

BG

BG

BG



ЕВРОПЕЙСКА КОМИСИЯ

Брюксел, 30.9.2010
COM(2010) 521 окончателен

2010/0275 (COD)

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно Европейската агенция за мрежова и информационна сигурност (ENISA)

{SEC(2010) 1126}

{SEC(2010) 1127}

ОБЯСНИТЕЛЕН МЕМОРАНДУМ

1. КОНТЕКСТ НА ПРЕДЛОЖЕНИЕТО

1.1. Политически контекст

Европейската агенция за мрежова и информационна сигурност (ENISA) е създадена през март 2004 г. за първоначален период от пет години с Регламент (ЕО) № 460/2004¹, с основната цел за *„гарантиране на високо и ефективно ниво на мрежова и информационна сигурност в рамките на [Съюза], [...] и с цел развитие на култура на мрежова и информационна сигурност в полза на гражданите, потребителите, предприятията и организациите от общественения сектор на Европейския съюз, с което да се допринесе за безпрепятственото функциониране на вътрешния пазар“*. С Регламент (ЕО) № 1007/2008² мандатът на ENISA беше удължен до март 2012 г.

С удължаването на мандата на ENISA през 2008 г. също така беше поставено началото на дебат за общата насока на европейските усилия за мрежовата и информационна сигурност (МИС), за който Комисията допринесе чрез започване на обществено допитване относно възможните цели за една по-развита политика за МИС на ниво Европейски съюз. Общественото допитване се проведе от ноември 2008 г. до януари 2009 г. и събра близо 600 приноса³.

На 30 март 2009 г. Комисията прие Съобщение относно защитата на критичната информационна инфраструктура⁴ (СИИ), фокусирано върху защитата на Европа от кибернетични атаки и кибернетични смущения чрез повишаване на подготвеността, сигурността и устойчивостта посредством план за действие, с който ENISA е призована да играе роля в тази насока, главно в подкрепа на държавите-членки. Планът за действие получи широка подкрепа в рамките на дискусиата по време на конференцията на министрите относно защитата на критичната информационна инфраструктура (СИИ), проведена в Талин, Естония, на 27 и 28 април 2009 г.⁵. В заключенията на председателството на Европейския съюз по време на конференцията се подчертава значението на *„насърчаването на оперативната подкрепа“* за ENISA; в тях се посочва, че ENISA *„осигурява ценен инструмент за подпомагане на съвместните усилия на целия Европейски съюз в тази насока“* и се подчертава необходимостта от преосмисляне и преформулиране на мандата на Агенцията *„с цел по-добро фокусиране върху приоритетите и нуждите на ЕС; придобиване на по-гъвкава способност за*

¹ 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 077, 13.3.2004 г., стр. 1).

² Регламент (ЕО) № 1007/2008 на Европейския парламент и на Съвета от 24 септември 2008 г. за изменение на 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, по отношение на срока на съществуване на агенцията (ОВ L 293, 31.10.2008 г., стр.1).

³ Обобщителният доклад за резултатите от обществената консултация *„Към засилена политика за мрежова и информационна сигурност в Европа“* е представен под формата на приложение 11 към оценката на въздействието, придружаваща настоящото предложение.

⁴ COM(2009) 149, 30.3.2009 г.

⁵ Документ за обсъждане: http://www.tallinnciip.eu/doc/discussion_paper_-_tallinn_ciip_conference.pdf

Заключения на председателството:

http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf

реагиране; развиване на умения и компетенции; увеличаване на оперативната ефективност и на цялостното влияние на Агенцията“ с цел превръщане на Агенцията в „постоянен актив за всяка държава-членка и за Европейския съюз като цяло“.

След проведено обсъждане в рамките на Съвета по далекосъобщения на 11 юни 2009 г., на което държавите-членки изразиха подкрепата си за удължаването на мандата на ENISA и увеличаването на нейните ресурси с оглед значението на МИС и новите предизвикателства в тази област, дебатът приключи по време на шведското председателството на Съюза. В резолюцията на Съвета от 18 декември 2009 г. относно европейски подход на сътрудничество по отношение на мрежовата и информационната сигурност⁶ също така се признават ролята и потенциалът на ENISA, както и необходимостта от „*допълнително развитие на ENISA за превръщането ѝ в ефикасен орган*“. В резолюцията се подчертава и необходимостта от модернизиране и укрепване на Агенцията с цел оказване на подкрепа на Комисията и държавите-членки при преодоляване на несъответствията между технологии и политика, превръщайки я в център на ЕС за експертни знания по въпроси, свързани с МИС.

1.2. Общ контекст

Информационните и комуникационни технологии (ИКТ) се превърнаха в гръбнака на европейската икономика и общество като цяло. ИКТ са уязвими за заплахи, които излизат извън националните граници и се променят в резултат на развитието на технологиите и пазара. Тъй като ИКТ са глобални, взаимосвързани и зависими от други инфраструктури, тяхната сигурност и устойчивост не могат да бъдат обезпечени чрез чисто национални и некоординирани подходи. Същевременно предизвикателствата, свързани с МИС, бележат динамично развитие. Мрежовите и информационни системи трябва да бъдат ефективно защитени срещу всякакви видове смущения и срывове, включително и от извършени от хора атаки.

Политиките относно мрежовата и информационна сигурност (МИС) играят ключова роля в Програмата в областта на цифровите технологии за Европа⁷ (DAE), водеща инициатива в рамките на стратегията „ЕС — 2020“, за използване и укрепване на потенциала на ИКТ и за превръщането на този потенциал в устойчив растеж и иновации. Насърчаването на въвеждането на ИКТ и изграждането на доверие в информационното общество са ключови приоритети на DAE.

Първоначално ENISA беше създадена, за да гарантира високо и ефективно ниво на мрежова и информационна сигурност в рамките на Съюза. Натрупаният опит с Агенцията, както и предизвикателствата и заплахите, свидетелстват за необходимост от модернизиране на мандата на Агенцията, така че по-добре да отговори на нуждите на Европейския съюз, произтичащи от:

- фрагментираността на националните подходи за справяне с развиващите се предизвикателства;
- липсата на модели за сътрудничество при прилагането на политиките за МИС;

⁶ Резолюция на Съвета от 18 декември 2009 г. относно европейски подход на сътрудничество по отношение на мрежовата и информационната сигурност (ОВ С 321, 29.12.2009 г., стр. 1), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:BG:PDF>.

⁷ COM(2010) 245, 19.5.2010 г.

- недостатъчното ниво на подготвеност, дължащо се и на ограничената европейска способност за ранно предупреждаване и реагиране;
- липсата на надеждни европейски данни и ограничените познания за променящите се проблеми;
- ниската степен на осведоменост за рисковете и предизвикателствата в сферата на МИС;
- предизвикателството аспектите на МИС да бъдат интегрирани в политиките за по-ефективна борба срещу кибернетичните престъпления.

1.3. Цели на политиката

Общата цел на предложения регламент е да се позволи на ЕС, държавите-членки и заинтересованите страни да развият висока степен на способност и подготвеност за предотвратяване, установяване и по-добро реагиране на проблеми в сферата на МИС. Това ще допринесе за изграждане на доверие, което е в основата на развитието на информационното общество, за повишаване на конкурентоспособността на европейските предприятия и за обезпечаване на ефективно функциониране на вътрешния пазар.

1.4. Съществуващи разпоредби в областта на предложението

Настоящото предложение допълва регулаторните и нерегулаторните политически инициативи в областта на мрежовата и информационна сигурност, предприети на нивото на Европейския съюз с цел засилване на сигурността и устойчивостта на ИКТ:

- В плана за действие, стартиран със съобщението относно СИР, беше предвидено създаването на:
 - (1) Европейски форум за държавите-членки (EFMS), чиято цел е насърчаване на дискусиите и обмена в сферата на добрите политически практики с оглед споделяне на политически цели и приоритети относно сигурността и устойчивостта на инфраструктурата на ИКТ, който също така пряко се възползва от дейността и подкрепата на Агенцията.
 - (2) Европейско публично-частно партньорство за устойчивост (EP3R), представляващо гъвкава общоевропейска ръководна рамка за устойчивост на инфраструктурата на ИКТ, което функционира чрез насърчаване на сътрудничеството между публичния и частния сектор за целите на сигурността и устойчивостта, основните изисквания, добрите политически практики и мерки.
- Програмата от Стокхолм, приета от Европейския Съвет на 11 декември 2009 г., подкрепя политиките, с които се осигурява мрежова сигурност и се дава възможност за по-бързо реагиране в случай на кибернетични атаки в Съюза.
- Тези инициативи допринасят за практическата реализация на Програмата в областта на цифровите технологии за Европа. Политиките относно МИС играят централна роля в онази част от стратегията, която е насочена към повишаване на доверието в информационното общество. Те също така подкрепят мерките за подпомагане и

политиката на Комисията по отношение на защитата на неприкосновеността на личния живот (най-вече „неприкосновеност на личния живот чрез проектното решение“) и личните данни (преразглеждане на рамката), мрежата за сътрудничество в областта на защитата на потребителите (CPC), управлението на личните данни и Програмата за по-безопасен интернет.

1.5. **Новости в настоящата политика за МИС във връзка с предложението**

Няколко нови тенденции в сферата на политиката за МИС, най-вече посочените в Програмата в областта на цифровите технологии за Европа, се възползват от подкрепата и експертните знания на ENISA. Те включват:

- Укрепване на сътрудничеството в сферата на политиката за МИС чрез засилване на дейностите в **Европейския форум на държавите-членки (EFMS)**, което, заедно с пряката подкрепа от страна на ENISA, ще подпомогне за:
 - определяне на начини за изграждане на ефективна европейска мрежа чрез трансгранично сътрудничество между националните/правителствени екипи за незабавно реагиране при компютърни инциденти (CERT);
 - установяване на дългосрочни цели и приоритети за мащабни общоевропейски учения в областта на инциденти, свързани с МИС;
 - установяване на минимални изисквания по отношение възлагането на обществени поръчки с цел повишаване на сигурността и устойчивостта на публичните системи и мрежи;
 - определяне на икономически и регулаторни стимули за сигурност и устойчивост;
 - оценяване на състоянието на МИС в Европа.
- Засилване на сътрудничеството и партньорството между публичния и частния сектор чрез подпомагане на **Европейското публично-частно партньорство за устойчивост (EP3R)**. ENISA играе все по-голяма роля при улесняването на заседанията и дейностите на EP3R. Следващите стъпки на EP3R ще включват:
 - Обсъждане на иновационни мерки и инструменти за подобряване на сигурността и устойчивостта, например:
 - (1) основни изисквания относно сигурността и устойчивостта, по-специално в сферата на обществените поръчки за ИКТ продукти или услуги, които да осигурят равни условия и същевременно да гарантират подходящо ниво на подготвеност и превантивни действия;
 - (2) разглеждане на въпросите за отговорността на икономическите субекти, например при прилагането на минималните изисквания относно сигурността;
 - (3) икономически стимули за разработване и въвеждане на практики за управление на риска и на процеси и продукти, свързани със сигурността;

- (4) схеми за оценка и управление на риска, с които да се оценяват и управляват сериозни инциденти при обща основа на разбиране;
 - (5) сътрудничество между частния и публичния сектор в случай на мащабни инциденти;
 - (6) организиране на **бизнес среща на високо ниво** относно икономическите бариери и стимули за сигурност и устойчивост.
- Практическа реализация на изискванията относно сигурността, заложи в регулаторния пакет за електронни комуникации, за което са необходими експертните знания и съдействието на ENISA с оглед:
 - оказване на подкрепа на държавите-членки и Комисията, като се вземат под внимание мненията на частния сектор по целесъобразност, за разработване на рамка от правила и процедури за въвеждане на разпоредбите за уведомяване за пробиви в сигурността (заложи в член 13, буква а) от преработената Рамкова директива).
 - учредяване на годишен форум за националните компетентни органи/националните регулаторни органи в сферата на МИС и заинтересовани страни от частния сектор с цел обсъждане на направените изводи и обмен на добри практики за прилагане на регулаторни мерки за МИС.
 - Улесняване на **ученията за подготовка във връзка с кибернетичната сигурност в целия ЕС** с подкрепата на Комисията и с приноса на ENISA, с оглед последващо провеждане на тези учения и на международно ниво.
 - **Изграждане на CERT (екип за незабавно реагиране при компютърни инциденти) за институциите на ЕС.** Основно действие 6 от Програмата в областта на цифровите технологии за Европа гласи, че Комисията ще представи „мерки за засилена политика за мрежова и информационна сигурност на високо равнище, включващи [...] мерки, позволяващи по-бързо реагиране в случаи на кибератаки, включително екипи за незабавно реагиране при компютърни инциденти в европейските институции“⁸. Това ще изисква Комисията и другите институции на Съюза да анализират и създадат екип за незабавно реагиране при компютърни инциденти, за което ENISA може да предостави техническа подкрепа и експертни знания.
 - Мобилизиране и подпомагане на държавите-членки при попълването, а при необходимост и при създаването на **национални/правителствени CERT с цел изграждане на добре функционираща мрежа от CERT, покриваща цяла Европа.** Тази дейност също така ще способства за доразработването на Европейска система

⁸ Резолюция на Съвета от 18 декември 2009 г. относно европейски подход на сътрудничество по отношение на мрежовата и информационната сигурност „Съветът [...] признава [...] значението да се проучат стратегическите последствия, рискове и перспективи от създаването на CERT за институциите на ЕС и да се обмисли евентуална бъдеща роля на ENISA в тази област“.

