рамковия Финансов регламент за органите, посочени в член 208 от Регламент (ЕС, Евратом) № 966/2012 на Европейския парламент и на Съвета (ОВ L 328, 7.12.2013 г., стр. 42).

Съвета и Комисията не по-късно от 31 януари следващата година, както и всички следващи актуализирани варианти на този документ.

4. Единният програмен документ става окончателен след окончателното приемане на общия бюджет на Съюза и, ако е необходимо, съответно се коригира.

5. Годишната работна програма включва подробни цели и очаквани резултати, включително показатели за изпълнение. В нея също така са описани действията, които ще се финансират, и са посочени финансовите и човешките ресурси, разпределени за всяко действие, в съответствие с принципите за бюджетиране и управление по дейности. Годишната работна програма е съгласувана с многогодишната работна програма, посочена в параграф 7. В годишната работна програма се посочват ясно добавените, променените или отменените задачи в сравнение с предходната финансова година.

6. Управителният съвет внася изменения в приетата годишна работна програма, когато на Агенцията бъде възложена нова задача. Всяко съществено изменение на годишната работна програма се приема по същата процедура като първоначалната годишна работна програма. Управителният съвет може да делегира на изпълнителния директор правомощие за внасяне на несъществени изменения в годишната работна програма.

7. В многогодишната работна програма е определен общият стратегически план, включително целите, очакваните резултати и показателите за изпълнението. В нея се съдържа също програмирането на ресурсите, включително на многогодишния бюджет и персонала.

8. Програмирането на ресурсите се актуализира ежегодно. Стратегическото програмиране се актуализира по целесъобразност, и по-специално в отговор на резултата от оценката, посочена в член 56.

Член 22

Деклариране на интерес

1. Членовете на управителния съвет, изпълнителният директор и длъжностните лица, временно командировани от държавите членки, представят декларация за ангажираност и декларация за липса или наличие на преки или косвени интереси, които биха могли да се считат за накърняващи тяхната независимост. Тези декларации са точни и изчерпателни, правят се писмено всяка година и се актуализират при необходимост.

2. Членовете на управителния съвет, изпълнителният директор и външните експерти, участващи в ad hoc работни групи, декларират точно и изчерпателно най-късно в началото на всяко заседание наличието на интереси, които биха могли да се считат за засягащи тяхната независимост по отношение на точките в дневния ред, и се въздържат от участие в обсъждането на тези точки и гласуването по тях.

3. Агенцията установява във вътрешния правилник за дейността си практическите ред и условия за прилагане на правилата за деклариране на интереси, посочени в параграфи 1 и 2.

Член 23

Прозрачност

1. Агенцията осъществява дейността си при високо ниво на прозрачност и в съответствие с член 25.

2. Агенцията гарантира, че на обществеността и на заинтересованите страни се предоставя целесъобразна, обективна, достоверна и леснодостъпна информация, по-специално по отношение на резултатите от нейната дейност. Освен това тя оповестява публично декларациите за интереси, направени в съответствие с член 22.

3. По предложение на изпълнителния директор управителният съвет може да разреши на заинтересовани страни да наблюдават хода на някои от дейностите на Агенцията.

4. Агенцията установява във вътрешния правилник за дейността си практическите ред и условия за прилагане на правилата на прозрачност, посочени в параграфи 1 и 2.

Член 24

Поверителност

1. Без да се засяга член 25, Агенцията няма право да разкрива на трети страни информация, която обработва или получава, за която е отправено обосновано искане за поверително цялостно или частично обработване.

2. Членовете на управителния съвет, изпълнителният директор, членовете на Постоянната група на заинтересовани страни, участващите в работните ad hoc групи външни експерти и членовете на персонала на Агенцията, включително временно командированите от държавите членки длъжностни лица, са задължени да спазват изискванията за поверителност съгласно член 339 от Договора за функционирането на Европейския съюз (ДФЕС), дори и след приключване на службата им.

3. Агенцията установява във вътрешния правилник за дейността си практическите ред и условия за прилагане на правилата на поверителност, посочени в параграфи 1 и 2.

4. Ако това се изисква за изпълнението на задачите на Агенцията, управителният съвет решава да позволи на Агенцията да работи с класифицирана информация. В такъв случай управителният съвет, със съгласието на службите на Комисията, приема вътрешен правилник за дейността, като прилага принципите на сигурността, установени в решения (ЕС, Евратом) 2015/443[37] и 2015/444[38] на Комисията. Посоченият правилник включва разпоредби за обмена, обработката и съхранението на класифицирана информация.

---

37 Решение (ЕС, Евратом) 2015/443 на Комисията от 13 март 2015 г. относно сигурността в Комисията (ОВ L 72, 17.3.2015 г., стр. 41).

38 Решение (ЕС, Евратом) 2015/444 на Комисията от 13 март 2015 г. относно правилата за сигурност за защита на класифицираната информация на ЕС (ОВ L 72, 17.3.2015 г., стр. 53).

Член 25

Достъп до документи

1. Регламент (ЕО) № 1049/2001 се прилага за документи, притежавани от Агенцията.

2. Управителният съвет приема реда за прилагането на Регламент (ЕО) № 1049/2001 в срок до шест месеца от създаването на Агенцията.

3. Срещу решенията, взети от Агенцията съгласно член 8 от Регламент (ЕО) № 1049/2001, може да се подава жалба до омбудсмана по реда и при условията на член 228 от ДФЕС или те може да се обжалват пред Съда на Европейския съюз по реда и при условията на член 263 от ДФЕС.

ГЛАВА III
СЪСТАВЯНЕ И УСТРОЙСТВО НА БЮДЖЕТА

Член 26

Съставяне на бюджета

1. Всяка година изпълнителният директор изготвя проект на разчета за предвидените приходи и разходи на Агенцията за следващата финансова година и го изпраща на управителния съвет заедно с проект на щатно разписание. Приходите и разходите са балансирани.

2. Въз основа на проекта на разчета за предвидените приходи и разходи, посочен в параграф 1, управителният съвет ежегодно изготвя разчет за предвидените приходи и разходи на Агенцията за следващата финансова година.

3. До 31 януари всяка година управителният съвет изпраща разчета за предвидените средства, посочен в параграф 2, който е част от проекта на единен програмен документ, на Комисията и на третите държави, с които Европейският съюз е сключил споразумения в съответствие с член 39.

4. Въз основа на този разчет Комисията включва в проекта за бюджет на Съюза прогнозните средства, които прецени за необходими за щатното разписание, и размера на вноската, която се заделя от общия бюджет, и ги представя на Европейския парламент и на Съвета в съответствие с членове 313 и 314 от ДФЕС.

5. Европейският парламент и Съветът разрешават отпускане на бюджетни кредити за вноската в Агенцията.

6. Европейският парламент и Съветът приемат щатното разписание на Агенцията.

7. Заедно с единния програмен документ управителният съвет приема бюджета на Агенцията. Той става окончателен след окончателното приемане на общия бюджет на Съюза. Когато е уместно, управителният съвет коригира бюджета и единния програмен документ на Агенцията в съответствие с общия бюджет на Съюза.

Член 27

Устройство на бюджета

1. Без да се засягат други ресурси, приходите на Агенцията включват:

   а) вноска от бюджета на Съюза;

   б) приходи, заделени за финансиране на определени разходи съгласно финансовите правила, посочени в член 29;

   в) финансиране от Съюза под формата на споразумения за делегиране или ad hoc безвъзмездни средства в съответствие с нейните финансови правила, посочени в член 29, и с разпоредбите на съответните инструменти за подкрепа на политиките на Съюза;

   г) вноски от трети държави, участващи в работата на Агенцията, както е предвидено в член 39;

   д) всякакви доброволни парични или непарични вноски от държавите членки. Държавите членки, осигуряващи доброволни вноски, не могат да предявяват претенции за особени права или услуги в резултат от тези вноски.

2. Разходите на Агенцията се състоят от разходи за персонал, административна и техническа поддръжка, разходи за инфраструктура и оперативни разходи, както и разходи в резултат от договори, сключени с трети страни.

Член 28

Изпълнение на бюджета

1. Изпълнителният директор отговаря за изпълнението на бюджета на Агенцията.

2. Вътрешният одитен орган на Комисията се ползва със същите правомощия спрямо Агенцията като тези спрямо отделите на Комисията.

3. До 1 март на следващата финансова година (1 март на година N + 1) счетоводителят на Агенцията изпраща междинния счетоводен отчет на счетоводителя на Комисията и на Сметната палата.

4. След като получи забележките на Сметната палата по междинния счетоводен отчет, счетоводителят на Агенцията изготвя на своя отговорност нейния окончателен счетоводен отчет.

5. Изпълнителният директор изпраща окончателния счетоводен отчет на управителния съвет за становище.

6. До 31 март на година N + 1, изпълнителният директор изпраща доклада за бюджетното и финансовото управление до Европейския парламент, Съвета, Комисията и Сметната палата.

7. До 1 юли на година N + 1 счетоводителят изпраща окончателния счетоводен отчет заедно със становището на управителния съвет до Европейския парламент, Съвета, счетоводителя на Комисията и до Сметната палата.

8. В деня на предаване на окончателния си счетоводен отчет счетоводителят също така изпраща на Сметната палата представително писмо относно окончателния отчет с копие до счетоводителя на Комисията.

9. Изпълнителният директор публикува окончателния счетоводен отчет до 15 ноември на следващата година.

10. Изпълнителният директор изпраща на Сметната палата отговор на нейните констатации в срок до 30 септември на година N + 1, с копие до управителния съвет и до Комисията.

11. Изпълнителният директор представя на Европейския парламент по искане на последния цялата информация, необходима за безпрепятственото изпълнение на процедурата по освобождаване от отговорност за въпросната финансова година, както е предвидено в член 165, параграф 3 от Финансовия регламент.

12. До 15 май на година N + 2 по препоръка на Съвета Европейският парламент освобождава изпълнителния директор от отговорност по отношение на изпълнението на бюджета за година N.

Член 29

Финансови правила

Финансовите правила, приложими за Агенцията, се приемат от управителния съвет след консултация с Комисията. Те не се отклоняват от Регламент (ЕС) № 1271/2013, освен ако специфичните изисквания за функционирането на Агенцията го налагат и ако Комисията е дала предварителното си съгласие.

Член 30

Борба с измамите

1. За улесняване на борбата с измамите, корупцията и други неправомерни дейности в рамките на Регламент (ЕС, Евратом) № 883/2013 на Европейския парламент и на Съвета[39], в срок от шест месеца от деня на започване на дейността си Агенцията се присъединява към Междуинституционалното споразумение от 25 май 1999 г. относно вътрешните разследвания от Европейската служба за борба с измамите (OLAF) и приема съответните разпоредби, приложими по отношение на всички служители на Агенцията, като използва образеца в приложението към посоченото споразумение.

2. Сметната палата на Европейския съюз има правомощия за извършване на одити по документи и на място на всички бенефициери на безвъзмездни средства, изпълнители и подизпълнители, които са получили средства от Съюза чрез Агенцията.

3. OLAF може да извършва разследвания, включително проверки и инспекции на място, в съответствие с разпоредбите и процедурите, предвидени в Регламент (ЕС, Евратом) № 883/2013 на Европейския парламент и на Съвета и Регламент (Евратом, ЕО) № 2185/96 на Съвета[40] от 11 ноември 1996 г. относно контрола и проверките на място, извършвани от Комисията за защита на финансовите

---

39 Регламент (ЕС, Евратом) № 883/2013 на Европейския парламент и на Съвета от 11 септември 2013 година относно разследванията, провеждани от Европейската служба за борба с измамите (OLAF), и за отмяна на Регламент (ЕО) № 1073/1999 на Европейския парламент и на Съвета и Регламент (Евратом) № 1074/1999 на Съвета (ОВ L 248, 18.9.2013 г., стр. 1).

40 Регламент (Евратом, ЕО) № 2185/96 на Съвета от 11 ноември 1996 г. относно контрола и проверките на място, извършвани от Комисията за защита на финансовите интереси на Европейските общности срещу измами и други нередности (ОВ L 292, 15.11.1996 г., стр. 2).

интереси на Европейския съюз срещу измами и други нередности, с цел да се установи дали е налице измама, корупция или друга незаконна дейност, накърняваща финансовите интереси на Съюза, във връзка с безвъзмездни средства или поръчка, финансирани от Агенцията.

4. Без да се засягат параграфи 1, 2 и 3, споразуменията за сътрудничество с трети държави и международни организации, договорите, споразуменията и решенията на Агенцията за отпускане на безвъзмездни средства съдържат разпоредби, с които Сметната палата и OLAF изрично се упълномощават да провеждат такива одити и разследвания съгласно съответните техни компетенции.

ГЛАВА IV
ПЕРСОНАЛ НА АГЕНЦИЯТА

Член 31
Общи разпоредби

Правилникът за длъжностните лица и Условията за работа на другите служители, както и правилата за прилагането им, приети чрез споразумение между институциите на Съюза, се прилагат за персонала на Агенцията.

Член 32
Привилегии и имунитет

Протокол № 7 за привилегиите и имунитетите на Европейския съюз, приложен към Договора за Европейския съюз и към ДФЕС, се прилага за Агенцията и нейния персонал.

Член 33
Изпълнителен директор

1. Изпълнителният директор се назначава като срочно нает служител на Агенцията съгласно член 2, буква а) от Условията за работа на другите служители.

2. Изпълнителният директор се назначава от управителния съвет от списък с кандидати, предложен от Комисията, след открита и прозрачна процедура по подбор.

3. За целите на сключването на договора на изпълнителния директор Агенцията се представлява от председателя на управителния съвет.

4. Преди назначаването избраният от управителния съвет кандидат се поканва да направи изявление пред съответната комисия на Европейския парламент и да отговори на въпроси на членовете.

5. Мандатът на изпълнителния директор е пет години. Към края на този период Комисията извършва оценка, която взема предвид оценката на работата на изпълнителния директор и бъдещите цели и предизвикателства пред Агенцията.

6. Управителният съвет взема решения относно назначаването, удължаването на мандата и освобождаването от длъжност на изпълнителния директор с мнозинство от две трети от своите членове с право глас.

7. По предложение на Комисията, което взема предвид оценката, посочена в параграф 5, управителният съвет може еднократно да удължи мандата на изпълнителния директор с не повече от пет години.

8. Управителният съвет уведомява Европейския парламент за намерението си да удължи мандата на изпълнителния директор. Най-късно три месеца преди такова удължаване изпълнителният директор, ако бъде поканен, прави изявление пред съответната комисия на Европейския парламент и отговаря на въпроси на членовете.

9. Изпълнителен директор, чийто мандат е бил удължен, не може да участва в нова процедура за подбор за същата длъжност.

10. Изпълнителният директор може да бъде отстранен от длъжност единствено с решение на управителния съвет по предложение на Комисията.

Член 34

Командировани национални експерти и друг персонал

1. Агенцията може да използва командировани национални експерти или друг персонал, който не е нает от Агенцията. Правилникът за длъжностните лица и Условията за работа на другите служители не се прилагат за такъв персонал.

2. Управителният съвет приема решение за определяне на правилата относно командироването на национални експерти в Агенцията.

ГЛАВА V
ОБЩИ РАЗПОРЕДБИ

Член 35

Юридически статут на Агенцията

1. Агенцията е орган на Съюза и притежава правосубектност.

2. Във всяка държава членка Агенцията се ползва с най-широката правоспособност, предоставяна на юридически лица съгласно националното законодателство. По-специално тя може да придобива или да се разпорежда с движимо и недвижимо имущество и да бъде страна по съдебни производства, или и двете.

3. Агенцията се представлява от нейния изпълнителен директор.

Член 36

Отговорност на Агенцията

1. Договорната отговорност на Агенцията се урежда от правото, приложимо към съответния договор.

2. Съдът на Европейския съюз е компетентен да се произнася с решение на основание на арбитражна клауза, съдържаща се в сключен от Агенцията договор.

3. В случай на извъндоговорна отговорност, съгласно общите принципи, общи за правните системи на държавите членки, Агенцията поправя всяка вреда, причинена от нея или от нейните служители при изпълнението на техните задължения.

4. Съдът на Европейския съюз е компетентен по отношение на всякакви спорове, отнасящи се до поправянето на такива вреди.

5. По отношение на личната отговорност на служителите спрямо Агенцията се прилагат съответните условия, приложими по отношение на служителите на Агенцията.

Член 37

Езиков режим

1. Към Агенцията се прилага Регламент № 1 на Съвета[41]. Държавите членки и другите органи, определени от тях, могат да се обръщат към Агенцията и да получават отговор на избран от тях официален език на институциите на Съюза.

2. Преводаческите услуги, необходими за функционирането на Агенцията, се предоставят от Центъра за преводи за органите на Европейския съюз.

Член 38

Защита на личните данни

1. При обработката на лични данни от Агенцията се прилагат разпоредбите на Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета[42].

2. Управителният съвет приема мерките по прилагане, посочени в член 24, параграф 8 от Регламент (ЕО) № 45/2001. Управителният съвет може да приеме допълнителни мерки, необходими за прилагането на Регламент (ЕО) № 45/2001 от Агенцията.

Член 39

Сътрудничество с трети държави и международни организации

1. Доколкото е необходимо за постигането на целите, посочени в настоящия регламент, Агенцията може да си сътрудничи с компетентните органи на трети държави или с международни организации, или и двете. За тази цел след предварително одобрение от Комисията Агенцията може да установява работни договорености с органите на трети държави и с международни организации. Тези договорености не създават правни задължения за Съюза и неговите държави членки.

---

41 Регламент № 1 за определяне на езиковия режим на Европейската икономическа общност (ОВ 17, 6.10.1958 г., стр. 401).

42 Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни (ОВ L 8, 12.1.2001 г., стр. 1).

2. Агенцията е отворена за участие на трети държави, които са сключили споразумения със Съюза за тази цел. Съгласно съответните разпоредби на тези споразумения се постигат договорености, уточняващи по-специално естеството, степента и начина на участие на тези държави в работата на Агенцията, включително разпоредби, свързани с участието в инициативите, предприемани от Агенцията, финансовите вноски и персонала. По въпросите, свързани с персонала, при всички случаи посочените договорености са в съответствие с Правилника за длъжностните лица.

3. Управителният съвет приема стратегия за отношенията с трети държави или международни организации, отнасящи се до въпроси от компетентността на Агенцията. Комисията гарантира, че Агенцията действа в обхвата на своя мандат и съществуващата институционална рамка посредством сключване на подходяща работна договореност с изпълнителния директор.

Член 40

Правила за сигурност за защита на класифицирана информация и на чувствителна некласифицирана информация

Като се консултира с Комисията, Агенцията приема свои правила за сигурност, прилагайки принципите, залегнали в правилата за сигурност на Комисията за защита на класифицирана информация на Европейския съюз и на чувствителна некласифицирана информация, както е посочено в Решения (ЕС, Евратом) 2015/443 и 2015/444 на Комисията. Това обхваща, наред с другото, разпоредби за обмена, обработката и съхранението на такава информация.

Член 41

Споразумение за седалището и условия за дейността

1. Необходимите разпоредби за установяването на Агенцията в приемащата държава членка и за съоръженията, които трябва да бъдат предоставени от тази държава, както и конкретните правила, приложими в приемащата държава членка по отношение на изпълнителния директор, членовете на управителния съвет, персонала на Агенцията и членовете на семействата им, се определят в споразумение за седалището между Агенцията и държавата членка, в която се намира седалището, като това споразумение се сключва след одобрение от управителния съвет и не по-късно от [2 години след влизането в сила на настоящия регламент].

2. Приемащата Агенцията държава членка предоставя най-добрите възможни условия за гарантиране на правилното функциониране на Агенцията, включително на достъпност на мястото, наличие на съответната учебна инфраструктура за децата на служителите, подходящ достъп до пазара на труда, социално осигуряване и медицински услуги както за децата, така и за съпрузите.

Член 42

Административен контрол

Дейността на Агенцията подлежи на надзор от омбудсмана в съответствие с член 228 от ДФЕС.

ДЯЛ III
РАМКА ЗА СЕРТИФИЦИРАНЕ НА КИБЕРСИГУРНОСТТА

Член 43

Европейски схеми за сертифициране на киберсигурността

Дадена европейска схема за сертифициране на киберсигурността удостоверява, че ИКТ продуктите и услугите, които са били сертифицирани в съответствие с такава схема, отговарят на определени изисквания по отношение на тяхната способност да устояват, при определено ниво на обезпечаване, на действия, целящи да се компрометира наличността, автентичността, целостта или поверителността на съхраняваните, предавани или обработвани данни, или на функциите и услугите, предлагани или направени достъпни чрез тези продукти, процеси, услуги и системи.

Член 44

Изготвяне и приемане на Европейска схема за сертифициране на киберсигурността

1. По искане на Комисията ENISA изготвя проект за европейска схема за сертифициране на киберсигурността, която отговаря на изискванията на членове 45, 46 и 47 от настоящия регламент. Държавите членки или Европейската група за сертифициране на киберсигурността („групата“), създадена съгласно член 53, може да предложат на Комисията изготвянето на проект за европейска схема за сертифициране на киберсигурността.

2. При подготовката на проектите за схеми, посочени в параграф 1 от настоящия член, ENISA провежда консултации с всички съответни заинтересовани страни и си сътрудничи тясно с групата. Групата предоставя на ENISA съдействие и експертни консултации, необходими на Агенцията във връзка с изготвянето на проекта за схема, включително и становища, когато е необходимо.