за информационен обмен и предупреждаване (EISAS) за граждани и МСП, която трябва да бъде изградена с национални ресурси и капацитет до края на 2012 г.

- **Повишаване на осведомеността** за предизвикателствата в сферата на МИС, което ще включва:
 - съвместна работа на Комисията и ENISA за съставяне на насоки за насърчаване на стандартите за МИС, добри практики и култура на управление на риска. Ще бъдат изготвени първите примерни насоки.
 - Организиране от страна на ENISA, в сътрудничество с държавите-членки, на **„Европейски месец на мрежовата и информационна сигурност за всички“** с национални/европейски състезания по кибернетична сигурност.

1.6. Съгласуваност с други политики и цели на Съюза

Предложението е съгласувано със съществуващите политики и цели на Европейския съюз и напълно съответства на целта за осъществяване на принос към безпрепятственото функциониране на вътрешния пазар чрез повишаване на подготвеността и на способността за реагиране на предизвикателствата в сферата на мрежовата и информационна сигурност.

2. РЕЗУЛТАТИ ОТ КОНСУЛТАЦИИТЕ И ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО

2.1. Консултация със заинтересованите страни

Настоящата политическа инициатива е резултат на широкообхватни дискусии, проведени съгласно приобщаващ подход и при спазването на принципите на участие, откритост, отчетност, ефективност и съгласуваност. Осъщественият обширен процес включи оценка на Агенцията през 2006—2007 г., последвана от препоръки от страна на Управителния съвет на ENISA, две обществени консултации (през 2007 г. и през 2008—2009 г.), както и редица семинари по въпроси, свързани с МИС.

Първата обществена консултация беше организирана във връзка със Съобщението на Комисията относно средносрочната оценка на ENISA. Консултацията, насочена към бъдещето на Агенцията, беше проведена между 13 юни и 7 септември 2007 г. и получи общо 44 отзива по интернет, както и два в писмен вид. Отговорите дойдоха от разнообразни заинтересовани страни и проявяващи интерес лица, включително министерства на държави-членки, регулаторни органи, индустриални и потребителски асоциации, академични институции, компании и отделни граждани.

В отговорите се подчертават редица интересни въпроси относно развитието на сценария за заплаха; необходимостта от изясняване и повишаване на гъвкавостта на регламента с оглед адаптирането на ENISA към предизвикателствата; важноста на обезпечаването на ефективно взаимодействие със заинтересованите страни; както и възможността за ограничено нарастване на нейните ресурси.

Целта на втората обществена консултация, проведена от 7 ноември 2008 г. до 9 януари 2009 г., беше определяне на приоритетните цели за укрепване на политиката за МИС на европейско ниво и средствата за постигане на тези цели. Бяха получени близо 600 отзива от органи на държави-членки, академични/научноизследователски институции,

индустриални асоциации, частни компании и други заинтересовани страни, като например организации и консултантски агенции за защита на данните, както и частни лица.

Голяма част от анкетираните⁹ подкрепиха удължаването на мандата на Агенцията и по-голямата ѝ роля при координирането на дейностите в сферата на МИС на европейско ниво, както и увеличаването на нейните ресурси. Сред очертаните ключови приоритети бяха необходимостта от по-координиран подход към кибернетичните заплахи в цяла Европа, транснационалното сътрудничество в отговор на мащабни кибернетични атаки, изграждането на доверие и подобряването на информационния обмен сред заинтересованите страни.

По отношение на предложението беше проведена оценка на въздействието, с начало през септември 2009 г., въз основа на подготвително проучване, извършено от външен изпълнител. В процеса взеха участие широк кръг заинтересовани страни и експерти. Сред участниците бяха органи на държави-членки в областта на МИС, национални регулаторни органи, телекомуникационни оператори, доставчици на интернет услуги и свързани с тях отраслови асоциации, потребителски асоциации, производители на ИКТ, екипи за незабавно реагиране при компютърни инциденти (CERT), академици и корпоративни потребители. Беше създадена междуведомствена ръководна група, съставена от представители на съответните генерални дирекции на Комисията, чиято задача е да подпомогне процеса на изготвяне на оценката на въздействието.

2.2. Оценка на въздействието

Запазването на Агенцията беше сметено за подходящо решение за постигане на целите на европейската политика¹⁰. След предварителен подбор бяха избрани пет варианта на политика, които да бъдат подложени на допълнителен анализ:

- Вариант 1 — Липса на политика;
- Вариант 2 — Продължаване без изменения, т.е. с подобен мандат и при същото ниво на ресурсите;
- Вариант 3 — Разширяване на задачите на ENISA и добавяне на органите за правоприлагане и защита на неприкосновеността на личния живот като пълноправни заинтересовани страни;
- Вариант 4 — Добавяне на борбата срещу кибернетичните атаки и реагирането на кибернетични инциденти към нейните задачи;
- Вариант 5 — Добавяне на подкрепата на правоприлагащите и на съдебните органи при борбата срещу кибернетичните престъпления към нейните задачи.

След провеждане на сравнителен анализ на разходите и ползите вариант 3 беше определен като най-рентабилният и ефективен начин за постигане на целите на политиката.

⁹ Вж. приложение XI към оценката на въздействието.

¹⁰ Вж. приложение IV към оценката на въздействието.

Във вариант 3 се предвижда разширяване на ролята на ENISA с фокусиране върху:

- изграждане и поддържане на мрежа за връзка между заинтересованите страни и мрежа за знания с цел обезпечаване на пълната информираност на ENISA за контекста на МИС в Европа;
- превръщане на Агенцията в център за подпомагане на МИС чрез разработване и прилагане на политики (по-специално по отношение на правото на неприкосновеност на личния живот и електронните съобщения, електронния подпис, електронната идентификация и стандартите за обществени поръчки във връзка с МИС);
- подпомагане на политиката на ЕС по отношение на СИП и политиката за устойчивост (учения, ЕРЗР, Европейска система за информационен обмен и предупреждаване и др.);
- създаване на рамка на ЕС за събирането на данни във връзка с МИС, включително разработване на методи и практики за изисквани от закона задължения за докладване и споделяне на данни;
- изследване на икономиката на МИС;
- стимулиране на сътрудничеството с трети държави и международни организации с цел насърчаване на общ глобален подход към въпросите на МИС и придаване на тежест на международни инициативи на високо ниво в Европа);
- осъществяване на задачи с неоперативен характер, свързани с аспекти на МИС, в областта на кибернетичните престъпления и съдебното сътрудничество.

3. ПРАВНИ ЕЛЕМЕНТИ НА ПРЕДЛОЖЕНИЕТО

3.1. Обобщение на предлаганите мерки

Предложеният регламент има за цел укрепването и модернизирването на Европейската агенция за мрежова и информационна сигурност (ENISA), както и установяването на нов мандат за период от пет години.

Предложението включва някои ключови промени в сравнение с първоначалния регламент:

- (1) **Увеличаване на гъвкавостта, приспособимостта и способността за тясна насоченост.** Задачите са цялостно актуализирани и преформулирани с цел разширяване обхвата на дейностите на Агенцията; те са достатъчно прецизни, за да опишат средствата за постигане на целите. По този начин мисията на Агенцията получава по-добра насоченост, подобрява се нейната способност за постигане на целите и се укрепват задачите ѝ за подпомагане на прилагането на политиката на Съюза.
- (2) **По-добро обвързване на Агенцията с политиката и регулаторния процес на Съюза.** Европейските институции и органи могат да се обръщат към Агенцията за съдействие и консултации. Това е в съответствие с политическите и регулаторни тенденции: Съветът е започнал да се обръща директно към Агенцията в резолюции, а Европейският парламент и Съветът са възложили на

Агенцията задачи, свързани с мрежовата и информационна сигурност, в регулаторната рамка за електронни съобщения.

- (3) **Взаимовръзка с борбата срещу кибернетичните престъпления.** При постигането на своите цели Агенцията взема под внимание борбата срещу кибернетичните престъпления. Органите за правоприлагане и защита на неприкосновеността на личния живот стават пълноправни заинтересовани страни в Агенцията, най-вече в Постоянната група на заинтересовани страни.
- (4) **Укрепена структура на управление.** Предложението подчертава надзорната роля на Управителния съвет на Агенцията, в който са представени държавите-членки и Комисията. Например, Управителният съвет може да издава общи инструкции относно свързани с персонала въпроси, което преди беше отговорност единствено на изпълнителния директор. Той може също така да учредява оперативни органи, които да му съдействат при изпълнението на неговите задачи, включително наблюдение на изпълнението на неговите решения.
- (5) **Оптимизиране на процедурите.** Процедури, които са се оказали ненужно тромави, са опростени. Примери: а) опростена процедура за вътрешния правилник на Управителния съвет, б) становището за работната програма на ENISA се издава от службите на Комисията, а не чрез решение на Комисията. Управителният съвет също така получава достатъчни ресурси, в случай че трябва да приема изпълнителни решения и да ги прилага (например ако член на персонала подаде жалба срещу изпълнителния директор или самия Управителен съвет).
- (6) **Постепенно увеличаване на ресурсите.** С цел да отговори на засилените европейски приоритети и разрастващите се предизвикателства, без това да засяга предложението на Комисията за следващата многогодишна финансова рамка, се предвижда финансовите и човешки ресурси на Агенцията да нараснат постепенно в периода 2012—2016 г. Въз основа на предложението на Комисията за регламент за определяне на многогодишна финансова рамка след 2013 г. и предвид заключенията на оценката на въздействието Комисията ще представи изменена законодателна финансова обосновка.
- (7) **Вариант за удължаване на мандата на изпълнителния директор.** Управителният съвет може да удължи мандата на изпълнителния директор с три години.

3.2. Правно основание

Настоящото предложение се основава на член 114 от Договора за функционирането на Европейския съюз (ДФЕС)¹¹.

В съответствие с решение на Съда на Европейските общности¹², преди влизането в сила на Договора от Лисабон **член 95 от Договора за ЕО** се считаеше за подходящото правно

¹¹ ОВ С 115, 9.5.2008 г., стр. 94.

¹² Съд на Европейските общности, 2.5.2006 г., С-217/04, *Обединено кралство на Великобритания и Северна Ирландия/Европейски парламент и Съвет на Европейския съюз*.

основание за създаването на орган с цел осигуряване на високо и ефективно ниво на МИС в рамките на Съюза. Използвайки израза „мерки за сближаване“ в член 95 авторите на договора са имали за цел да предоставят на законодателството на Съюза правото на избор на подходящи мерки за постигане на желанния резултат. Поради това засилването на сигурността и устойчивостта на инфраструктурите на ИКТ представлява важен елемент, допринасящ за безпрепятственото функциониране на вътрешния пазар.

По смисъла на Договора от Лисабон **член 114 от ДФЕС**¹³ описва — почти по същия начин — отговорността за вътрешния пазар. Поради горепосочените причини той ще продължи да представлява приложимото правно основание за приемането на мерки за подобряване на МИС. Понастоящем отговорността за вътрешния пазар е в съвместните компетенции на Съюза и държавите-членки (член 4, параграф 2, буква а) от ДФЕС). Това означава, че Съюзът и държавите-членки могат да приемат мерки (със задължителен характер), както и че държавите-членки ще предприемат действия, ако Съюзът не упражни своите компетенции или реши да прекрати действията си (член 2, параграф 2 от ДФЕС).

Мерките в рамките на отговорността за вътрешния пазар ще изискват обикновената законодателна процедура (членове 289 и 294 от ДФЕС), която е подобна¹⁴ на предходната процедура за съвместно вземане на решения (член 251 от Договора за ЕО).

Договорът от Лисабон премахна предходното разграничение между стълбовете. Предотвратяването и борбата с престъпността се превърнаха в съвместна компетенция на Съюза. По този начин беше създадена възможността ENISA да служи като платформа за свързаните с МИС аспекти на борбата с кибернетичните престъпления, както и да обменя мнения и най-добри практики с органи за кибернетична отбрана, правоприлагане и защита на неприкосновеността на личния живот.

3.3. Принцип на субсидиарност

Предложението съответства на принципа на субсидиарност: политиката за МИС изисква подход на сътрудничество и целите на предложението не могат да бъдат постигнати от отделните държави-членки.

Една стратегия на пълна ненамеса в националните политики за МИС от страна на Съюза би оставила задачата на държавите-членки, пренебрегвайки ялната взаимозависимост между съществуващите информационни системи. По тази причина една мярка, която осигурява подходяща степен на координация между държавите-членки с цел гарантиране на правилно управление на свързаните с МИС рискове в трансграничния контекст на тяхното възникване, е в съответствие с принципа на субсидиарност. Освен това действие на европейско ниво би подобрило ефективността на съществуващите национални политики и по този начин би създавало добавена стойност.

В допълнение към това, разработването на съгласувана и съвместна политика за МИС ще окаже благоприятно въздействие върху защитата на основните права, и по-специално правото на защита на личните данни и на неприкосновеността на личния живот. Необходимостта от защита на данните понастоящем е критична предвид факта,

¹³ Вж. по-горе.

¹⁴ Обикновената законодателна процедура се различава по-специално от гледна точка на изискванията за необходимото мнозинство в Съвета и Европейския парламент.

че европейските граждани все повече поверяват своите данни на сложни информационни системи, или доброволно, или по необходимост, без задължително да са в състояние да оценят правилно съответните рискове за защитата на данните. Ето защо не е сигурно, че при възникването на инциденти те ще могат да предприемат необходимите стъпки, нито пък че държавите-членки ще са в състояние ефективно да се справят с международни инциденти при липсата на европейска координация на МИС.

3.4. Принцип на пропорционалност

Настоящото предложение е в съответствие с принципа на пропорционалност, тъй като не надхвърля необходимото за постигането на своята цел.

3.5. Избор на инструменти

Предлаган инструмент: регламент, директно приложим във всички държави-членки.

4. ОТРАЖЕНИЕ ВЪРХУ БЮДЖЕТА

Предложението ще има отражение върху бюджета на Съюза.

Тъй като задачите, които ще бъдат включени в новия мандат на ENISA, са уточнени, се очаква Агенцията да получи необходимите ресурси за задоволителното извършване на нейните дейности. Оценката на Агенцията, обстойният процес на консултации със заинтересованите страни на всички нива и оценката на въздействието показват наличието на общо съгласие, че размерът на Агенцията е под нейната критична маса и че е необходимо увеличение на ресурсите. Последствията и ефектите от увеличаването на персонала и бюджета на Агенцията са анализирани в оценката на въздействието, приложена към предложението.

Финансирането от страна на ЕС след 2013 г. ще бъде проверено в рамките на дискусия на Комисията по всички предложения за периода след 2013 г.

5. ДОПЪЛНИТЕЛНИ ЗАБЕЛЕЖКИ

5.1. Продължителност

Регламентът следва да обхване период от пет години.

5.2. Клауза за преразглеждане

Регламентът предвижда оценка на Агенцията за периода от предходната оценка през 2007 г. насам. Тя ще оцени ефективността на Агенцията при постигането на нейните цели, както са посочени в Регламента, дали тя все още представлява ефективен инструмент и дали срокът ѝ на съществуване следва да бъде допълнително удължен. Въз основа на констатациите Управителният съвет ще направи препоръки към Комисията относно промените в настоящия регламент, Агенцията и нейните работни практики. С оглед да позволи на Комисията да изготви предложение за удължаване на мандата в разумен срок, оценката ще трябва да бъде направена до края на втората година от мандата, предвиден от регламента.

5.3. Временни мерки

Комисията осъзнава, че законодателната процедура в Европейския парламент и Съвета може да изисква дълъг период от време за обсъждане на предложението и съществува риск от създаване на правен вакуум, ако новият мандат на Агенцията не бъде приет в срок преди изтичането на текущия мандат. По тази причина заедно с настоящото предложение Комисията предлага регламент за удължаване на текущият мандат на Агенцията с 18 месеца с цел осигуряване на достатъчно време за обсъждане и правилно осъществяване на процеса.

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно Европейската агенция за мрежова и информационна сигурност (ENISA)

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,

като взеха предвид становището на Европейския икономически и социален комитет¹⁵,

като взеха предвид становището на Комитета на регионите¹⁶,

след предаване на предложението на националните парламенти,

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

- (1) Електронните съобщения, инфраструктура и услуги представляват съществен фактор за икономическото и социално развитие. Те играят ключова роля за обществото и са се превърнали в широко използвани услуги, подобно на електро- и водоснабдяването. Тяхното смущаване би могло да причини значителни икономически щети, което подчертава значението на мерките за повишаване на защитата и устойчивостта с цел осигуряване на непрекъснатост на критични услуги. Сигурността на електронните съобщения, инфраструктура и услуги, по-специално тяхната цялост и наличност, са изправени пред постоянно нарастващи предизвикателства. Това е повод за нарастващо обществено безпокойство, не на последно място заради възможността от възникване на проблеми поради сложността на системата, инциденти, грешки и атаки, които могат да имат последствия за физическата инфраструктура, осигуряваща услуги от огромно значение за благосъстоянието на европейските граждани.
- (2) Картината на заплахите постоянно претърпява промени и инцидентите, свързани със сигурността, могат да застрашат доверието на потребителите. Докато сериозните смущения на електронните съобщения, инфраструктура и услуги могат да окажат значително икономическо и социално въздействие, ежедневните нарушения, проблеми и неприятности, свързани със сигурността, също излагат на риск общественото доверие в технологиите, мрежите и услугите.

¹⁵ ОВ С , , стр. .

¹⁶ ОВ С , , стр. .

- (3) В този смисъл редовното оценяване на състоянието на мрежовата и информационна сигурност в Европа въз основа на надеждни европейски данни е важно за разработването на политика, за индустрията и потребителите.
- (4) Представителите на държавите-членки решиха на срещата си на 13 декември 2003 г. седалището на Европейската агенция за мрежова и информационно сигурност (ENISA), която трябваше да бъде създадена въз основа на внесеното от Комисията предложение, да бъде установено в град в Гърция, който да бъде определен от гръцкото правителство.
- (5) През 2004 г. Европейският парламент и Съветът приеха Регламент (ЕО) № 460/2004¹⁷ относно създаване на Европейската агенция за мрежова и информационна сигурност с цел подпомагане на стремежа към осигуряване на високо ниво на мрежова и информационна сигурност в 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) № 1007/2008¹⁸ за удължаване на мандата на Агенцията до март 2012 г.
- (6) През периода след създаването на Агенцията предизвикателствата, свързани с мрежовата и информационна сигурност, се променяха успоредно с развитието на технологиите, пазарните и социално-икономически условия и бяха обект на допълнително разглеждане и дебати. В отговор на променящите се предизвикателства Съюзът актуализира своите приоритети относно политиката за мрежовата и информационна сигурност в редица документи, включително в Съобщение на Комисията от 2006 г. относно *Стратегия за сигурност на информационното общество — диалог, партньорство и оправомощаване*¹⁹, Резолюция на Съвета от 2007 г. относно Стратегия за сигурност на информационното общество в Европа²⁰, Съобщение от 2009 г. относно защитата на критичната информационна инфраструктура — „*Защита на Европа от широкомащабни кибернетични атаки и смущения: повишаване на готовността, сигурността и устойчивостта*“²¹, Заключениета на председателството от Конференцията на министрите относно защитата на критичната информационна инфраструктура (СИИР), Резолюция на Съвета от 2009 г. относно европейски подход на сътрудничество по отношение на мрежовата и информационната сигурност²². Признава се необходимостта от модернизирани и укрепване на Агенцията, така че успешно да подпомага усилията на европейските институции и на държавите-членки за изграждането на европейски капацитет за справяне с предизвикателствата в сферата на мрежовата и информационна сигурност. По-късно Комисията прие Програма в областта на цифровите технологии за Европа²³, която представляваше водеща инициатива в рамките на стратегията „Европа—2020“. Тази изчерпателна

¹⁷ ОВ L 77, 13.3.2004 г., стр. 1.

¹⁸ ОВ L 293, 31.10.2008 г., стр. 1.

¹⁹ COM(2006) 251, 31.5.2006 г.

²⁰ Резолюция на Съвета от 22 март 2007 г. относно Стратегия за сигурност на информационното общество в Европа (ОВ С 68, 24.3.2007 г., стр. 1).

²¹ COM(2009) 149, 30.3.2009 г.

²² Резолюция на Съвета от 18 декември 2009 г. относно европейски подход на сътрудничество по отношение на мрежовата и информационната сигурност (ОВ С 321, 29.12.2009 г., стр. 1).

²³ COM(2010) 245, 19.5.2010 г.

програма е насочена към използване и разширяване на потенциала на ИКТ с цел постигането на съществен растеж и новаторство. Укрепването на надеждността и доверието в информационното общество е една от ключовите цели на тази изчерпателна програма, в която са обявени множество действия на Комисията в тази област, включително настоящото предложение.

- (7) Мерките в рамките на вътрешния пазар в областта на сигурността на електронните съобщения и по-общо на мрежовата и информационна сигурност, изискват различни форми на технически и организационни приложения от страна на държавите-членки и Комисията. Разнородното прилагане на тези изисквания може да доведе до неефективни решения и да създаде препятствия пред вътрешния пазар. Това налага създаването на център за експертни знания на европейско ниво, който да дава насоки, съвети и, когато бъде призован, да предоставя помощ по въпросите на мрежовата и информационна сигурност, на която могат да разчитат държавите-членки и европейските институции. Агенцията може да отговори на тези нужди чрез разработване и поддържане на високо ниво на експертни знания и подпомагане на държавите-членки, Комисията и съответно бизнес средите, за да им помогне да изпълнят правните и регулаторни изисквания относно мрежовата и информационна сигурност, като по този начин се подпомага нормалното функциониране на вътрешния пазар.
- (8) Агенцията следва да изпълнява задачите, възложени ѝ от настоящото законодателство на Съюза в областта на електронните съобщения, и в по-общ план да допринася за увеличаване нивото на сигурност на електронните съобщения, като наред с други неща предоставя и експертни знания и консултации и насърчава обмена на добри практики.
- (9) В Директива 2002/21/ЕО на Европейския парламент и на Съвета от 7 март 2002 г. относно общата регулаторна рамка за електронните съобщителни мрежи и услуги (Рамкова директива)²⁴ се определя допълнително изискване доставчиците на обществени електронни съобщителни мрежи или обществени електронни съобщителни услуги да предприемат подходящи мерки за защита на тяхната цялост и сигурност и се въвеждат изисквания за уведомяване за пробиви в сигурността и за нарушаване на целостта. По целесъобразност Агенцията трябва да бъде уведомявана и от националните регулаторни органи, които също така трябва да представят на Комисията и Агенцията годишен обобщителен доклад за получените уведомления и предприетите действия. Освен това в Директива 2002/21/ЕО Агенцията се призовава да допринася за хармонизирането на подходящите технически и организационни мерки за сигурност чрез предоставяне на мнения.
- (10) В Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации)²⁵ се изисква доставчиците на публично достъпни електронни комуникационни услуги да предприемат необходимите технически и организационни мерки за защита на сигурността на своите услуги и също така се

²⁴ ОВ L 108, 24.4.2002 г., стр. 33.