3. ENISA предава подготвения съгласно параграф 2 от настоящия член проект за европейска схема за сертифициране на киберсигурността на Комисията.

4. На основата на проекта за схема, предложен от ENISA, Комисията може да приема актове за изпълнение съгласно член 55, параграф 2, с които осигурява европейски схеми за сертифициране на киберсигурността за ИКТ продукти и услуги, отговарящи на изискванията по членове 45, 46 и 47 от настоящия регламент.

5. ENISA поддържа специален уебсайт, на който предоставя информация и популяризира европейските схеми за сертифициране на киберсигурността.

Член 45

Цели за сигурност на европейските схеми за сертифициране на киберсигурността

Европейските схеми за сертифициране на киберсигурността се проектират така, че да вземат предвид, според нуждите, следните цели за сигурност:

а) да се защитават съхраняваните, предавани или обработвани по друг начин данни от случайно или неразрешено съхраняване, обработване, достъп или разкриване;

б) да се защитават съхраняваните, предавани или обработвани по друг начин данни от случайно или неразрешено унищожаване, случайна загуба или промяна;

в) да се гарантира, че единствено оправомощени лица, програми или машини имат достъп до данните, услугите или функциите, за които се отнася правото им на достъп;

г) да се регистрира кои данни, функции или услуги са били предадени, кога и от кого;

д) да се гарантира, че е възможно да се провери до кои данни, услуги или функции е имало достъп или са били използвани, кога и от кого;

е) да се възстановяват своевременно наличието и достъпът до данни, услуги и функции в случай на физически или технически инцидент;

ж) да се гарантира, че ИКТ продуктите и услугите се предоставят с актуален софтуер, който няма известни към момента уязвими точки, и че са осигурени механизми за безопасни софтуерни актуализации.

Член 46

Нива на обезпеченост на европейските схеми за сертифициране на киберсигурността

1. Европейските схеми за сертифициране на киберсигурността могат да посочват едно или повече от следните нива на обезпечаване на сигурност: основно, значително и/или високо, за ИКТ продукти и услуги, сертифицирани по тази схема.

2. Нивата „основно“, „значително“ и „високо“ отговарят съответно на следните критерии:

а) основното ниво на обезпеченост се отнася до сертификат, издаден по европейска схема за сертифициране на киберсигурността, който предоставя ограничена степен на увереност в декларираните качества на ИКТ продукт или услуга по отношение на киберсигурността и се характеризира с препратка към технически спецификации, стандарти и процедури, свързани с нея, включително технически проверки, чиято цел е да се намали рискът от киберинциденти;

б) значителното ниво на обезпеченост се отнася до сертификат, издаден по европейска схема за сертифициране на киберсигурността, който предоставя значителна степен на увереност в декларираните качества на ИКТ продукт или услуга по отношение на киберсигурността и се характеризира с препратка към технически спецификации, стандарти и процедури, свързани с нея, включително технически проверки, чиято цел е да се намали съществено рискът от киберинциденти;

в) високото ниво на обезпеченост се отнася до сертификат, издаден по европейска схема за сертифициране на киберсигурността, който предоставя по-висока степен на увереност в декларираните качества на

ИКТ продукт или услуга по отношение на киберсигурността в сравнение със сертификатите със значително ниво на обезпеченост и се характеризира с препратка към технически спецификации, стандарти и процедури, свързани с нея, включително технически проверки, чиято цел е да се предотвратят киберинциденти.

Член 47

Елементи на европейските схеми за сертифициране на киберсигурността

1. Европейските схеми за сертифициране на киберсигурността включват следните елементи:

   а) предмет и обхват на сертифицирането, включително вида или категориите ИКТ продукти и услуги, обхванати от него;

   б) подробна спецификация на изискванията за киберсигурност, по които се оценяват конкретните ИКТ продукти и услуги, например чрез позоваване на международни стандарти или технически спецификации или стандарти и спецификации на Съюза;

   в) когато е уместно, едно или повече нива на обезпечаване на сигурност;

   г) конкретните критерии и методи за оценка (включително типовете оценки), използвани с цел да се докаже постигането на конкретните цели, посочени в член 45;

   д) необходимата за сертифициране информация, която кандидатът трябва да предостави на органите за оценяване на съответствието;

   е) когато схемата предвижда маркировки или етикети — условията, при които те могат да бъдат използвани;

   ж) когато надзорът е част от схемата — правила за наблюдение на съответствието на сертификатите с изискванията, включително механизми за удостоверяване на трайното съответствие с определените изисквания на киберсигурността;

   з) условия за предоставяне, поддържане, продължаване, разширяване и стесняване на обхвата на сертифицирането;

   и) правила за последиците от несъответствието на сертифицирани ИКТ продукти и услуги с изискванията за сертифициране;

   й) правила за начина, по който неоткрити до момента уязвими точки на киберсигурността на ИКТ продукти и услуги трябва да се докладват и отстраняват;

   к) правила за съхраняването на документация от органите за оценяване на съответствието;

   л) списък на националните схеми за сертифициране на киберсигурността, които обхващат същия тип или категории ИКТ продукти и услуги;

   м) съдържанието на издадения сертификат.

2. Определените изисквания на схемата не противоречат на никои приложими правни изисквания, по-специално на изискванията, произтичащи от хармонизираното законодателство на ЕС.

3. Когато това е предвидено в конкретен акт на Съюза, сертифицирането по европейска схема за сертифициране на киберсигурността може да се използва за удостоверяване на презумпцията за съответствие с изискванията на посочения акт.

4. При липса на хармонизирани правни актове на Съюза в законодателството на държавата членка може да се предвиди също така, че дадена европейска схема за сертифициране на киберсигурността може да се използва за установяване на презумпцията за съответствие с правните изисквания.

Член 48

Сертифициране на киберсигурността

1. ИКТ продуктите и услугите, сертифицирани по европейска схема за сертифициране на киберсигурността, приета съгласно член 44, по презумпция се приемат за съответстващи на изискванията на такава схема.

2. Сертифицирането е доброволно, освен ако не е посочено друго в законодателството на Съюза.

3. Европейски сертификат за киберсигурност по силата на настоящия член се издава от органите за оценяване на съответствието, посочени в член 51, на основата на критерии, включени в европейската схема за сертифициране на киберсигурността, приета съгласно член 44.

4. Чрез дерогация от параграф 3 в надлежно обосновани случаи дадена европейска схема за сертифициране на киберсигурността може да предвиди, че европейски сертификат за киберсигурност в резултат от тази схема може да бъде издаден само от публичен орган. Такъв публичен орган е един от следните:

   а) национален надзорен орган по сертифицирането, посочен в член 50, параграф 1;

   б) орган, акредитиран като орган за оценяване на съответствието съгласно член 51, параграф 1, или

   в) орган, създаден по силата на закони, нормативни актове, или други официални административни процедури на съответната държава членка, които отговарят на изискванията за органи, които сертифицират продукти, процеси или услуги по ISO/IEC 17065:2012.

5. Физическото или юридическото лице, което подлага своите ИКТ продукти или услуги на процедурите за сертифициране, предоставя на органа за оценяване на съответствието, посочен в член 51, цялата необходима информация за провеждане на процедурата по сертифициране.

6. Сертификатите се издават за максимален срок от три години и могат да бъдат подновени при същите условия, ако съответните изисквания продължават да се изпълняват.

7. Европейски сертификат за киберсигурност, издаден съгласно настоящия член, се признава във всички държави членки.

Член 49

Национални сертификати и схеми за сертифициране на киберсигурността

1. Без да се засягат разпоредбите на параграф 3, националните схеми за сертифициране на киберсигурността и свързаните с тях процедури за ИКТ продукти и услуги, обхванати от европейска схема за сертифициране на киберсигурността, прекратяват правното си действие от датата, посочена в акта за изпълнение, приет съгласно член 44, параграф 4. Действащите национални схеми за сертифициране на киберсигурността и свързаните с тях процедури за ИКТ продукти и услуги, обхванати от европейска схема за сертифициране на киберсигурността, продължават да съществуват.
2. Държавите членки не въвеждат нови национални схеми за сертифициране на киберсигурността на ИКТ продукти и услуги, обхванати от съществуваща европейска схема за сертифициране на киберсигурността.
3. Съществуващите сертификати, издадени по силата на националните схеми за сертифициране на киберсигурността, остават в сила до изтичането си.

Член 50

Национални надзорни органи за сертифицирането

1. Всяка държава членка определя национален надзорен орган за сертифицирането.
2. Всяка държава членка уведомява Комисията за наименованието на определения надзорен орган.
3. Всеки национален надзорен орган за сертифицирането е независим от субектите, върху които упражнява надзор, по отношение на своята организация, решения за финансиране, правна структура и процес вземане на решения.
4. Държавите членки гарантират, че националните надзорни органи за сертифицирането разполагат с достатъчно ресурси за упражняване на правомощията си и ефективно изпълнение на възложените им задачи.
5. За ефективното изпълнение на регламента е целесъобразно тези органи да участват активно, реално и съобразно правилата за поверителност в Европейската група за сертифициране на киберсигурността, създадена по силата на член 53.
6. Националните надзорни органи за сертифицирането:

   а) наблюдават и осигуряват прилагането на разпоредбите на настоящия дял и упражняват надзор върху съответствието на сертификатите, издадени от органите за оценяване на съответствието, установени на тяхна територия, с изискванията, определени в настоящия дял и в съответната европейска схема за сертифициране на киберсигурността;

   б) наблюдават и упражняват надзор върху дейностите на органите за оценяване на съответствието за целите на настоящия регламент, включително по отношение на уведомленията за органите и съответните задачи, определени в член 52 от настоящия регламент;

в) разглеждат жалбите, внесени от физически или юридически лица във връзка със сертификати, издадени от органите за оценяване на съответствието на техните територии, разследват жалбите по същество, доколкото е необходимо, и информират жалбоподателя за напредъка и резултатите от разследването в разумен срок;

г) сътрудничат си с други национални надзорни органи за сертифицирането или други публични органи, включително чрез споделяне на информация за възможни несъответствия на ИКТ продукти и услуги с изискванията на настоящия регламент или с конкретни европейски схеми за сертифициране на киберсигурността.

д) наблюдават промените в областта на сертифицирането на киберсигурността.