²⁵ ОВ L 201, 31.7.2002 г., стр. 37.

изисква поверителност на комуникациите и свързаните с тях данни за трафик. Директива 2002/58/ЕО въвежда изискванията за доставчиците на електронни комуникационни услуги да информират и уведомяват за нарушение на сигурността на личните данни. Тя също така изисква Комисията да консултира Агенцията по всякакви технически мерки за изпълнение, които следва да бъдат приети във връзка с обстоятелствата или формата на изискванията за информиране и уведомяване и приложимите към това процедури. Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни²⁶ изисква държавите-членки да гарантират, че контролният орган прилага подходящи технически и организационни мерки за защита на личните данни от случайно или незаконно унищожаване или случайна загуба, промяна, неразрешено оповестяване или достъп, особено когато обработката им включва преноса на данни по мрежа, както и от всички други незаконни форми на обработка.

- (11) Агенцията следва да допринася за постигането на високо ниво на мрежова и информационна сигурност в рамките на Съюза и за създаването на култура на мрежова и информационна сигурност в полза на гражданите, потребителите, предприятията и организациите от публичния сектор в Европейския съюз, като по този начин подпомага гладкото функциониране на вътрешния пазар.
- (12) Набор от задачи следва да посочи как Агенцията да постигне своите цели, като същевременно с това ѝ даде възможност за гъвкаво функциониране. Реализираните от Агенцията задачи следва да включват събирането на подходяща информация и данни, необходими за извършването на анализи на рисковете за сигурността и устойчивостта на електронните съобщения, инфраструктура и услуги, както и за оценяването, в сътрудничество с държавите-членки, на състоянието на мрежовата и информационна сигурност в Европа. Агенцията следва да осигури координация с държавите-членки и да засили сътрудничеството между заинтересованите страни в Европа, по-специално чрез привличане на компетентни държавни органи и експерти от частния сектор в областта на мрежовата и информационна сигурност към своите дейности. Агенцията следва да окаже съдействие на Комисията и държавите-членки в диалога им с индустрията с цел решаване на свързани със сигурността проблеми с хардуерни и софтуерни продукти, като по този начин подпомогне съвместния подход към мрежовата и информационна сигурност.
- (13) Агенцията следва да служи като отправна точка и да изгражда доверие благодарение на своята независимост, качеството на консултациите, които предоставя, и на информацията, която разпространява, прозрачността на процедурите и методите ѝ на работа, както и старанието ѝ при изпълнението на възложените ѝ задачи. Агенцията следва да надгради националните усилия и тези на Съюза и по този начин да изпълнява своите задачи в пълно сътрудничество с държавите-членки и да бъде отворена за контакти с индустрията и други уместни заинтересовани страни. Освен това Агенцията следва да надгради приноса от и сътрудничеството с частния сектор, който играе

²⁶ ОВ L 281, 23.11.1995 г., стр. 31.

важна роля за сигурността на електронните съобщения, инфраструктура и услуги.

- (14) Комисията постави началото на Европейско публично-частно партньорство за устойчивост като гъвкава общоевропейска рамка за управление на устойчивостта на инфраструктурата на ИКТ, в която Агенцията следва да играе спомагателна роля, обединявайки заинтересованите страни от държавния и частния сектор с цел дискутиране на обществени политически приоритети, икономически и пазарни измерения на предизвикателствата и мерки за устойчивост на инфраструктурата на ИКТ, както и определяне на отговорността на заинтересованите страни.
- (15) Агенцията следва да предостави консултации на Комисията чрез мнения и технически и социално-икономически анализи, по молба на Комисията или по собствена инициатива, с цел да подпомогне разработването на политиката в областта на мрежовата и информационна сигурност. Агенцията следва също така да подпомага държавите-членки и европейските институции и органи по тяхна молба в усилията им за разработване на политика и капацитет за мрежова и информационна сигурност.
- (16) Агенцията следва да подпомага държавите-членки и европейските институции в усилията им за изграждане и увеличаване на трансграничната способност и подготвеност за предотвратяване, установяване, смекчаване и реагиране на проблеми и инциденти, свързани с мрежовата и информационна сигурност; в това отношение Агенцията следва да улесни сътрудничеството между държавите-членки и между държавите-членки и Комисията. За целта Агенцията следва да играе активна роля в подкрепата на постоянните усилия на държавите-членки за подобряване на тяхната способност за реагиране, както и за организиране и провеждане на национални и европейски учения за инциденти, свързани със сигурността.
- (17) Директива 95/46/ЕО регламентира обработката на лични данни, извършвана при условията на настоящия регламент.
- (18) С цел по-добро разбиране на предизвикателствата в сферата на мрежовата и информационна сигурност, Агенцията трябва да анализира текущите и нововъзникващи рискове. За целта тя следва, в сътрудничество с държавите-членки и по целесъобразност със статистически органи, да събира съответната информация. Освен това Агенцията следва да подпомага държавите-членки и европейските институции и органи в усилията им за събиране, анализиране и разпространение на данни за мрежовата и информационна сигурност.
- (19) При осъществяването на дейности по наблюдение в Съюза Агенцията следва да улесни сътрудничеството между Съюза и държавите-членки по отношение на оценяването на състоянието на мрежовата и информационна сигурност в Европа и да подпомогне дейностите по оценяване в сътрудничество с държавите-членки.
- (20) Агенцията следва да улесни сътрудничеството между компетентните държавни органи на държавите-членки, по-специално в подкрепа на разработването и обмена на добри практики и стандарти за образователни програми и схеми за

повишаване на осведомеността. Увеличаването на информационния обмен между държавите-членки ще улесни подобна дейност. Агенцията следва също така да подкрепи сътрудничеството между заинтересовани страни от публичния и частния сектор на нивото на Европейския съюз, отчасти чрез насърчаване на споделянето на информация, кампании за повишаване на осведомеността и образователни и обучителни програми.

- (21) Ефективните политики на сигурност следва да се основават на добре разработени методи за оценяване на риска както в публичния, така и в частния сектор. Методите и процедурите за оценка на риска се използват на различни нива, без да има обща практика в ефективното им прилагане. Насърчаването 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 повишат нивото на сигурност на мрежите и информационните системи в Европа. За целта Агенцията следва да подкрепя сътрудничеството между заинтересовани страни от публичния и частния сектор на нивото на Европейския съюз, като улеснява техните усилия, свързани с разработването и използването на стандарти за управление на риска и за измерима сигурност на електронните продукти, системи, мрежи и услуги.
- (22) В работата си Агенцията следва да използва текущата научноизследователска и развойна дейност и дейностите за оценка на технологиите, по-специално тези, извършвани от различните научноизследователски инициативи на Европейския съюз.
- (23) В случаите, когато е уместно и полезно за изпълнението на обхвата, целите и задачите си, Агенцията следва да споделя опит и обща информация с органите и агенциите, създадени по силата на законодателството на Европейския съюз и занимаващи се с въпросите на мрежовата и информационна сигурност.
- (24) В сътрудничеството си с правоприлагащите органи относно свързаните със сигурността аспекти на кибернетичните престъпления Агенцията спазва съществуващите информационни канали и изградени мрежи, например контактните звена, посочени в предложението за директива на Европейския парламент и на Съвета относно атаките срещу информационните системи, отменяща Рамково решение 2005/222/ПВР, или работната група на началниците на отделите за високотехнологични престъпления към Европол.
- (25) С оглед да гарантира цялостното постигане на своите цели, Агенцията следва да си сътрудничи с правоприлагащи органи и органи за защита на неприкосновеността на личния живот, за да подчертае и управлява по подходящ начин аспектите на борбата с кибернетичните престъпления, свързани с мрежовата и информационна сигурност. Представителите на тези органи следва да станат пълноправни заинтересовани страни в Агенцията и следва да бъдат представени в Постоянната група на заинтересовани страни.
- (26) Проблемите на мрежовата и информационната сигурност са глобални. Съществува необходимост от по-тясно международно сътрудничество с цел подобряване на стандартите за сигурност, подобряване на информационния обмен и насърчаване на общ глобален подход към въпросите на мрежовата и информационна сигурност. За целта Агенцията следва да подкрепя

сътрудничеството с трети държави и международни организации в сътрудничество, където е уместно, с Европейската служба за външни действия.

- (27) Изпълнението на задачите на Агенцията следва да не нарушава компетенциите, нито да изземва, възпрепятства или припокрива съответните правомощия и задачи на: националните регулаторни органи, както е посочено в директивите, свързани с електронните съобщителни мрежи и услуги, както и Органа на европейските регулатори за електронни съобщения (ОЕРЕС), създадена с Регламент (ЕО) № 1211/2009²⁷ на Европейския парламент и Съвета, и Комитета по регулиране на съобщенията, посочен в Директива 2002/21/ЕО, европейските органи по стандартизация, националните органи по стандартизация и Постоянния комитет, както е посочено в Директива 98/34/ЕО на Европейския парламент и на Съвета от 22 юни 1998 г. за определяне на процедура за предоставяне на информация в областта на техническите стандарти и регламенти и правила относно услугите на информационното общество²⁸, както и на надзорните органи в държавите-членки, свързани със защитата на физическите лица по отношение на обработката на лични данни и на свободното движение на такива данни.
- (28) С цел да се гарантира ефективността на Агенцията държавите-членки и Комисията следва да бъдат представени в Управителен съвет, който следва да определи общата насока на дейността на Агенцията и да гарантира, че тя извършва своите задачи в съответствие с настоящия регламент. Управителният съвет следва да получи необходимите правомощия 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 работната програма на Агенцията, приемане на свои собствени процедурни правила и на вътрешен правилник за дейността на Агенцията, както и назначаване и вземане на решение за удължаването или прекратяването на мандата на изпълнителния директор. Управителният съвет следва да е в състояние да сформира работни органи, които да оказват съдействие при изпълнението на неговите задачи; подобни органи биха могли например да изготвят неговите решения или да осъществяват наблюдение върху тяхното изпълнение.
- (29) Гладкото функциониране на Агенцията налага нейният изпълнителен директор да се назначава въз основа на своите заслуги и документирани административни и управленски умения, както и на компетентност и опит, свързани с мрежовата и информационната сигурност, и да изпълнява своите задължения с пълна независимост от организацията на вътрешното функциониране на Агенцията. За целта изпълнителният директор следва да изготви предложение за работна програма на Агенцията след предварителни консултации със службите на Комисията и да предприеме всички необходими стъпки за гарантиране на правилното изпълнение на работната програма на Агенцията. Той следва да изготвя ежегодно общ проектодоклад, който да бъде представян на Управителния съвет, да съставя проект на разчета за предвидените приходи и разходи на Агенцията, както и да изпълнява бюджета.

²⁷ ОВ L 337, 18.12.2009 г., стр. 1.

²⁸ ОВ L 204, 21.7.1998 г., стр. 37.

- (30) Изпълнителният директор следва да разполага с възможността да сформира работни *ad hoc* групи за решаване на специфични въпроси, по-специално с научен или технически, правен или социално-икономически характер. При сформирването на работни *ad hoc* групи изпълнителният директор следва да събира и използва уместни външни експертни знания, необходими за обезпечаването на Агенцията с най-актуалната налична информация за предизвикателствата пред сигурността, произтичащи от непрекъснато развиващото се информационно общество. Агенцията следва да гарантира, че членовете на работните *ad hoc* групи се избират въз основа на най-високите стандарти за експертни знания, като надлежно се отчита балансът при представянето на всички страни, в зависимост от конкретния случай, между държавните администрации на държавите-членки, частния сектор, включително индустрията, потребителите и академични експерти в областта на мрежовата и информационна сигурност. В зависимост от конкретния случай, Агенцията може при необходимост да покани отделни експерти, признати като компетентни в съответната област, да участват в заседанията на работните групи. Техните разходи следва да се покриват от Агенцията в съответствие с нейния процедурен правилник и при спазване на съществуващите финансови регламенти.
- (31) Агенцията следва да разполага с Постоянна група на заинтересовани страни в ролята на консултативен орган, за да се гарантира редовен диалог с частния сектор, потребителските организации и други уместни заинтересовани страни. Постоянната група на заинтересовани страни, сформирана от Управителния съвет по предложение на изпълнителния директор, следва да се съсредоточи върху въпроси, засягащи всички заинтересовани страни, и да насочи вниманието на Агенцията към тях. Когато е уместно и в съответствие с дневния ред на заседанията, изпълнителният директор може да кани за участие в заседанията на групата представители на Европейския парламент и на други уместни органи.
- (32) Агенцията следва да развива дейността си, като следва съответно i) принципа на субсидиарност, чрез който се гарантира подходяща степен на координация между държавите-членки по свързани с МИС въпроси и се подобрява ефективността на националните политики, осигурявайки по този начин добавена стойност, и ii) принципа на пропорционалност, като не излиза извън границите на необходимото за постигане на целите, определени в настоящия регламент.
- (33) Агенцията следва да прилага законодателството на Съюза относно публичния достъп до документи, както е посочено в Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета²⁹, и относно защитата на физическите лица по отношение на обработката на лични данни, както е посочено в 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 данни³⁰.

²⁹ 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).

³⁰ 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).

- (34) В рамките на своя обхват, цели и изпълнението на задачите си Агенцията следва да спазва по-специално разпоредбите, приложими по отношение на европейските институции, както и националното законодателство относно третирането на чувствителни документи. Управителният съвет следва да разполага с правомощия да взема решение, позволяващо на Агенцията да обработва класифицирана информация.
- (35) С оглед гарантирането на пълната автономност и независимост на Агенцията се счита за необходимо да ѝ бъде предоставен автономен бюджет, чийто приходи произтичат най-вече от вноса на Съюза и вноски на трети държави, вземащи участие в работата на Агенцията. Приемашата държава-членка или всяка друга държава-членка следва да могат да правят доброволни вноски към приходите на Агенцията. Бюджетната процедура на Съюза остава приложима по отношение на всякакви субсидии, платими от общия бюджет на Европейския съюз. Освен това ревизиите на финансовите отчети следва да се поемат от Сметната палата.
- (36) Агенцията следва да бъде правоприменик на ENISA, съгласно определението в Регламент № 460/2004. В контекста на решението на представителите на държавите-членки на срещата на 13 декември 2003 г., държавата-домакин следва да запази и доразвие съществуващите понастоящем структури, за да осигури гладко и ефикасно функциониране на Агенцията, особено с оглед на сътрудничеството между Агенцията и Комисията и подкрепата от страна на Агенцията за Комисията, държавите-членки и техните компетентни органи, други институции и органи на Съюза, както и публични и частни заинтересовани страни от цяла Европа.
- (37) Агенцията следва да бъде създадена за ограничен период. Нейните дейности следва да бъдат оценявани с оглед на ефективността на постигане на целите и нейните работни практики, за да се установи дали целите на Агенцията продължават да са валидни или са отпаднали и на тази основа да се определи дали срокът ѝ на функциониране следва да бъде удължен,

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

РАЗДЕЛ 1 ОБХВАТ, ЦЕЛИ И ЗАДАЧИ

Член 1

Предмет и обхват

1. С настоящия регламент се учредява Европейска агенция за мрежова и информационна сигурност (наричана по-долу „Агенцията“) с цел допринасяне за високо ниво на мрежова и информационна сигурност в рамките на Съюза и с оглед повишаване на осведомеността и създаване на култура на мрежова и информационна сигурност сред обществото в полза на гражданите, потребителите, предприятията и организациите от държавния сектор в Съюза, като по този начин се подпомогне гладкото функциониране на вътрешния пазар.

2. Целите и задачите на Агенцията не накърняват компетенциите на държавите-членки относно мрежовата и информационна сигурност и във всеки случай дейностите, свързани с обществената сигурност, отбраната, държавната сигурност (включително

икономическото благосъстояние на държавата, когато въпросите касаят аспекти на държавната сигурност) и дейностите на държавата в областта на наказателното право.

3. За целите на настоящия регламент под „*мрежова и информационна сигурност*“ се разбира способността на дадена мрежа или информационна система да проявява устойчивост, при определено равнище на доверие, спрямо случайни събития или незаконни или злонамерени действия, които излагат на риск наличността, автентичността, целостта и поверителността на съхранявани или пренасяни данни и на свързаните с тях услуги, предлагани от или достъпни посредством тези мрежи и системи.

Член 2

Цели

1. Агенцията подпомага Комисията и държавите-членки в спазването на правните и регулаторни изисквания на мрежовата и информационна сигурност, заложи в настоящото и бъдещо законодателство на Съюза, като по този начин допринася за гладкото функциониране на вътрешния пазар.

2. Агенцията укрепва способността и подготвеността на Съюза и на държавите-членки за предотвратяване, установяване и реагиране на проблеми и инциденти, свързани с мрежовата и информационна сигурност.

3. Агенцията разработва и поддържа високо ниво на експертни знания и използва тези знания, за да стимулира широкото сътрудничество между представителите на публичния и частния сектор.

Член 3

Задачи

1. В рамките на целта, посочена в член 1, Агенцията извършва следните задачи:

а) подпомага Комисията, по нейна молба или по собствена инициатива, при разработването на политика за мрежова и информационна сигурност, като ѝ предоставя консултации и мнения и технически и социално-икономически анализи, както и при подготвителната работа за разработването и актуализирането на законодателството на Съюза в областта на мрежовата и информационна сигурност;

б) улеснява сътрудничеството между държавите-членки и между държавите-членки и Комисията в трансграничните им усилия за предотвратяване, установяване и реагиране на инциденти, свързани с мрежовата и информационна сигурност;

в) подпомага държавите-членки и европейските институции и органи в усилията им за събиране, анализиране и разпространяване на данни, свързани с мрежовата и информационна сигурност;

г) редовно оценява, в сътрудничество с държавите-членки и европейските институции, състоянието на мрежовата и информационна сигурност в Европа;

- д) подкрепя сътрудничеството между компетентните държавни органи в Европа, по-специално техните усилия за разработване и обмен на добри практики и стандарти;
- е) подпомага Съюза и държавите-членки да насърчават използването на управление на риска и на добри практики и стандарти относно сигурността в сферата на електронните продукти, системи и услуги;
- ж) подкрепя сътрудничеството между заинтересовани страни от публичния и частния сектор на нивото на Европейския съюз *inter alia* чрез насърчаване на споделянето на информация и повишаването на осведомеността и чрез подпомагане на техните усилия за разработване и използване на стандарти за управление на риска и за сигурността на електронните продукти, мрежи и услуги;
- з) улеснява диалога и обмена на добри практики между представители на публичния и частния сектор относно мрежовата и информационна сигурност, включително аспекти на борбата срещу кибернетичните престъпления; подпомага Комисията в разработването на политики, в които се отчитат аспектите на мрежовата и информационна сигурност в борбата срещу кибернетичните престъпления;
- и) подпомага държавите-членки и европейските институции и органи, по тяхна молба, в усилията им за развиване на способност за установяване, анализиране и реагиране на проблеми в сферата на мрежовата и информационна сигурност;
- й) подпомага диалога и сътрудничеството между Съюза и трети държави и международни организации, по целесъобразност в сътрудничество с Европейската служба за външни действия, с оглед насърчаване на международното сътрудничество и на общ глобален подход към въпросите на мрежовата и информационна сигурност;
- к) изпълнява задачи, възложени на Агенцията по силата на законодателни актове на Съюза.

РАЗДЕЛ 2 ОРГАНИЗАЦИЯ

Член 4

Органи на Агенцията

Агенцията се състои от:

- а) Управителен съвет;
- б) Изпълнителен директор и персонал; както и
- в) Постоянна група на заинтересовани страни.

Член 5

Управителен съвет

1. Управителният съвет определя общата насока на дейността на Агенцията и гарантира, че тя реализира своите задачи в съответствие с правилата и принципите, заложиени 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.

2. Управителният съвет приема своите процедурни правила в споразумение със съответните служби на Комисията.

3. Управителният съвет също така приема вътрешния правилник на Агенцията в споразумение със съответните служби на Комисията. Правилата са обществено достъпни.

4. Управителният съвет назначава изпълнителния директор в съответствие с член 10, параграф 2 и може да отстранява изпълнителния директор. Управителният съвет упражнява дисциплинарна власт над изпълнителния директор.

5. Управителният съвет приема работната програма на Агенцията в съответствие с член 13, параграф 3 и общия доклад за дейностите на Агенцията през предходната година в съответствие с член 14, параграф 2.

6. Управителният съвет приема финансовите правила, приложими за Агенцията. Те не могат да се отклоняват от Регламент (ЕО, Евратом) № 2343/2002 на Комисията от 19 ноември 2002 г. относно рамковия Финансов регламент за органите, посочени в член 185 от Регламент (ЕО, Евратом) № 1605/2002 на Съвета относно Финансовия регламент, приложим за общия бюджет на Европейските общности³¹, освен ако такова отклонение се налага специално за дейността на Агенцията и Комисията е дала предварителното си съгласие.

7. Управителният съвет, по споразумение с Комисията, приема подходящи правила за прилагане в съответствие с предвиденото в член 110 от Правилника за длъжностните лица.

8. Управителният съвет може да създаде работни органи, съставени от негови членове, с цел да му съдействат при изпълнението на неговите задачи, включително при изготвянето на решения и наблюдаване на тяхното прилагане.

9. Управителният съвет може да приема многогодишния план за политика по отношение на персонала след консултация със службите на Комисията и след като надлежно е информирал бюджетния орган.

Член 6

Състав на управителния съвет

1. Съставът на Управителния съвет включва по един представител на всяка държава-членка, трима представители, назначени от Комисията, както и трима представители без право на глас, назначени от Комисията, всеки от които представлява една от следните групи:

а) отрасъла на информационните и комуникационните технологии;

б) групи на потребителите;

³¹ ОВ L 357, 31.12.2002 г., стр. 72.

в) академични експерти по мрежова и информационна сигурност.

2. Членовете на съвета и техните заместници се назначават въз основа на степента на съответния им опит и на експертните им знания в областта на мрежовата и информационната сигурност.

3. Мандатът на представителите на групите, посочени в параграф 1, букви а), б) и в) е четири години. Той може да бъде подновяван само еднократно. В случай че даден представител прекрати своето участие в съответната група, Комисията назначава негов заместник.

Член 7

Председател на Управителния съвет

Управителният съвет избира свой председател и заместник-председател измежду членовете си за срок от три години, като този срок може да бъде подновяван. Заместник-председателят замества служебно председателя, ако последният не е в състояние да изпълнява своите задължения.

Член 8

Съвещания

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

2. Управителният съвет провежда редовно заседание два пъти годишно. Той провежда и извънредни заседания по искане на председателя или по искане на най-малко една трета от членовете си с право на глас.

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

Член 9

Гласуване

1. Управителният съвет взема решенията си с мнозинство на членовете си с право на глас.

2. За приемането на процедурния правилник, вътрешния правилник за дейността на Агенцията, бюджета, годишната работна програма, както и за назначаването, удължаването на мандата и освобождаването на изпълнителния директор е необходимо мнозинство от две трети от всички членове на Управителния съвет с право на глас.

Член 10

Изпълнителен директор

1. Агенцията се ръководи от изпълнителен директор, който е независим при изпълнението на своите задължения.

2. Изпълнителният директор се назначава и освобождава от Управителния съвет. Назначаването се извършва въз основа на списък от кандидати, предложени от Комисията, за срок от пет години, въз основа на заслуги и документираны административни и управленски умения, както и на специфични компетенции и опит. Преди назначаването избраният от Управителния съвет кандидат може да бъде поканен да направи изявление пред компетентния комитет на Европейския парламент и да отговори на въпроси, поставени от неговите членове.

3. Комисията прави оценка през деветте месеца, предшестващи изтичането на този период. При извършването на оценката Комисията се спира по-специално на:

- резултатите от работата на изпълнителния директор;
- задълженията на Агенцията и изискванията през следващите години.

4. По предложение на Комисията и като се взема предвид доклада за оценка и само в случаите, когато това може да се обоснове със задълженията и изискванията на Агенцията, Управителният съвет може да удължава мандата на изпълнителния директор за не повече от три години.