7. Всеки национален надзорен орган за сертифицирането разполага поне със следните правомощия:

а) да изисква от органите за оценяване на съответствието и притежателите на европейски сертификати за киберсигурност да представят всяка информация, която му е необходима за изпълнението на неговите задачи;

б) да провежда разследвания под формата на одити на органите за оценяване на съответствието и притежателите на европейски сертификати за киберсигурност за целите на проверка на съответствието с разпоредбите по дял III;

в) да взема подходящи мерки съгласно националното законодателство, за да гарантира, че органите за оценяване на съответствието или притежателите на сертификати спазват настоящия регламент или дадена европейска схема за сертифициране на киберсигурността;

г) да получава достъп до всички помещения на органите за оценяване на съответствието и на притежателите на европейски сертификати за киберсигурност за целите на провеждане на разследвания съгласно процесуалното право на Съюза или на държавата членка;

д) да отнема в съответствие с националното законодателство сертификати, които не са в съответствие с настоящия регламент или с дадена европейска схема за сертифициране на киберсигурността;

е) да налага санкции, както е предвидено в член 54, съгласно националното законодателство, и да изисква незабавното преустановяване на нарушенията на задълженията по настоящия регламент.

8. Националните надзорни органи за сертифицирането си сътрудничат помежду си и с Комисията, и по-специално обменят информация, опит и добри практики във връзка със сертифицирането на киберсигурността и техническите въпроси, засягащи киберсигурността на ИКТ продукти и услуги.

Член 51

Органи за оценяване на съответствието

1. Органите за оценяване на съответствието се акредитират от националния орган по акредитация, определен по силата на Регламент (ЕО) № 765/2008, само

когато те отговарят на изискванията, определени в приложението към настоящия регламент.

2. Акредитацията се издава за максимален срок от пет години и може да бъде подновена при същите условия, ако органът за оценяване на съответствието отговаря на изискванията, определени в настоящия член. Органите по акредитация отнемат акредитацията на органа за оценяване на съответствието по параграф 1 от настоящия член, ако условията за акредитация не са били спазени или вече не се спазват или ако действия, предприети от органа за оценяване на съответствието, нарушават настоящия регламент.

Член 52

Уведомления

1. За всяка европейска схема за сертифициране на киберсигурността, приета съгласно член 44, националните надзорни органи за сертифицирането уведомяват Комисията за акредитираните органи за оценяване на съответствието, оправомощени да издават сертификати при определени нива на обезпечаване на сигурност, както е посочено в член 46, и без неоправдано закъснение за всяка свързана с тях промяна.

2. Една година след датата на влизане в сила на дадена европейска схема за сертифициране на киберсигурността Комисията публикува списък на съобщените ѝ органи за оценяване на съответствието в Официален вестник на Европейския съюз.

3. Ако Комисията получи уведомление след изтичането на посочения в параграф 2 срок, тя публикува в Официален вестник на Европейския съюз измененията на списъка, посочен в параграф 2, в срок от два месеца от датата на получаване на уведомлението.

4. Всеки национален надзорен орган за сертифицирането може да представи на Комисията искане за заличаване на даден орган за оценяване на съответствието, съобщен от този национален надзорен орган по сертифицирането, от списъка, посочен в параграф 2 от настоящия член. Комисията публикува в Официален вестник на Европейския съюз съответните изменения на списъка в срок от един месец от датата на получаване на искането от националния надзорен орган за сертифициране.

5. Комисията може да определи посредством актове за изпълнение обстоятелствата, форматите и процедурите за уведомяването, посочено в параграф 1 от настоящия член. Актовете за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 55, параграф 2.

Член 53

Европейска група за сертифициране на киберсигурността

1. Създава се Европейска група за сертифициране на киберсигурността („групата“).

2. Групата се състои от националните надзорни органи за сертифициране, представени от своите ръководители или други високопоставени представители.

3. Групата има следните задачи:

а) да консултира и подпомага Комисията в работата ѝ с цел гарантиране на съгласувано изпълнение и прилагане на настоящия дял, по-специално по въпроси на политиката на сертифицирането на киберсигурността, както и в изготвянето на европейски схеми за сертифициране на киберсигурността;

б) да подпомага, консултира и сътрудничи на ENISA във връзка с подготовката на проекти за схеми съгласно член 44 от настоящия регламент;

в) да предлага на Комисията да отправи искане до Агенцията да подготви даден проект за Европейска схема за сертифициране на киберсигурността съгласно член 44 от настоящия регламент;

г) да приема становища, адресирани до Комисията, свързани с поддръжката и преразглеждането на съществуващите европейски схеми за сертифициране на киберсигурността;

д) да проучва важните новости в областта на сертифицирането на киберсигурността и да обменя добри практики във връзка със схемите за сертифициране на киберсигурността;

е) да улеснява сътрудничеството между националните надзорни органи за сертифициране по настоящия дял чрез обмен на информация, по-специално чрез установяване на методи за ефективен обмен на информация, свързана с всички въпроси на сертифицирането на киберсигурността.

4. Комисията председателства групата и осигурява нейния секретариат с помощта на ENISA, както е предвидено в член 8, буква а).

Член 54
Санкции

Държавите членки определят правилата относно санкциите, приложими при нарушаване на настоящия дял и на Европейските схеми за сертифициране на киберсигурността, и вземат всички необходими мерки, за да гарантират прилагането на тези санкции. Предвидените санкции трябва да са ефективни, пропорционални и възпиращи. Държавите членки съобщават на Комисията тези правила и мерки [до …/незабавно] и я уведомяват за всяко последващо изменение, което ги засяга.

ДЯЛ IV
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

*Член 55****Процедура на комитет***

1. Комисията се подпомага от комитет. Този комитет е комитет по смисъла на Регламент (ЕС) № 182/2011.

2. При позоваване на настоящия параграф се прилага член 5 от Регламент (ЕС) № 182/2011.

Член 56
Оценка и преглед

1. Не по-късно от пет години след датата, посочена в член 58, и на всеки пет години след това Комисията извършва оценка на въздействието и ефективността на работата на Агенцията и нейните работни практики, както и на евентуалната необходимост от изменение на мандата на Агенцията и финансовите последици от такова изменение. В оценката се взема предвид всякаква обратна информация, предоставена в Агенцията в отговор на нейните дейности. Ако Комисията сметне, че съществуването на Агенцията вече не е оправдано от гледна точка на възложените ѝ цели, мандат и задачи, тя може да предложи настоящият регламент да бъде изменен в частта му, свързана с Агенцията.

2. Оценката също така разглежда въздействието и ефективността на разпоредбите на дял III по отношение на целите за осигуряване на адекватно ниво на киберсигурност на ИКТ продукти и услуги в Съюза и се подобряване на функционирането на вътрешния пазар.

3. Комисията изпраща доклада за оценка заедно със своите заключения на Европейския парламент, Съвета и управителния съвет. Заключенията от оценката се оповестяват публично.

Член 57
Отмяна и правоприемство

1. Регламент (ЕС) № 526/2013 се отменя считано от [….].

2. Позоваванията на Регламент (ЕО) № 526/2013 и на ENISA се считат за позовавания на настоящия регламент и на Агенцията.

3. Агенцията е правоприемник на агенцията, учредена с Регламент (ЕО) № 526/2013, по отношение на цялата собственост, споразумения, правни задължения, трудови договори, финансови ангажименти и задължения. Всички съществуващи решения на управителния съвет и изпълнителния съвет остават в сила, доколкото не противоречат на разпоредбите на настоящия регламент.

4. Агенцията се учредява за неограничен срок считано от [….].

5. Изпълнителният директор, назначен съгласно член 24, параграф 4 от Регламент (ЕС) № 526/2013, е изпълнителен директор на Агенцията за останалата част от мандата си.

6. Членовете и техните заместници в управителния съвет, назначени съгласно член 6 от Регламент (ЕС) № 526/2013, са членове и техни заместници в управителния съвет на Агенцията за останалата част от мандата си.

Член 58

Влизане в сила

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

2. 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

Предложение за регламент на Европейския парламент и на Съвета относно ENISA, „Агенцията на ЕС за киберсигурност“, и за отмяна на Регламент (ЕС) № 526/2013, както и относно сертифицирането на сигурността на информационните и комуникационните технологии („Акт/Регламент за киберсигурността“)

1.2. Засегната(и) област(и) на политиката

Област на политиката: 09 — Комуникационни мрежи, съдържание и технологии

Дейност: 09.02 Цифров единен пазар

1.3. Естество на предложението/инициативата

☒ Предложението/инициативата е във връзка с **нова дейност (дял III — Сертифициране)**

☐ Предложението/инициативата е във връзка с **нова дейност след пилотен проект/подготвителна дейност**[43]

☒ Предложението/инициативата е във връзка с **продължаване на съществуваща дейност (дял II — Мандат на ENISA)**

☐ Предложението/инициативата е във връзка с **дейност, пренасочена към нова дейност**

1.4. Цел(и)

1.4.1. Многогодишни стратегически цели на Комисията, за чието изпълнение е предназначено предложението/инициативата

1. Засилване на устойчивостта на държавите членки, предприятията и на ЕС като цяло

2. Гарантиране на доброто функциониране на вътрешния пазар на ЕС за ИКТ продукти и услуги

3. Увеличаване на глобалната конкурентоспособност на предприятията в ЕС, упражняващи дейност в сектора на ИКТ.

4. Сближаване на законите, наредбите и административните разпоредби на държавите членки, които изискват киберсигурност

1.4.2. Конкретни цели

С оглед на общите цели и по-широкия контекст на преразгледана стратегия за киберсигурността инструментът, като очертава полето на действие и мандата на ENISA и установява Европейска рамка за сертифициране на ИКТ продукти и услуги, има следните конкретни цели:

1. увеличаване на **способностите и подготвеността** на държавите членки и предприятията;
2. подобряване на **сътрудничеството и координацията** между държавите

[43] Съгласно член 54, параграф 2, буква а) или б) от Финансовия регламент.

членки и институциите, агенциите и органите на ЕС;

3. увеличаване на **способностите на равнище ЕС за допълване на действията на държавите членки**, особено в случай на трансгранични кризи на киберсигурността;
4. повишаване на **осведомеността** на гражданите и предприятията по въпроси, свързани с киберсигурността;
5. укрепване на доверието в цифровия единен пазар и в цифровите иновации чрез повишаване на цялостната **прозрачност на обезпечаването на киберсигурността**[44] на ИКТ продукти и услуги.

ENISA ще допринесе за постигането на горепосочените цели посредством:

Подобрено съдействие при определянето на политики — предоставяне на насоки и консултации на Комисията и на държавите членки относно актуализирането и разработването на цялостна нормативна рамка в областта на киберсигурността, както и специфични за отрасъла политически и законодателни инициативи по въпросите на киберсигурността; принос към работата на групата за сътрудничество съгласно член 11 от Директива (ЕС) 2016/1148 чрез предоставяне на експертен опит и помощ; подкрепа за разработването и изпълнението на политиките в областта на електронната идентификация и удостоверителните услуги; насърчаване обмена на най-добри практики между компетентните органи;

Подобрено съдействие за изграждане на капацитет — предоставяне на подкрепа на държавите членки, институциите, органите, службите и агенциите на Съюза при разработването и подобряването на превенцията, откриването и анализа, както и способността за реагиране на проблеми и инциденти в областта на киберсигурността; подпомагане на държавите членки по тяхно искане при изграждането на националните CSIRT и националните стратегии за киберсигурност; подпомагане на институциите на Съюза при изготвянето и прегледа на стратегиите за киберсигурност на Съюза; осигуряване на обучения в областта на киберсигурността; подпомагане на държавите членки чрез групата за сътрудничество при обмена на най-добри практики; улесняване на създаването на секторни центрове за споделяне и анализ на информация (ISAC).