5. Управителният съвет уведомява Европейския парламент за намерението си да удължи мандата на изпълнителния директор. В рамките на един месец преди удължаването на неговия мандат изпълнителният директор може да бъде поканен да направи изявление пред компетентния комитет на Европейския парламент и да отговори на въпроси, поставени от неговите членове.

6. Ако мандатът не бъде удължен, изпълнителният директор остава на поста си до назначаването на негов правопреемник.

7. Изпълнителният директор отговаря за:

- а) ежедневното управление на Агенцията;
- б) изпълнението на работната програма и решенията, приети от Управителния съвет;
- в) гарантирането, че Агенцията осъществява своите дейности в съответствие с изискванията на ползвателите на нейните услуги, по-специално що се отнася до адекватността на предоставяните услуги;
- г) всички специфични въпроси по отношение на персонала, като гарантира спазване на общите насоки на Управителния съвет и на решенията на Управителния съвет с общ характер;
- д) установяването и поддържането на контакт с европейските институции и органи;
- е) установяването и поддържането на контакт с бизнес общността и потребителските организации с цел осигуряване на редовен диалог с уместните заинтересовани страни;
- ж) други задачи, възложени му по силата на настоящия регламент.

8. При необходимост и в рамките на целите и задачите на Агенцията, изпълнителният директор може да сформира работни *ad hoc* групи, съставени от експерти. Управителният съвет се информира предварително за това. Процедурите, по-специално относно състава, назначаването на експертите от изпълнителния директор и дейността на работните *ad hoc* групи, се определят във вътрешния правилник за дейността на Агенцията.

9. Изпълнителният директор осигурява на Управителния съвет административен помощен персонал и други налични ресурси, когато е необходимо.

Член 11

Постоянна група на заинтересовани лица

1. Управителният съвет учредява Постоянна група на заинтересовани страни по предложение на изпълнителния директор, съставена от експерти, представляващи уместни заинтересовани страни, например отрасли на информационни и комуникационни технологии, потребителски групи, академични експерти в областта на мрежовата и информационна сигурност и органи за правоприлагане и защита на неприкосновеността на личния живот.

2. Процедурите, по-специално процедурите относно броя, състава и 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. Групата се председателства от изпълнителния директор.

4. Мандатът на членовете на групата е с продължителност две години и половина. Членовете на Управителния съвет не могат да бъдат членове на групата. Служителите на Комисията имат право да присъстват на срещите и да участват в работата на групата.

5. Групата консултира Агенцията при изпълнението на нейните дейности. По-специално групата консултира изпълнителния директор относно изготвянето на предложение за работна програма на Агенцията и гарантирането на диалог с уместните заинтересовани страни относно всички въпроси, свързани с работната програма.

РАЗДЕЛ 3 ДЕЙНОСТ

Член 12

Работна програма

1. Агенцията извършва дейността си в съответствие със своята работна програма, която съдържа всички планирани дейности. Работната програма не възпрепятства Агенцията да осъществява непредвидени дейности, попадащи в обхвата на нейните цели и задачи, както и в границите на нейния бюджет. Изпълнителният директор уведомява Управителния съвет за дейностите на Агенцията, които не са предвидени в работната програма.

2. Изпълнителният директор отговаря за изготвянето на проект на работна програма на Агенцията след предварителни консултации със службите на Комисията. В срок до 15 март всяка година изпълнителният директор представя на Управителния съвет проекта на работна програма за следващата година.

3. В срок до 30 ноември всяка година Управителният съвет приема работната програма на Агенцията за следващата година, консултирайки се със службите на Комисията. Работната програма съдържа многогодишна визия. Управителният съвет гарантира съвместимостта на работната програма с целите на Агенцията, както и със законодателните и политическите приоритети на Съюза в областта на мрежовата и информационната сигурност.

4. Работната програма се организира в съответствие с принципа на управление по дейности (ABM). Тя съответства на прогнозните отчети за приходите и разходите на Агенцията и на бюджета на Агенцията за същата финансова година.

5. След приемането ѝ от Управителния съвет, изпълнителният директор изпраща работната програма на Европейския парламент, на Съвета, на Комисията и на държавите-членки и я публикува.

Член 13 **Общ доклад**

1. Изпълнителният директор ежегодно представя на Управителния съвет общ проектодоклад, обхващащ всички дейности на Агенцията през предходната година.

2. В срок до 31 март всяка година Управителният съвет приема общия доклад за дейностите на Агенцията през предходната година.

3. След приемането му от Управителния съвет изпълнителният директор предава общия доклад на Агенцията на Европейския парламент, на Съвета, на Комисията, на Сметната палата, на Европейския икономически и социален комитет и на Комитета на регионите и го публикува.

Член 14 **Искания към Агенцията**

1. Искания за консултации и помощ, попадащи в обхвата на целите и задачите на Агенцията, се отправят към изпълнителния директор и се придружават с обща информация, разясняваща въпроса, който трябва да бъде разгледан. Изпълнителният директор уведомява Управителния съвет за получените искания и за последващите действия спрямо тях в разумни срокове. Ако Агенцията откаже искане, отказът трябва да бъде придружен с мотивация.

2. Исканията, посочени в параграф 1, могат да се отправят от:

а) Европейския парламент;

б) Съвета;

в) Комисията;

г) всеки компетентен орган, назначен от държава-членка, като например национален регулаторен орган, както е определено в член 2 от Директива 2002/21/ЕО.

3. Практическите договорености за прилагането на параграфи 1 и 2, по-специално относно представянето, подреждането в приоритетен ред, последващите действия и информирането на Управителния съвет относно исканията до Агенцията, се регламентират от Управителния съвет във вътрешния правилник за дейността на Агенцията.

Член 15

Деклариране на интерес

1. Изпълнителният директор и длъжностните лица, временно командировани от държавите-членки, представят писмена декларация за ангажименти и писмена декларация за липса на каквито и да било преки или косвени интереси, които биха могли да се считат за накърняващи тяхната независимост.

2. Външните експерти, участващи в работни *ad hoc* групи, декларират на всяко заседание наличието на интереси, които биха могли да се считат за накърняващи тяхната независимост по отношение на точките от дневния ред, и се въздържат от участие в обсъждането на тези точки.

Член 16

Прозрачност

1. Агенцията гарантира, че тя осъществява дейността си при високо ниво на прозрачност и в съответствие с членове 13 и 14.

2. Агенцията гарантира, че на обществеността и на заинтересованите страни се предоставя обективна, достоверна и леснодостъпна информация, по-специално по отношение на резултатите от нейната дейност, ако това е целесъобразно. Тя е длъжна също така да оповестява публично декларациите за интереси, подадени от изпълнителния директор и от длъжностните лица, временно командировани от държави-членки, заедно с декларациите за интереси, подадени от експертите относно точките от дневния ред на заседанията на работни *ad hoc* групи.

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 договорености за прилагане на правилата на прозрачност, посочени в параграфи 1 и 2.

Член 17
Поверителност

1. Без да се засяга член 14, Агенцията няма право да разкрива на трети страни информация, която обработва или получава, за която е поискано поверително обработване.
2. Членове на Управителния съвет, изпълнителният директор, членовете на Постоянната група на заинтересовани страни, участващите в работните *ad hoc* групи външни експерти и членове на персонала на Агенцията, включително временно командированите от държавите-членки длъжностни лица, са задължени да спазват изискванията за поверителност съгласно член 339 от Договора, дори и след приключване на служебните им задължения.
3. Агенцията установява във вътрешния правилник за дейността си практическите договорености за прилагане на правилата на поверителност, посочени в параграфи 1 и 2.
4. Управителният съвет може да вземе решение да позволи на Агенцията да работи с класифицирана информация. В такъв случай Управителният съвет, в споразумение със съответните служби на Комисията, приема вътрешен правилник за дейността, като прилага принципите относно сигурността, заложи в Решение 2001/844/ЕО на Комисията, ЕОВС, Евратом, от 29 ноември 2001 г. за изменение на нейния процедурен правилник³². Това обхваща *inter alia* разпоредби за обмена, обработката и съхранението на класифицирана информация.

Член 18
Достъп до документи

1. Регламент (ЕО) № 1049/2001 се прилага за документи, притежавани от Агенцията.
2. Управителния съвет приема реда за прилагането на Регламент (ЕО) № 1049/2001 в срок до шест месеца от създаването на Агенцията.
3. Решенията, взети от Агенцията съгласно член 8 от Регламент (ЕО) № 1049/2001, могат да се обжалват пред омбудсмана или пред Съда на Европейския съюз съгласно съответно членове 228 и 263 от Договора.

РАЗДЕЛ 4 ФИНАНСОВИ РАЗПОРЕДБИ

Член 19
Приемане на бюджета

1. Приходите на Агенцията се състоят от вноски от бюджета на Европейския съюз, вноски от трети държави, вземащи участие в работата на Агенцията, както е предвидено в член 29, и вноски от държави-членки.

³² ОВ L 317, 03.12.2001 г., стр. 1.

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.
3. В срок до 1 март 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.
4. Приходите и разходите са балансирани.
5. Ежегодно, на основата на проект на разчета за предвидените приходи и разходи, изготвен от изпълнителния директор, Управителният съвет изготвя разчет за предвидените приходи и разходи на Агенцията за следващата финансова година.
6. Този разчет за предвидените средства, който включва проект на щатно разписание, заедно с проект на работна програма, се предава в срок не по-късно от 31 март от Управителния съвет на Комисията и на държавите, с които Европейският съюз е сключил споразумения в съответствие с член 24.
7. Комисията предава разчета на Европейския парламент и на Съвета (наричани по-долу „бюджетният орган“), заедно с общия проектобюджет на Европейския съюз.
8. Въз основа на този разчет Комисията включва в общия проектобюджет на Европейския съюз средствата, които прецени за необходими за щатното разписание и размера на субсидията, която трябва да бъде начислена от общия бюджет, и ги представя на бюджетния орган в съответствие с член 314 от Договора.
9. Бюджетният орган разрешава отпускането на бюджетни кредити за субсидията, предназначена за Агенцията.
10. Бюджетният орган приема щатното разписание за Агенцията.
11. Заедно с работната програма, Управителният съвет приема бюджета на Агенцията. Той става окончателен след окончателното приемане на общия бюджет на Европейския съюз. Когато е уместно, Управителният съвет адаптира бюджета и работната програма на Агенцията в съответствие с общия бюджет на Европейския съюз. Управителният съвет незабавно го изпраща на Комисията и на бюджетния орган.

Член 20

Борба с измамите

1. За борба с измамите, корупцията и други неправомерни дейности се прилагат без ограничения разпоредбите на Регламент (ЕО) № 1073/1999 на Европейския парламент и на Съвета от 25 май 1999 г. относно разследванията, провеждани от Европейската служба за борба с измамите (OLAF)³³.
2. Агенцията се присъединява към Междуинституционалното споразумение от 25 май 1999 г. между Европейския парламент и Съвета на Европейския съюз и Комисията на Европейските общности относно вътрешните разследвания от Европейската служба за

³³ ОВ L 136, 31.5.1999 г., стр. 1.

борба с измамите (OLAF)³⁴ и незабавно издава съответните разпоредби, приложими по отношение на всички служители на Агенцията.