Подпомагане на оперативното сътрудничество и управлението на кризи — подпомагане на сътрудничеството между компетентните публични органи и между заинтересованите страни чрез установяване на системно сътрудничество с институциите, органите, службите и агенциите на Съюза, работещи в областта на киберсигурността, борбата с киберпрестъпността и защитата на неприкосновеността на личния живот и личните данни; осигуряване на секретариат на мрежата на CSIRT съгласно член 12, параграф 2 от Директива (ЕС) 2016/1148) и дава приноса си за оперативното сътрудничество в мрежата чрез предоставяне съвместно с CERT-EU на помощ на държавите членки по тяхно искане; организиране на редовни учения в областта на киберсигурността; принос в разработването на колективна реакция на мащабни трансгранични киберинциденти и кризи; провеждане съвместно с мрежата на CSIRT на последващи технически разследвания на сериозни инциденти и изготвяне на препоръки за последващи действия;

[44] Прозрачност на обезпечаването на киберсигурността означава да се предостави на потребителите достатъчно информация за свойствата на киберсигурността, за да могат те да определят обективно степента на сигурност на даден ИКТ продукт, дадена ИКТ услуга или даден ИКТ процес.

Задачи, свързани с пазара (стандартизация, сертифициране) — извършване на редица функции конкретно за подпомагане на вътрешния пазар: „обсерватория на пазара“ на киберсигурността чрез анализиране на съответните тенденции на пазара на киберсигурността с цел по-добро съчетаване на търсенето и предлагането; подпомагане и насърчаване на разработването и изпълнението на политиката на Съюза за сертифициране на киберсигурността на ИКТ продукти и услуги чрез подготовка на проекти за европейски схеми за сертифициране на киберсигурността на ИКТ продукти и услуги, осигуряване на секретариата на групата за сертифициране на киберсигурността на Съюза, предоставяне на насоки и добри практики относно изискванията за сигурността на ИКТ продукти и услуги съвместно с националните надзорни органи за сертифицирането и промишлеността; **Засилена подкрепа за разширяване на познанията, информацията и осведомеността** — оказване на помощ и предоставяне на съвети на Комисията и на държавите членки за постигане на високо ниво на познания в целия ЕС относно въпроси, свързани с МИС, и прилагане на тези познания спрямо заинтересованите страни от отрасъла. Това предполага също обединяване на ресурси, организиране и предоставяне на разположение на обществеността чрез специален портал на информация относно сигурността на мрежовите и информационните системи [или киберсигурността]. Друг важен елемент са дейностите за повишаване на осведомеността и информационните кампании, насочени към широката общественост и разглеждащи рисковете за киберсигурността.

Засилена подкрепа за научните изследвания и иновациите — осигуряване на консултации относно нуждата от научни изследвания и определяне на приоритетите в областта на киберсигурността;

Подкрепа за международното сътрудничество — подпомагане на Съюза в усилията му да си сътрудничи с трети държави и международни организации с оглед насърчаване на международното сътрудничество в областта на киберсигурността.

СЕРТИФИЦИРАНЕ

Рамката за сертифициране ще допринесе за постигане на целите чрез повишаване на цялостната прозрачност в обезпечаването на киберсигурността[45] на ИКТ продукти и услуги, което ще укрепи доверието в цифровия единен пазар и в цифровите иновации. Това следва да помогне за избягване на разпокъсаността на схемите за сертифициране в ЕС и свързаните с тях изисквания за сигурност и критерии за оценка в различните държави членки и сектори;

1.4.3. Очаквани резултати и отражение

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

Очаква се укрепването на ENISA (което ще подпомогне развитието на способностите, превенцията, сътрудничеството и повишаването на осведомеността на равнище ЕС, поради което се очаква да доведе до увеличаване на цялостната киберустойчивост на ЕС) и подпомагането на мрежата на ЕС за сертифициране на ИКТ продукти и услуги да имат следните въздействия (неизчерпателен списък):

45 Прозрачност на обезпечаването на киберсигурността означава да се предостави на потребителите достатъчно информация за свойствата на киберсигурността, за да могат те да определят обективно степента на сигурност на даден ИКТ продукт, дадена ИКТ услуга или даден ИКТ процес.

Цялостно въздействие:

- цялостно положително въздействие върху вътрешния пазар благодарение на намаляване на разпокъсаността и изграждане на доверие в цифровите технологии чрез по-добро сътрудничество, по-хармонизиран подход към политиките на ЕС за киберсигурност и увеличени способности на равнище ЕС. Това следва да доведе до положително икономическо въздействие, като спомогне за снижаването на разходите, причинени от киберинциденти/киберпрестъпност; икономическото въздействие за ЕС се оценява на 0,41 % от БВП на ЕС, т.е. около 55 милиарда евро.

Конкретни резултати:

Подобряване на способностите и подготвеността на държавите членки и предприятията

- Подобряване на способностите и подготвеността на държавите членки в областта на киберсигурността (благодарение на дългосрочен стратегически анализ на киберзаплахи и инциденти, насоки и доклади, предлагане на експертни знания и добри практики, наличие на обучения и учебни материали, подобрени учения CyberEurope)

- Подобряване на способностите на частния сектор благодарение на подкрепата за създаването на центрове за споделяне и анализ на информация (ISAC) в различни сектори

- Подобряване на подготвеността на ЕС и държавите членки в областта на киберсигурността благодарение на наличието на отработени и съгласувани планове в случай на мащабни трансгранични киберинциденти, изпитани по време на ученията CyberEurope

Подобряване на сътрудничеството и координацията между държавите членки и институциите, агенциите и органите на ЕС

- Подобряване на сътрудничеството в публичния и частния сектор, както и между тях

- Подобряване на съгласуваността на подхода за изпълнението на Директивата за МИС между различните отрасли и отделните държави

- Подобряване на сътрудничеството в областта на сертифицирането благодарение на институционална рамка, която позволява разработването на европейски схеми за сертифициране на киберсигурността и обща политика в тази област

Увеличаване на способностите на равнище ЕС за допълване на действията на държавите членки

- Увеличаване на „оперативния капацитет на ЕС“ за допълване на действията на държавите членки и подкрепа по тяхно искане и във връзка с ограничени и предварително определени услуги. Очаква се това да има положително въздействие за успешното предотвратяване, установяване и реагиране на инциденти както в отделните държави членки, така и в целия ЕС

Повишаване на осведомеността на гражданите и предприятията по въпроси, свързани с киберсигурността

- Подобряване на осведомеността на гражданите и предприятията по въпроси, свързани с киберсигурността

- Подобряване на способността за вземане на информирани решения за покупки, свързани с ИКТ продукти и услуги, благодарение на сертифицирането на киберсигурността

Укрепване на доверието в цифровия единен пазар и в цифровите иновации чрез повишена цялостна прозрачност на обезпечаването на киберсигурността на ИКТ продукти и услуги

- Увеличаване на прозрачността на обезпечаването на киберсигурността[46] на ИКТ продукти и услуги благодарение на опростяването на процедурите за сертифициране на сигурността посредством обща за целия ЕС рамка

- Подобряване на нивото на обезпечаване на сигурността на ИКТ продукти и услуги

- По-широко навлизане на сертифицирането на киберсигурността, стимулирано от опростени процедури, намалени разходи и подобрена перспектива за стопанска дейност в целия ЕС, която не страда от разпокъсаността на пазара

- Засилване на конкурентоспособността на пазара за киберсигурност в ЕС поради намалени разходи и административна тежест за МСП и премахване на евентуални препятствия пред навлизане на пазара, породени от множеството национални системи за сертифициране

Други

- Не се очаква значително въздействие върху околната среда за която и да било от целите.

- По отношение на бюджета на ЕС може да се очаква подобряване на ефикасността чрез засилено сътрудничество и координация на дейности на дейности между институциите, агенциите и органите на ЕС.

1.4.4. Показатели за резултатите и за отражението

Да се посочат показателите, които позволяват да се проследи изпълнението на предложението/инициативата.

а)

Цел: Увеличаване на способностите и подготвеността на държавите членки и предприятията:

- Брой на обученията, организирани от ENISA
- Географско покритие (брой държави и райони) на пряката помощ, осигурявана от ENISA
- Равнище на подготвеност, достигнато от държавите членки, според зрелостта на CSIRT и надзора на съответните регулаторни мерки
- Брой на предоставените от ENISA добри практики в целия ЕС за критични инфраструктури
- Брой на предоставените от ENISA добри практики в целия ЕС за МСП
- Публикуване на годишния стратегически анализ на ENISA за киберзаплахите и инцидентите, за да се установят възникващи тенденции
- Редовен принос от ENISA за работата на работните групи за

[46] Прозрачност на обезпечаването на киберсигурността означава да се предостави на потребителите достатъчно информация за свойствата на киберсигурността, за да могат те да определят обективно степента на сигурност на даден ИКТ продукт, дадена ИКТ услуга или даден ИКТ процес.

киберсигурност на европейските организации по стандартизация (ЕОС). **Цел: Подобряване на сътрудничеството и координацията между държавите членки и институциите, агенциите и органите на ЕС:** · Брой държави членки, възползвали се от препоръките на ENISA в процеса на разработване на политиките си · Брой институции, агенции и органи на ЕС, възползвали се от препоръките на ENISA в процеса на разработване на политиките си · Редовно изпълнение на работната програма на мрежата на CSIRT и добро функциониране на ИТ инфраструктурата и комуникационните канали на мрежата CSIRT · Брой на техническите доклади, предоставени и използвани от групата за сътрудничество · Съгласуван подход към изпълнението на Директивата за МИС между различните отрасли и отделните държави · Брой оценки на спазването на регулаторните изисквания, направени от ENISA · Брой на наличните ISAC в различните сектори, особено за критичните инфраструктури · Създаване и редовно използване на информационна платформа за разпространение на информация за киберсигурността от институциите, агенциите и органите на ЕС · Редовно участие в изготвянето на работните програми на ЕС за научни изследвания и иновации · Сключено споразумение за сътрудничество между ENISA, EC3 и CERT-EU · Брой на схемите за сертифициране, включени и разработени съгласно рамката **Цел: Увеличаване на способностите на равнище ЕС за допълване на действията на държавите членки, особено в случай на трансгранични кризи на киберсигурността:** · Публикуване на годишния стратегически анализ на ENISA за киберзаплахите и инцидентите, за да се установят възникващи тенденции · Публикуване на обобщена информация за инциденти, докладвани от ENISA в изпълнение на Директивата за МИС · Брой на общоевропейските учения, координирани от Агенцията, и брой на участвалите държави членки и организации · Брой на исканията за подкрепа от държавите членки за реагиране при извънредни ситуации, на които ENISA е откликнала · Брой на анализите на уязвими точки, артефакти и инциденти, които ENISA е извършила съвместно с CERT-EU · Наличие на ситуационни доклади въз основа на информацията, предоставена на ENISA от държавите членки и други субекти в случай на мащабни трансгранични киберинциденти **Цел: Повишаване на осведомеността на гражданите и предприятията по**

въпроси, свързани с киберсигурността:

- Редовно провеждане на европейски и национални кампании за повишаване на осведомеността и редовно актуализиране на темите в зависимост от нововъзникващите потребности от обучение
- Повишаване на осведомеността по въпросите на киберсигурността сред гражданите на ЕС
- Редовно провеждане на викторини за осведомеността по въпросите на киберсигурността и увеличаване на дела на верните отговори с времето
- Редовно публикуване на добри практики за киберсигурността и киберхигиената, насочени към работниците и организациите

Цел: Укрепване на доверието в цифровия единен пазар и в цифровите иновации чрез повишаване на цялостната прозрачност на обезпечаването на киберсигурността[47] на ИКТ продукти и услуги:

- Брой на схемите, които се придържат към рамката на ЕС
- Намалени разходи за получаване на сертификат за сигурност на ИКТ продукти
- Брой на организациите за оценяване на съответствието, специализирани в областта на ИКТ в държавите членки
- Създаване на Европейската група за сертифициране на киберсигурността и редовно свикване на заседания
- Наличие на насоки за сертифициране съгласно съществуващата рамка на ЕС
- Редовно публикуване на анализи на основните тенденции на пазара на киберсигурността в ЕС
- Брой на сертифицираните ИКТ продукти и услуги съгласно правилата на Европейската рамка за сертифициране на сигурността на ИКТ
- Увеличен брой крайни потребители, които са осведомени относно елементите на сигурността в ИКТ продукти и услуги

б)

1.4.5. Нужди, които трябва да бъдат задоволени в краткосрочен или дългосрочен план

Предвид нормативните изисквания и бързо променящата се картина на киберзаплахите, мандатът на ENISA трябва да бъде преразгледан, за да се определи нов набор от задачи и функции с цел да се подкрепят ефективно усилията на държавите членки, институциите на ЕС и други заинтересовани страни за гарантиране на сигурно киберпространство в Европейския съюз. Предложеният обхват на мандата е очертан така, че да укрепи капацитета в областите, където Агенцията е доказала ясно своята добавена стойност и да добави новите области, в които е необходима подкрепа с оглед на новите политически приоритети и инструменти, по-специално Директивата за МИС, прегледа на стратегията на ЕС за киберсигурност, разработваната в момента концепция на ЕС за киберсигурността

[47] Прозрачност на обезпечаването на киберсигурността означава да се предостави на потребителите достатъчно информация за свойствата на киберсигурността, за да могат те да определят обективно степента на сигурност на даден ИКТ продукт, дадена ИКТ услуга или даден ИКТ процес.

относно сътрудничеството при киберкризи и сертифицирането на сигурността на ИКТ. Предлаганият нов мандат има за цел да даде по-значителна и централна роля на Агенцията, особено в активната подкрепа на държавите членки при противодействието на определени заплахи (оперативен капацитет); тя ще се превърне в средище на експерти, което ще подпомага държавите членки и Комисията във връзка със сертифицирането на киберсигурността.

Същевременно предложението установява Европейска рамка за сертифициране на киберсигурността на ИКТ продукти и услуги и определя съществените функции и задачи на ENISA в областта на киберсигурността. Рамката определя общи разпоредби и процедури, с помощта на които се създават схеми за сертифициране на киберсигурността в целия ЕС за конкретни ИКТ продукти/услуги или конкретни рискове. Създаването на европейски схеми за сертифициране на киберсигурността в съответствие с рамката ще позволи сертификатите, издадени по тези схеми, да бъдат валидни и признати във всички държави членки и да се преодолее съществуващата в момента разпокъсаност на пазара.

1.4.6. Добавена стойност от участието на Съюза

Киберсигурността действително е трансграничен по същността си световен проблем, който засяга едновременно различни сектори поради взаимозависимостта на мрежовите и информационните системи. Броят, сложността и мащабът на киберинцидентите и тяхното въздействие върху икономиката и обществото нарастват с течение на времето и се очаква да се увеличат още с напредъка на технологиите, например с широкото навлизане на интернет на нещата. Това предполага, че нуждата от по-голямо съвместно усилие от държавите членки, институциите на ЕС и частния сектор за преодоляване на киберзаплахите ще продължи да нараства занапред.

От създаването си през 2004 г. ENISA има за цел да насърчава сътрудничеството между държавите членки и заинтересованите страни по МИС, включително публично-частното сътрудничество. Тази подкрепа за сътрудничеството включва техническата работа по осигуряване на обща картина на киберзаплахите в целия ЕС, създаването на експертни групи и организирането на общоевропейски учения за киберинциденти и управление на кризи за публичния и частния сектор (по-специално „CyberEurope“). Директивата за МИС натовари ENISA с допълнителни задачи, включително ролята на секретариат на мрежата CSIRT за оперативното сътрудничество между държавите членки.

Добавената стойност на действията на равнището на ЕС, по-специално с цел да се засили сътрудничеството между държавите членки, но и между общностите за МИС, беше отчетена в заключенията на Съвета от 2016 г.[48] и проличава ясно и в оценката на ENISA от 2017 г., която показва, че нейната добавена стойност се крие главно в способността ѝ да насърчава сътрудничеството между тези заинтересовани страни. Няма друг участник на равнище ЕС, който да подкрепя сътрудничеството между толкова широк набор от заинтересовани страни в областта на МИС.

Добавената стойност на ENISA за свързването на общности и заинтересовани лица в областта на киберсигурността е валидна и в областта на сертифицирането.

[48] Заключения на Съвета относно укрепването на отбранителната способност на Европа срещу кибератаки и изграждането на конкурентен и иновативен сектор на киберсигурността – 15 ноември 2016 г.

Зачестяването на киберпрестъпленията и заплахите за сигурността доведе до възникването на национални инициативи за определяне на високи изисквания за киберсигурност и сертифициране на ИКТ компонентите, използвани в традиционната инфраструктура. Макар и важни, тези инициативи носят риск от разпокъсване на единния пазар и възникване на пречки за оперативната съвместимост. Може да се наложи продавачите на ИКТ да преминават през различни процедури на сертифициране, за да могат да продават в няколко държави членки. Малко вероятно е неефективността на настоящите схеми за сертифициране да бъде преодоляна без намеса от страна на ЕС. При липса на действия е много вероятно разпокъсаността на пазара да се увеличи в краткосрочен план (следващите 5—10 години) с появата на нови схеми за сертифициране. Липсата на координация и оперативна съвместимост между тези схеми е фактор, ограничаващ потенциала на цифровия единен пазар. Това доказва добавената стойност на създаването на една европейска рамка за сертифициране на ИКТ продукти и услуги, която да осигури правилните условия за ефективно решаване на проблема, свързан с паралелното съществуване на различни процедури за сертифициране в различните държави членки, да намали разходите за сертифициране и така да направи сертифицирането в ЕС като цяло по-привлекателно от гледна точка на търговията и конкуренцията.

1.4.7. Поуки от подобен опит в миналото

В съответствие с нормативната база за ENISA Комисията извърши оценка на Агенцията, включваща независимо проучване и обществена консултация. Оценката стигна до заключението, че целите на ENISA продължават да са актуални и днес. В контекста на технологичното развитие и променящите се заплахи и значителната необходимост от по-голяма сигурност на мрежовите и информационни системи (МИС) в ЕС е нужен технически експертен опит в областта на сигурността на МИС. В държавите членки трябва да се изгради капацитет за разбиране на заплахите и съответно реагиране и заинтересованите страни трябва да си сътрудничат отвъд границите на конкретни тематични области и конкретни институции.

Агенцията успешно допринася за по-голяма сигурност на МИС в Европа като предлага изграждане на капацитет в 28 държави членки, засилване на сътрудничеството между държавите членки и заинтересованите страни в сферата на МИС; осигуряване на експертен опит, изграждане на общности и подкрепа на политиката.

Макар ENISA да успя, поне в известна степен, да окаже влияние в огромната област на мрежовата и информационната сигурност, тя не успя напълно да си създаде име и да придобие достатъчна популярност, за да бъде призната като „най-важен“ център на експертен опит в Европа. Това се обяснява с широкия мандат на ENISA, който не беше подкрепен от пропорционални по размер ресурси. Освен това ENISA остава единствената агенция на ЕС с мандат за ограничен срок, което ограничава нейните възможности да развива дългосрочна концепция и да оказва трайна подкрепа на съответните заинтересовани страни. Това също така е в противоречие с разпоредбите на Директивата за МИС, с която на ENISA се възлагат задачи без краен срок.

Що се отнася до сертифицирането на киберсигурността на ИКТ продукти и услуги, понастоящем не съществува европейска рамка. Зачестяването на киберпрестъпленията и заплахите за сигурността обаче доведе до възникването на национални инициативи, които пораждат риск от разпокъсаност на единния пазар.

1.4.8. Съвместимост и евентуална синергия с други подходящи инструменти

Инициативата е силно съгласувана със съществуващите политики, по-специално в областта на вътрешния пазар. Всъщност тя е проектирана в съответствие с цялостния подход към киберсигурността, определен в прегледа на Стратегията на ЕС за цифров единен пазар, за да допълва всеобхватен набор от мерки, например прегледа на Стратегията на ЕС за киберсигурност, концепцията за сътрудничество при киберкризи и инициативите за борба с киберпрестъпността. Тя осигурява съгласуваност с разпоредбите на съществуващото законодателство в областта на киберсигурността, особено с Директивата за МИС, и ги доразвива, за да бъде постигната още по-голяма киберустойчивост на ЕС чрез подобряване на способностите, сътрудничеството, управлението на риска и осведомеността.

Предложените мерки за сертифицирането следва да бъдат насочени към преодоляването на потенциалната разпокъсаност, предизвикана от съществуващи и нови национални схеми за сертифициране, с което ще се подпомогне развитието на цифровия единен пазар. Инициативата подкрепя и допълва изпълнението на Директивата за МИС, като предоставя на предприятията, за които се прилага директивата, инструмент за доказване на спазването на изискванията за МИС в целия Съюз.