Член 21

Изпълнение на бюджета

1. Изпълнителният директор прилага бюджета на Агенцията.
2. Вътрешният одитен орган на Комисията се ползва със същите правомощия спрямо Агенцията, като тези спрямо отделите на Комисията.
3. В срок до 1 март след края на всяка финансова година счетоводителят на Агенцията запознава счетоводителя на Комисията с предварителните счетоводни отчети, заедно с доклад за бюджетното и финансово управление за изминалата финансова година. Счетоводителят на Комисията консолидира предварителните отчети на институциите и децентрализираните органи в съответствие с член 128 от Регламент (ЕО, Евратом) № 1605/2002 на Съвета от 25 юни 2002 г. относно Финансовия регламент, приложим за общия бюджет на Европейските общности³⁵ (наричан по-долу „общ Финансов регламент“).
4. В срок до 31 март след приключване на всяка финансова година счетоводителят на Комисията предава на Сметната палата предварителните отчети на Агенцията заедно с доклада за бюджетното и финансовото управление за изминалата година. Докладът за бюджетното и финансовото управление за финансовата година се изпраща и на бюджетния орган.
5. След получаване на наблюденията на Сметната палата относно предварителните отчети на Агенцията, съгласно член 129 от общия Финансов регламент, изпълнителният директор изготвя окончателните отчети на Агенцията на своя собствена отговорност и ги предава на Управителния съвет за становище.
6. Управителният съвет дава становище относно окончателните отчети на Агенцията.
7. В срок до 1 юли след приключване на всяка финансовата година изпълнителният директор изпраща на Европейския парламент, на Съвета, на Комисията и на Сметната палата окончателните отчети заедно със становището на Управителния съвет.
8. Изпълнителният директор публикува окончателните отчети.
9. Изпълнителният директор изпраща на Сметната палата отговор на нейните констатации най-късно до 30 септември. Той изпраща отговора и на Управителния съвет.
10. 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 146, параграф 3 от общия Финансов регламент.

³⁴ ОВ L 136, 31.5.1999 г., стр. 15.

³⁵ ОВ L 248, 16.9.2002 г., стр. 1.

11. В срок до 30 април на година N + 2, по препоръка на Съвета, Европейският парламент освобождава изпълнителния директор от отговорност по отношение на изпълнението на бюджета за година N.

РАЗДЕЛ 5 ОБЩИ РАЗПОРЕДБИ

Член 22

Правен статус

1. Агенцията е орган на Съюза. Тя притежава юридическа правосубектност.
2. Във всяка от държавите-членки Агенцията има най-широките законови правомощия, давани на юридическите лица съгласно законодателството на съответната държава-членка. Тя може по-специално да придобива и да се разпорежда с движимо и недвижимо имущество и да бъде страна по юридически производства.
3. Агенцията се представлява от нейния изпълнителен директор.

Член 23

Служители

1. Правилата и разпоредбите, приложими по отношение на длъжностните лица и други служители на Европейския съюз, се прилагат по отношение на персонала на Агенцията, включително нейния изпълнителния директор.
2. По отношение на изпълнителния директор Управителният съвет упражнява правомощията, предоставени на назначаващия орган съгласно Правилника за длъжностните лица и на органа, упълномощен да сключва договори съгласно Условието за работа.
3. По отношение на персонала на Агенцията изпълнителният директор упражнява правомощията, предоставени на назначаващия орган съгласно Правилника за длъжностните лица и на органа, упълномощен да сключва договори съгласно Условието за работа.
4. Агенцията може да командирова на работа национални експерти от държави-членки. Тя регламентира практическите договорености в тази насока във вътрешния правилник за своята дейност.

Член 24

Привилегии и имунитети

Протоколът за привилегиите и имунитетите на Европейските общности се прилага по отношение на Агенцията и нейния персонал.

Член 25
Отговорност

1. Договорната отговорност на Агенцията се регламентира от приложимото по отношение на съответния договор законодателство.

Съдът на Европейския съюз е компетентен да се произнася по силата на всяка арбитражна клауза, съдържаща се в сключен от Агенцията договор.

2. 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.

Съдът на Европейските общности е компетентен по отношение на всякакви спорове, отнасящи се до поправянето на такива вреди.

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

Член 26
Езици

1. По отношение на Агенцията се прилагат разпоредбите на Регламент № 1 от 15 април 1958 г. за определяне на езиковия режим на Европейската икономическа общност³⁶. Държавите-членки и другите органи, назначени от тях, могат да се обръщат към Агенцията и да получават отговор на избран от тях език на Европейския съюз.

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

Член 27
Защита на личните данни

При обработка на данни, отнасящи се до физически лица, Агенцията е обект на разпоредбите на Регламент (ЕО) № 45/2001.

Член 28
Участие на трети държави

1. Агенцията е отворена за участие на трети държави, които са сключили споразумения с Европейския съюз, по силата на които те са приели и прилагат законодателството на Съюза в областта, обхваната от настоящия регламент.

2. Съгласно съответните клаузи на тези споразумения се изготвят разпоредби, уточняващи по-специално естеството, степента и начина, по който тези държави ще участват в работата на Агенцията, включително разпоредби, свързани с участието в инициативите, предприемани от Агенцията, финансовите вноски и персонала.

³⁶ ОВ 17, 6.10.1958 г., стр. 385/58. Последно изменен с Акта за присъединяване от 1994 г.

РАЗДЕЛ 6 ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 29

Клауза за преразглеждане

1. В рамките на три години от датата на учредяване, посочена в член 34, Комисията извършва оценка въз основа на условията, договорени с Управителния съвет, като взема под внимание гледните точки на всички съответни заинтересовани страни. Оценката анализира влиянието и ефективността на Агенцията при постигането на целите, посочени в член 2, както и ефективността на работните практики на Агенцията. Комисията извършва оценката най-вече за да установи дали една Агенция все още представлява ефективен инструмент и дали срокът на съществуването на Агенцията следва да се удължи допълнително извън определения в член 34 срок.
2. Констатациите от оценката се изпращат от Комисията на Европейския парламент и на Съвета и се публикуват.
3. Управителният съвет получава оценката и издава препоръки на Комисията за промени в настоящия регламент, в Агенцията и в нейните работни практики. Управителният съвет и изпълнителният директор вземат под внимание резултатите от оценката в многогодишните планове на Агенцията.

Член 30

Сътрудничество на приемащите държави-членки

Държавата-членка, която е приемаща за Агенцията, осигурява възможно най-добрите условия за безпроблемното и ефективно функциониране на Агенцията.

Член 31

Административен контрол

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

Член 32

Отменяне и правопримство

1. Регламент (ЕО) № 460/2004 се отменя.

Позоваванията на Регламент (ЕО) № 460/2004 и на ENISA се считат за позовавания на настоящия регламент и на Агенцията.

2. Агенцията е правопримник на агенцията, учредена с Регламент (ЕО) № 460/2004, по отношение на цялата собственост, споразумения, правни задължения, трудови договори, финансови ангажименти и задължения.

Член 33
Срок на съществуване

Агенцията се учредява на [...] за срок от пет години.

Член 34
Влизане в сила

Настоящият регламент влиза в сила в деня след публикуването му в *Официален вестник на Европейския съюз* и се прилага от 14 март 2012 г. или от деня след неговото публикуване, в зависимост от това коя от двете дати е по-късна.

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

Съставено в [...] на [...] година.

За Европейския парламент
Председател

За Съвета
Председател

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА ЗА ПРЕДЛОЖЕНИЯ

1. I. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1.

Предложение за Регламент на Европейския парламент и на Съвета относно Европейската агенция за мрежова и информационна сигурност (ENISA)

1.2. Засегнатата(и) област(и) на политиката в рамката на УД/БД³⁷

Информационно общество и медии.

Регулаторна рамка за Програмата в областта на цифровите технологии за Европа.

1.3. Естество на предложението/инициативата

Предложението/инициативата е свързано(а) с **ново действие**

Предложението/инициативата е свързано с **ново действие след пилотен проект/подготвително действие**³⁸

Предложението/инициативата е свързано(а) с **удължаването на съществуващо действие**

Предложението/инициативата е свързано(а) с **действие, пренасочено към ново действие**

1.4. Цели

1.4.1. Многогодишна(и) стратегическа(и) цел(и) на Комисията, към която(ито) е насочено(а) предложението/инициативата

Съгласуваност на регулаторните подходи — предоставяне на насоки и съвети на Комисията и на държавите-членки относно актуализирането и разработването на цялостна нормативна рамка в сферата на МИС.

Предотвратяване, установяване и реагиране — подобряване на подготвеността чрез принос към европейската способност за ранно предупреждаване и реагиране на инциденти, както и към паневропейските планове за действие при непредвидени ситуации.

Повишаване на познанията на лицата, разработващи политики — оказване на помощ и предоставяне на съвети на Комисията и на държавите-членки с оглед 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 включва също така генериране, анализиране и предоставяне на данни, свързани с

³⁷

УД: Управление по дейности — БД: Бюджетиране по дейности.

³⁸

Както е посочено в член 49, параграф 6, буква а) или б) от Финансовия регламент.

икономическите аспекти и въздействието от пробивите в МИС, начини за стимулиране на заинтересованите страни да инвестират в мерки за МИС, установяване на рискове, показатели за състоянието на МИС в ЕС и т. н.

Упълномощаване на заинтересованите страни — създаване на култура на управление на сигурността и риска чрез насърчаване на споделянето на информация и широко сътрудничество между участниците в процеса от обществения и частния сектор, също и в пряка полза на гражданите, и чрез създаването на култура на съзнание за МИС.

Предпазване на Европа от международни заплахи — постигане на високо ниво на сътрудничество с трети държави и международни институции с цел насърчаване на един общ глобален подход към МИС и придаване на тежест на международни инициативи на високо ниво в Европа.

Стремеж към съвместно прилагане — улесняване на сътрудничеството при прилагането на политиките относно МИС.

Борба срещу кибернетичните престъпления — включване на свързаните с МИС аспекти на борбата срещу кибернетичните престъпления в дискусиите и обмена на добри практики между заинтересовани страни от обществения и частния сектор, по-специално чрез сътрудничество с органи от (бивш) втори и трети стълб, например с Европол.

1.4.2. Специфична(и) цел(и) и съответна(и) дейност(и) във връзка с УД/БД

Специфична цел №

Повишаване на мрежовата и информационна сигурност (МИС) за изграждане на култура на мрежова и информационна сигурност в полза на гражданите, потребителите, предприятията и организациите от обществения сектор и определяне на политическите предизвикателства в резултат на бъдещите мрежи и интернет.

Съответна(и) дейност(и) във връзка с УД/БД

Политика в областта на електронните съобщения и мрежовата сигурност

1.4.3. Очакван(и) резултат(и) и въздействие

Очаква се инициатива да има следните икономически въздействия:

- повишено наличие на информация за текущите и бъдещи предизвикателства и рисковете за сигурността и устойчивостта
- избягване на дублирането на усилията за събиране на съответната информация за рискове, заплахи и уязвимости от всяка отделна държава-членка
- повишено ниво на информираност на лицата, разработващи политики, при вземането на решения
- повишено качество на разпоредбите в областта на политиката за МИС в държавите-членки поради разпространението на най-добри практики
- икономия от мащаба при реагирането на инциденти на ниво ЕС
- по-голям обем инвестиции, обусловени от общите политически цели и стандарти по отношение на сигурността и устойчивостта на ниво ЕС
- по-ниски оперативни рискове за предприятията поради по-високата степен на сигурност и устойчивост
- повишена съгласуваност на мерките за борба срещу кибернетичните престъпления.

Очаква се инициатива да има следните социални въздействия:

- повишено доверие на потребителите в услугите и системите на информационното общество;
- повишено доверие във функционирането на вътрешния пазар на ЕС чрез постигане на по-високи нива на потребителска защита;
- увеличен обмен на информация и познания с държави извън ЕС;
- по-добра защита на основните човешки права в ЕС чрез гарантиране на равни нива на защита на личните данни и на неприкосновеността на личния живот на гражданите на ЕС.

Очакваните екологични въздействия са минимални:

- намалено въздействие на емисиите от CO₂ поради, например, намаления обем пътувания в резултат на повишеното разчитане на използването на ИКТ системи и услуги, както и по-ниско потребление на електроенергия вследствие на икономии от мащаба при изпълнението на задълженията относно сигурността.

1.4.4. Показатели за резултатите и въздействието

Показателите за мониторинг на всяка от целите са следните:

Съгласуваност на регулаторните подходи:

- Брой държави-членки, възползвали се от препоръките на Агенцията в процеса на разработване на политиките си
- Брой изследвания, насочени към установяване на пропуските и несъответствията в стандартизационния модел относно МИС
- Намаляване на различията между подходите на държавите-членки относно МИС.

Предотвратяване, установяване и реагиране:

- Брой организирани обучения по мрежова сигурност
- Наличие на функционираща система за ранно предупреждение за нововъзникващи рискове и атаки
- Брой учения за МИС на ниво ЕС, координирани от Агенцията.