Европейската рамка за сертифициране на киберсигурността на ИКТ — такава, каквато е предложена — не накърнява Общия регламент относно защитата на данните[49], нито съответните разпоредби относно сертифицирането[50], тъй като те се отнасят до сигурността при обработването на лични данни. Не на последно място, схемите, които ще бъдат предлагани занапред по Европейската рамка, следва във възможно най-голяма степен да се основават на международни стандарти като начин за избягване на пречките пред търговията и осигуряване на съгласуваност с международните инициативи.

[49] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).

[50] Като например членове 42 (Сертифициране) и 43 (Сертифициращи органи), както и членове 57, 58 и 70 относно съответните задачи и правомощия на независимите надзорни органи и задачите на Европейския комитет по защита на данните.

1.5. Продължителност и финансово отражение

☐ Предложение/инициатива **с ограничен срок на действие**

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

– ☐ Финансово отражение от ГГГГ до ГГГГ

☒ Предложение/инициатива **с неограничен срок на действие**

– Осъществяване с период на започване на дейност от 2019 г. до 2020 г.,

– последван от функциониране с пълен капацитет.

1.6. Планирани методи на управление[51]

☒ **Пряко управление** от Комисията (дял III — Сертифициране)

– ☐ изпълнителни агенции

☐ **Споделено управление** с държавите членки

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

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

☐ ЕИБ и Европейския инвестиционен фонд;

☒ органите, посочени в членове 208 и 209 (дял II — ENISA)

☐ публичноправни органи;

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

☐ 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.

Бележки

В обхвата на регламента са включени: - в дял II от предложението за регламент се прави преглед на мандата на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA), като ѝ се възлага важна роля при сертифицирането, а - в дял III се установява рамка за създаването на европейски схеми за сертифициране на киберсигурността на ИКТ продукти и услуги, в която ENISA играе решаваща роля.

[51] 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.

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

Да се посочат честотата и условията.

Мониторингът ще започне веднага след приемането на правния инструмент и ще се съсредоточи върху прилагането му. Комисията ще организира срещи с представители на ENISA, държавите членки (например група от експерти) и съответните заинтересовани страни, по-специално за да улесни прилагането на правилата за сертифициране, като например създаването на съвета.

Първата оценка следва да се проведе 5 години след влизането в сила на правния инструмент, при положение че са налични достатъчно данни. В правния инструмент е включена изрична клауза за оценка и преглед [член XXX], по силата на която Комисията ще направи независима оценка. Впоследствие Комисията ще докладва на Европейския парламент и на Съвета за своята оценка, която при необходимост ще бъде придружена от предложение за преразглеждане, за да се оценят въздействието на регламента и неговата добавена стойност. Допълнителни оценки следва да бъдат извършвани на всеки пет години. При оценката ще бъде приложена методиката на Комисията за по-добро законотворчество. Тези оценки ще бъдат извършвани с помощта на целеви експертни дискусии, проучвания и широки консултации със заинтересованите страни.

Изпълнителният директор на ENISA следва да представя на управителния съвет доклад за последваща оценка на дейностите на ENISA на всеки две години. Агенцията следва също така на всеки две години да изготвя план за последващи действия във връзка със заключенията от предишни оценки и доклад за напредъка до Комисията. Управителният съвет следва да носи отговорност за надзора на подходящи последващи действия във връзка с тези заключения.

Сигналите за случаи на лошо администриране на дейността на Агенцията подлежат на разследване от страна на Европейския омбудсман в съответствие с разпоредбите на член 228 от Договора.

Източниците на данни за планирания мониторинг ще бъдат предимно ENISA, Европейската група за сертифициране на киберсигурността, групата за сътрудничество, мрежата на CSIRT и властите на държавите членки. Освен данните от докладите (включително годишните доклади за дейността) на ENISA, Европейската група за сертифициране на киберсигурността, групата за сътрудничество и мрежата на CSIRT, при необходимост ще се използват специфични инструменти за събиране на данни (например проучвания на националните органи, Евробарометър и доклади от кампанията „Месец на киберсигурността“ и общоевропейските учения).

2.2. Система за управление и контрол

2.2.1. Установен(и) риск(ове)

Установените рискове са ограничени: вече съществува агенция на Съюза и нейният мандат е очертан така, че да укрепи областите, където Агенцията е доказала ясно своята

добавена стойност, и да добави новите области, в които е необходима подкрепа с оглед на новите политически приоритети и инструменти, по-специално Директивата за МИС, прегледа на стратегията на ЕС за киберсигурност, разработваната в момента концепция на ЕС за киберсигурността относно сътрудничеството при киберкризи и сертифицирането на сигурността на ИКТ.

Поради това предложението разглежда подробно функциите на Агенцията и води до повишаване на ефективността. Увеличаването на оперативната компетентност и задачите не представлява реален риск, тъй като те допълват дейността на държавите членки и ги подкрепят по тяхно искане и във връзка с ограничени и предварително определени услуги.

Освен това предложеният модел на работа на Агенцията, съгласно Общия подход, осигурява достатъчен контрол, за да се гарантира, че ENISA ще работи за постигането на своите цели. Оперативните и финансовите рискове от предлаганите промени изглеждат ограничени.

Същевременно е необходимо да се осигурят достатъчни финансови ресурси, за да може ENISA да изпълнява задачите, възложени ѝ чрез новия мандат, включително в областта на сертифицирането.

2.2.2. Предвиден(и) метод(и) на контрол

Отчетите на агенцията се предават на Сметната палата за одобрение и за тях се прилага процедурата по освобождаване от отговорност и се предвиждат одити.

Също така, дейността на Агенцията подлежи на надзор от омбудсмана в съответствие с разпоредбите на член 228 от Договора.

Вж. точка 2.1 и точка 2.2.1 по-горе.

2.3. Мерки за предотвратяване на измами и нередности

Да се посочат съществуващите или планираните мерки за предотвратяване и защита.

Ще се прилагат мерките за предотвратяване и защита на ENISA, по-специално:

- Плащания за всякакви услуги или поискани проучвания се проверяват от персонала на агенцията преди те да бъдат извършени, като се взимат под внимание договорните задължения, икономическите принципи и добрите финансови и управленски практики. Разпоредби за борба с измамите (наблюдение, изисквания за докладване и т.н.) ще бъдат включени във всички договори и споразумения, сключени между агенцията и получателите на плащанията.

- С оглед на борбата с измамите, корупцията и други незаконни дейности, 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 ограничения.

- В срок от шест месеца от датата на влизане в сила на настоящия регламент Агенцията се присъединява към Междуинституционалното споразумение от 25 май 1999 г. между Европейския парламент, Съвета на Европейския съюз и Комисията на Европейските общности относно вътрешните разследвания, провеждани от Европейската служба за

борба с измамите (OLAF), и издава незабавно подходящи разпоредби, приложими към всички служители на агенцията.

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

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

- Съществуващи бюджетни редове

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

Функция от многогодишната финансова рамка	Бюджетен ред	Вид на разхода	Вноска			
		Много год./едногод. [52]	от държави от ЕАСТ [53]	от държави кандидатки [54]	от трети държави	по смисъла на член 21, параграф 2, буква б) от Финансовия регламент
1a Конкурентоспособност за растеж и заетост	09.0203 ENISA и сертифициране на сигурността на информационни и комуникационни технологии	Много год.	ДА	НЕ	НЕ	НЕ
5 Административни разходи]	09.0101 Разходи, свързани с активно заети служители в съобщителни мрежи, съдържание и технологии 09.0102 Разходи, свързани с активно заети външни служители в	Едного д.	НЕ	НЕ	НЕ	НЕ

[52] Многогод. = многогодишни бюджетни кредити / едногод. = едногодишни бюджетни кредити.

[53] ЕАСТ: Европейска асоциация за свободна търговия.

[54] Държави кандидатки и, където е приложимо, потенциални кандидатки от Западните Балкани.

	съобщителни мрежи, съдържание и технологии 09.010211 Други разходи за управление					

3.2. Очаквано отражение върху разходите

3.2.1. Обобщение на очакваното отражение върху разходите

млн. евро (до третия знак след десетичната запетая)

Функция от многогодишната финансова рамка	1 a	Конкурентоспособност за растеж и заетост

ENISA			**Базова стойност** **2017** **(31.12.2016 г.)**		**2019** ***(от 1.7.2019 г.)***	**2020**	**2021**	**2022**	**ОБЩО**
Дял 1: Разходи за персонал *(включително разходи, свързани с набирането на персонал, обучението, социална и медицинска инфраструктура и външни услуги)*	Поети задължения	(1)	6,387		9,899	12,082	13,349	13,894	**49,224**
	Плащания	(2)	6,387		9,899	12,082	13,349	13,894	**49,224**
Дял 2: Разходи за инфраструктура и оперативни разходи	Поети задължения	(1 a)	1,770		1,957	2,232	2,461	2,565	**9,215**
	Плащания	(2 a)	1,770		1,957	2,232	2,461	2,565	**9,215**
Дял 3: Оперативни разходи	Поети задължения	(3a)	3,086		4,694	6,332	6,438	6,564	**24,028**
	Плащания	(3b)	3,086		4,694	6,332	6,438	6,564	**24,028**
ОБЩО бюджетни кредити за ENISA	Поети задължения	=1+1 a +3a	**11,244**		16,550	20,646	22,248	23,023	**82,467**
	Плащания	=2+2 a +3b	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

Функция от многогодишната финансова рамка	**5**	„Административни разходи“

млн. евро (до третия знак след десетичната запетая)

		2019 *(от 1.7.2019 г.)*	**2020**	**2021**	**2022**	**ОБЩО**
ГД: „СЪОБЩИТЕЛНИ МРЕЖИ, СЪДЪРЖАНИЕ И ТЕХНОЛОГИИ“						
• Човешки ресурси		0,216	0,846	0,846	0,846	**2,754**
• Други административни разходи		0,102	0,235	0,238	0,242	**0,817**
ОБЩО за ГД CNECT	Бюджетни кредити	0,318	1,081	1,084	1,088	**3,571**

Разходите за персонал са изчислени съгласно предвидената дата на назначаване (наемане на работа е предвидено от 1.7.2019 г.)

Прогнозите за ресурсите след 2020 г. са приблизителни и не засягат предложенията на Комисията за многогодишната финансова рамка за периода след 2020 г.

ОБЩО бюджетни кредити за ФУНКЦИЯ 5 от многогодишната финансова рамка	(Общо поети задължения = Общо плащания)	0,318	1,081	1,084	1,088	**3,571**

млн. евро (до третия знак след десетичната запетая)

		2019	**2020**	**2021**	**2022**	**ОБЩО**
ОБЩО бюджетни кредити	Поети задължения	16,868	21,727	23,332	24,11	**86,038**

за ФУНКЦИИ 1—5 от многогодишната финансова рамка	Плащания	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Очаквано отражение върху бюджетните кредити за агенцията

– ☐ 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:

Бюджетни кредити за поети задължения в млн. EUR (до третия знак след десетичната запетая)

Да се посочат целите и резултатите[55] ⇩	**2019**	**2020**	**2021**	**2022**	**ОБЩО**
Увеличаване на способностите и подготвеността на държавите членки и предприятията	1,408	1,900	1,931	1,969	7,208
Подобряване на сътрудничеството и координацията между държавите членки и институциите, агенциите и органите на ЕС.	0,939	1,266	1,288	1,313	4,806
Увеличаване на способностите на равнище ЕС за допълване на действията на държавите членки, по-специално при трансгранични кризи на киберсигурността.	0,704	0,950	0,965	0,985	3,604
Повишаване на осведомеността на гражданите и предприятията по въпроси, свързани с киберсигурността	0,704	0,950	0,965	0,985	3,604
Укрепване на доверието в цифровия единен пазар и в цифровите иновации чрез повишаване на цялостната прозрачност на обезпечаването на киберсигурността на ИКТ продукти и услуги.	0,939	1,266	1,288	1,313	4,806
ОБЩО РАЗХОДИ	4,694	6,332	6,437	6,565	24,028

[55] В тази таблица са посочени единствено оперативните разходи по дял 3.

3.2.3. Очаквано отражение върху човешките ресурси на Агенцията

3.2.3.1. Обобщение

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

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

млн. евро (до третия знак след десетичната запетая)

	Q3/4 2019	**2020**	**2021**	**2022**
Временно наети лица (степени AD)	4,242	5,695	6,381	6,709
Временно наети лица (степени AST)	1,601	1,998	2,217	2,217
Договорно наети служители	2,041	2,041	2,041	2,041
Командировани национални експерти	0,306	0,447	0,656	0,796
ОБЩО	**8,190**	**10,181**	**11,295**	**11,763**

Разходите за персонал са изчислени съгласно предвидената дата на назначаване (за настоящия персонал на ENISA наемането на работа е предвидено от 1.1.2019 г.) За новия персонал е предвидено постепенно наемане на работа от 1.7.2019 г. и достигане на пълна заетост през 2022 г. Прогнозите за ресурсите след 2020 г. са приблизителни и не засягат предложенията на Комисията за многогодишната финансова рамка за периода след 2020 г.

Очаквано отражение върху персонала (допълнителни ЕПРВ) — щатно разписание

Категория и степен	2017 **Актуално състояние ENISA**	Q3/Q4.2019	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	
AD5					

Общо AD	34	9	8	6	3
AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST 3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
Общо AST	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
Общо AST/SC					
ОБЩО ВСИЧКО	48	12	10	7	3

Задачите, предвидени за допълнителния персонал AD/AST с оглед на постигането на целите на инструмента, както е описано в раздел 1.4.2:

Задачи	AD	AST	SNE	Общо
Политика и изграждане на капацитет	8	1		9
Оперативно сътрудничество	8	1	7	16
Сертифициране (свързани с пазара задачи)	9	3	2	14
Познания, информация и осведоменост	1	1		2
ОБЩО	26	6	9	41

Описание на задачите, които трябва да се изпълнят:

Задачи	**Необходими допълнителни ресурси**
Разработване и прилагане на политиката на ЕС и изграждане на капацитет	Задачите включват оказване на съдействие на групата за сътрудничество, подпомагане на трансгранично съгласувано прилагане на МИС, редовни доклади за състоянието на прилагането на правната рамка на ЕС; консултиране и координиране на секторните инициативи в областта на киберсигурността

	включително в енергетиката, транспорта (напр. въздушния, автомобилния и морския транспорт/свързани превозни средства), здравеопазването, финансите, осигуряване на подкрепа за създаването на центрове за споделяне на информация и анализи (ISAC) в различни сектори.
Оперативно сътрудничество и управление на кризи	**Задачите включват:** осигуряване на секретариат на мрежата на CSIRT като се гарантира, наред с другото, доброто функциониране на ИТ инфраструктурата и комуникационните канали на мрежата на CSIRT. Осигуряване на структурирано сътрудничество със CERT-EU, EC3 и други имащи отношение органи на ЕС. Организиране на **учения Cyber Europe**[56] — задачи, свързани с увеличаване на честотата на ученията — от веднъж на две години до веднъж годишно — и осигуряване на поглед върху цялостното протичане на инцидентите по време на ученията. **Техническа помощ** — задачите ще включват структурирано сътрудничество със CERT-EU за предоставяне на техническа помощ в случай на сериозни инциденти и за подпомагане на анализите на инцидентите. Това ще включва оказване на помощ на държавите членки при справянето с инциденти и анализа на уязвими точки, артефакти и инциденти. улесняване на сътрудничеството между отделните държави членки по отношение на незабавното реагиране чрез анализиране и обобщаване на националните доклади за ситуацията въз основа на информацията, предоставена на Агенцията от държавите членки и други субекти. **Концепция за координирана реакция на мащабни трансгранични киберинциденти** — Агенцията ще допринесе за разработването на колективна реакция на равнище ЕС и

[56] Cyber Europe е най-голямото и широкообхватно учение за киберсигурност в ЕС до момента и в него участват повече от 700 специалисти в сферата на киберсигурността от всички 28 държави членки. То се провежда на всеки две години. Оценката на ENISA и Стратегията на ЕС за киберсигурност от 2013 г. показват, че много заинтересовани страни подкрепят превръщането на Cyber Europe в ежегодно събитие предвид бързото развитие на киберзаплахите. Понастоящем това обаче не е възможно поради ограничените ресурси на Агенцията.

	държави членки на мащабни трансгранични инциденти или кризи във връзка с киберсигурността чрез редица задачи — от принос за осигуряването на ситуационна осведоменост на равнище ЕС до изпитване на плановете за сътрудничество при инциденти. **Последващи технически разследвания на инциденти** — Агенцията ще ръководи или участва в последващи технически разследвания на инциденти съвместно с мрежата на CSIRT с оглед издаването на препоръки и укрепването на способностите посредством обществено достъпни доклади с цел по-сигурно предотвратяване на бъдещи инциденти.
Задачи, свързани с пазара (стандартизация, сертифициране):	Задачите ще включват оказване на активна подкрепа на започнатата работа в рамката за сертифициране, включително осигуряване на технически експертен опит при подготовката на проекти за европейски схеми за сертифициране на киберсигурността. Задачите ще включват също така подкрепа за разработването и прилагането на политиката на Съюза за стандартизация, сертифициране и „обсерватория на пазара“ на киберсигурността, което ще изисква улесняване на въвеждането на стандарти за управление на риска за електронните продукти, мрежи и услуги, както и консултиране на операторите на основни услуги и доставчиците на цифрови услуги за техническите изисквания за сигурност. Задачите ще включват и осигуряване на анализ на основните тенденции на пазара на киберсигурността.
Познания, информация и повишаване на осведомеността:	С оглед да се осигури по-лесен достъп до по-добре структурирана информация относно рисковете за киберсигурността и потенциалните средства за защита, предложението възлага на Агенцията нова задача за разработване и поддържане на „информационен център“ на Съюза. Част от задачите му ще бъдат да събира, организира и предоставя на разположение на обществеността чрез специален портал осигурена от институциите, агенциите и органите на ЕС информация относно сигурността на мрежовите и

	информационните системи. Задачите включват и подкрепа за дейностите на ENISA в областта повишаването на осведомеността, за да може Агенцията да увеличи приноса си.

3.2.3.2. Очаквани нужди от човешки ресурси за отговарящата ГД

– ☐ Предложението/инициативата не налага използване на човешки ресурси.

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

Оценката се посочва в цели стойности (или най-много до един знак след десетичната запетая)

		Допълнителен персонал			
	Базов сценарий 2017 г.	3/4 трим. 2019	2020	2021	2020
• **Длъжности в щатното разписание (длъжностни лица и временно наети лица)**					
09 01 01 01 (Централа и представителства на Комисията)	1	2	3		
• **Външен персонал (в еквивалент на пълно работно време — ЕПРВ)**[57]					
09 01 02 01 (ДНП, КНЕ, ПНА от общия финансов пакет)	1	2			
ОБЩО		**4**	**3**		

Описание на възложените задачи:

Длъжностни лица и временно наети служители	Представляват Комисията в управителния съвет на агенцията. Изготвят становището на Комисията относно единния програмен документ на ENISA и следят за неговото изпълнение. Осъществяват надзор при изготвянето на бюджета на агенцията и наблюдават изпълнението му. Съдействат на агенцията при разработването на нейните дейности в съответствие с политиките на Съюза, включително чрез участие в съответните заседания. Осъществяват надзор на изпълнението на рамката за европейските схеми за сертифициране на киберсигурността

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

	на ИКТ продукти и услуги. Поддържат контакти с държавите членки и съответните заинтересовани страни във връзка с усилията за сертифициране. Сътрудничат с ENISA по проектите за схеми. Подготвят проекти за европейски схеми за киберсигурността.
Външен персонал	Както по-горе

3.2.4. Съвместимост с настоящата многогодишна финансова рамка

– ☐ Предложението/инициативата е съвместимо с настоящата многогодишна финансова рамка.

– ☒ Предложението/инициативата налага препрограмиране на съответната функция от многогодишната финансова рамка.

Предложението налага препрограмирането на статия 09 02 03 поради преразглеждането на мандата на ENISA, с което на Агенцията се възлагат нови задачи, свързани наред с другото с изпълнението на Директивата за МИС и Европейската рамка за сертифициране на киберсигурността. Съответни суми:

Година	Предвидени	Искане
2019	10,739	16,550
2020	10,954	20,646
2021	Не се прилага	22,248*
2022	Не се прилага	23,023*

* Стойността е прогнозна. Финансирането от страна на ЕС след 2020 г. ще бъде проверено в рамките на дискусия на Комисията по всички предложения за периода след 2020 г. Това означава, че след като направи своето предложение за следващата многогодишна финансова рамка, Комисията ще представи изменена законодателна финансова обосновка, в която са взети предвид заключенията на оценката на въздействието[58].

– ☐ Предложението/инициативата налага да се използва Инструментът за гъвкавост или да се преразгледа многогодишната финансова рамка[59].

3.2.5. Участие на трети страни във финансирането

– ☐ Предложението/инициативата не предвижда съфинансиране от трети страни.

[58] Връзка към страницата с оценката на въздействието.

[59] Вж. членове 11 и 17 от Регламент (ЕС, Евратом) № 1311/2013 на Съвета за определяне на многогодишната финансова рамка за годините 2014—2020.

– ☒ Предложението/инициативата предвижда съфинансиране съгласно следните прогнози:

	Година **2019**	Година **2020**	Година **2021**	Година **2022**
ЕАСТ	p.m[60].	p.m.	p.m.	p.m.

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

[60] Точният размер за следващите години ще стане известен, когато коефициентът за пропорционалност на ЕАСТ бъде определен за съответната година.