Повишаване на познанията на лицата, разработващи политики:

- Брой изследвания за събиране на информация относно текущи и очаквани рискове по отношение на МИС и технологиите за предотвратяване на риска
- Брой консултации с държавни органи, работещи в областта на МИС
- Наличие на европейска мрежа за организиране на събиране на данни за МИС.

Упълномощаване на заинтересованите страни:

- Брой установени добри практики за отрасъла
- Ниво на инвестиции в мерки за сигурност от страна на заинтересовани страни.

Предпазване на Европа от международни заплахи:

- Брой конференции/среци между държави-членки на ЕС за определяне на взаимнодоговорени цели относно МИС
- Брой среци между европейски и международни експерти по МИС.

Стремеж към съвместно прилагане:

- Брой оценки на спазването на регулаторните изисквания
- Брой практики относно МИС, действащи в целия ЕС.

Борба срещу кибернетичните престъпления:

- Степен на регулярност на взаимодействието с агенции от бивш 2-и и 3-и стълб
- Брой случаи, в които е предоставена експертна помощ относно криминални разследвания.

1.5. Основания за предложението/инициативата**1.5.1. Изискване(ия), което(ито) ще бъде(ат) спазено(и) в краткосрочен или дългосрочен план**

Първоначално ENISA беше създадена през 2004 г. за справяне със заплахите и евентуално възникващите в резултат на това нарушения в сферата на МИС. Оттогава свързаните с мрежовата и информационна сигурност предизвикателства претърпяха промени с технологичното и пазарното развитие и бяха обект на допълнителен размисъл и дебат, което днес дава възможност за актуализиране и по-подробно описание на конкретните проблеми и на начина, по който им въздейства променящият се контекст на МИС.

1.5.2. *Добавена стойност на приноса от участието на ЕС*

Проблемите в сферата на МИС надхвърлят националните граници и поради това не могат да бъдат разрешавани по ефективен начин единствено на национално ниво. Същевременно държавните органи в отделните държави-членки се справят с проблема по доста различни начини. Тези различия могат да представляват сериозна пречка пред прилагането в целия Съюз на подходящи механизми за повишаване на МИС в Европа. Поради взаимозависимия характер на инфраструктурите на ИКТ ефективността на мерките, предприети на национално ниво в дадена държава-членка, все още търпи силно влияние от по-ниското ниво на мерките в други държави-членки и от липсата на системно трансгранично сътрудничество. Инцидент в дадена държава-членка, произтичащ от недостатъчното ниво на мерките в областта на МИС, може да доведе до смущения в услугите в друга държава-членка.

Освен това нарастването на изискванията по отношение на сигурността в отделните държави-членки налага разходна тежест за предприятията, осъществяващи дейност в рамките на ЕС, което води до фрагментация и липса на конкурентоспособност на европейския вътрешен пазар.

Въпреки че зависимостта от мрежовите и информационни системи се увеличава, подготвеността за справяне с инциденти изглежда недостатъчна..

Настоящите национални системи за ранно предупреждаване и действия при инциденти имат сериозни недостатъци. Между държавите-членки съществуват значителни различия по отношение на процесите и практиките за мониторинг и докладване на инциденти, свързани с мрежовата сигурност. В някои държави процесите не са достатъчно формализирани, докато в други липсва компетентен орган, който да получава и обработва доклади за инциденти. Европейски системи не съществуват. В резултат на това обезпечаването на основни нужди може да бъде силно нарушено от инциденти, свързани с МИС, и следва да бъдат изготвени подходящи схеми за реагиране. В Съобщението на Комисията относно СИР също се подчертава необходимостта от европейската способност за ранно предупреждаване и реагиране на инциденти, която евентуално да бъде подпомогната чрез учения от европейски мащаб.

Налице е ясно изразена необходимост от инструменти на политиката, насочени към установяване на рискове и уязвими аспекти на МИС, за създаване на подходящи механизми за реагиране (например чрез определяне и разпространяване на добри практики) и за гарантиране, че заинтересованите страни познават и прилагат тези механизми за реагиране.

1.5.3. *Поуки от подобен опит в миналото*

Вж. точки 1.5.1 и 1.5.2

1.5.4. *Съгласуваност и евентуално полезно взаимодействие с други съответни инструменти*

Тази инициатива е изцяло съгласувана с общия дебат относно МИС и други политически инициативи, фокусирани върху бъдещето на МИС. Тя е един от основните компоненти на Европейската програма за цифрови технологии, която е водеща инициатива в рамките на стратегията „Европа — 2020“.

1.6. Срок на действие и финансово отражение

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

– Началната дата на петгодишния удължен срок е 14.3.2012 г. или денят на влизане в сила на регламента, в зависимост от това коя от двете дати е по-късна.

– Финансово отражение за периода 2012—2017 г.

Предложението/инициативата е с **неограничен срок на действие**

– Осъществяване с период на започване на дейност от ГТТГ до ГТТГ,

– последван от функциониране с пълен капацитет.

1.7. Предвидени(и) начин(и) на управление³⁹

Пряко централизирано управление от Комисията

Непряко централизирано управление с делегиране на задачи по изпълнението на:

– изпълнителни агенции,

– органи, създадени от Общностите⁴⁰

– национални органи от публичния сектор/органи със задължение за предоставяне на обществена услуга

– лица, натоварени с изпълнението на специфични дейности по силата на дял V от Договора за Европейския съюз и посочени в съответния основен акт по смисъла на член 49 от Финансовия регламент

Поделено управление с държавите-членки

Децентрализирано управление с трети държави

Съвместно управление с международни организации *(да се посочи кои)*

³⁹ Подробности за начините на управление и позовавания на Финансовия регламент могат да бъдат намерени на уебсайта „Бюджет“: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

⁴⁰ Както се посочва в член 185 от Финансовия регламент.

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

Изпълнителният директор е отговорен за ефективния мониторинг и оценка на дейността на Агенцията в съответствие с нейните цели и представя годишен доклад пред управителния съвет.

Изпълнителният директор изготвя проект на общ доклад, който обхваща всички дейности на Агенцията за предишната година, като по-специално сравнява постигнатите резултати с целите от годишната работна програма. След одобрението му от управителния съвет докладът се изпраща на Европейския парламент, Съвета, Комисията, Сметната палата, Европейския икономически и социален комитет и Комитета на регионите и се публикува.

2.2. Система за управление и контрол

2.2.1. Установени(и) риск(ове)

След създаването ѝ през 2004 г. ENISA е предмет на външни и вътрешни оценки.

В съответствие с член 25 от регламента за ENISA първата стъпка от този процес беше независима оценка на ENISA от група външни експерти през 2006—2007 г. Докладът на външните експерти⁴¹ потвърди, че първоначалните политически причини за създаването на ENISA и нейните първоначални цели са все още в сила и допринесе за поставяне на някои от проблемите, които трябва да бъдат разрешени.

През март 2007 г. Комисията представи на управителния съвет доклад за оценката, а впоследствие последният направи своите препоръки за бъдещето на Агенцията и за промяна на регламента за ENISA⁴².

През юни 2007 г. Комисията представи становището си относно резултатите от външната оценка и препоръките на управителния съвет в съобщение до Европейския парламент и Съвета⁴³. В съобщението се посочва, че трябва да се направи избор дали да се разшири мандатът на Агенцията или тя да се замести от друг механизъм, като например постоянно действащ форум на заинтересовани страни или мрежа от организации за сигурност. Съобщението също така постави началото на обществено допитване по този въпрос, като призова европейските заинтересовани страни да споделят своето мнение по списък с въпроси за очертаване на насоки за бъдещи дискусии⁴⁴.

⁴¹ http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm.

⁴² Както е предвидено в член 25 от Регламента относно ENISA. Пълният текст на документа, приет от управителния съвет на ENISA, включващ и съображенията на управителния съвет, е публикуван на следния уебсайт: http://enisa.europa.eu/pages/03_02.htm.

⁴³ Съобщение от Комисията до Европейския парламент и Съвета относно оценката на Европейската агенция за мрежова и информационна сигурност (ENISA), COM(2007) 285 окончателен, от 1.6.2007 г.: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:EN:NOT>.

⁴⁴ <http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=EnisaFuture&lang=en>.

2.2.2. *Предвидени(и) метод(и) за контрол*

Вж. точка 2.1 и точка 2.2.1 по-горе.

2.3. Мерки за предотвратяване на измами и нередности

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 др.) ще бъдат включени във всички договори и споразумения, сключени между Агенцията и получателите на плащанията.

3. ПРОГНОЗИРАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА*

3.1. Засегната(и) функция(и) от многогодишната финансова рамка и бюджетен(ни) ред(ове) за разходите

- Съществуващи бюджетни редове за разходите

Функция от многогодишната финансова рамка	Бюджетен ред	Вид на разходите	Вноска			
	Номер / Описание	МБК/ЕБК ⁽⁴⁵⁾	от страни от ЕАСТ ⁴⁶	от страни кандидатки ⁴⁷	от трети държави	по смисъла на член 18, параграф 1, буква аа) от Финансовия регламент.
1.а Конкурентоспособност за растеж и заетост	09 02 03 01 Европейска агенция за мрежова и информационна сигурност – субсидия по дял 1 и 2	МБК	ИМА	НЯМА	НЯМА	НЯМА
	09 02 03 02 Европейска агенция за мрежова и информационна сигурност – субсидия по дял 3	МБК	ИМА	НЯМА	НЯМА	НЯМА
5 Административни и разходи	09 01 01 Разходи, свързани с активно зает персонал в областта на административната политика на Комисията	ЕБК	НЯМА	НЯМА	НЯМА	НЯМА
	09 01 02 11 Други разходи за управление	ЕБК	НЯМА	НЯМА	НЯМА	НЯМА

* Очакваното финансово отражение на предложението за периода след края на настоящия финансов план 2007—2013 г. не е предмет на настоящата законодателна финансова обосновка. Въз основа на предложението на Комисията за регламент за определяне на многогодишна финансова рамка след 2013 г. и предвид заключенията на оценката на въздействието Комисията ще представи изменена законодателна финансова обосновка.

⁴⁵ МБК = многогодишни бюджетни кредити/ЕБК = едногодишни бюджетни кредити

⁴⁶ ЕФТА: Европейска асоциация за свободна търговия.

⁴⁷ Страни кандидатки и, където е приложимо, потенциални страни кандидатки от Западните Балкани.

3.2. Прогнозирано отражение върху разходите

3.2.1. Обобщение на прогнозираното отражение върху разходите

млн. EUR (до третия знак след десетичната запетая)

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

ENISA			1 януари— 13 март 2012 г.	14 март— 31 декември 2012 г.	2013 г.	2014 г.	2015 г.	2016 г.	1 януари— 13 март 2017 г.	ОБЩО 14 март 2012 г. — 13 март 2017 г.
Бюджетни кредити за оперативни разходи										
09 02 03 02 Европейска агенция за мрежова и информационна сигурност – субсидия по дял 3	Поети задължения	(1)	0,454	1,976	2,470	--	--	--	--	--
	Плащания	(2)	0,454	1,976	2,470	--	--	--	--	--
Бюджетни кредити за административни разходи										
09 02 03 01 Европейска агенция за мрежова и информационна сигурност – субсидия по дялове 1 и 2		(3)	1,293	4,697	6,120	--	--	--	--	--
ОБЩО бюджетни кредити по ФУНКЦИЯ 1a	Поети задължения	=1+3	1,747	6,673	8,590	--	--	--	--	--
	Плащания	=2+3	1,747	6,673	8,590	--	--	--	--	--

ОБЩО бюджетни кредити за оперативни разходи	Поети задължения	(4)	0,454	1,976	2,470	--	--	--	--	--
	Плащания	(5)	0,454	1,976	2,470	--	--	--	--	--
ОБЩО бюджетни кредити с административен характер, финансирани от пакета от специфични програми		(6)	1,293	5,144	4,697	6,120	--	--	--	--
ОБЩО бюджетни кредити по ФУНКЦИЯ 1.a от многогодишната рамкова програма	Поети задължения	=4+ 6	1,747	6,673	8,590	--	--	--	--	--
	Плащания	=5+ 6	1,747	6,673	8,590	--	--	--	--	--

млн. EUR (до третия знак след десетичната запетая)

Функция от многогодишната финансова рамка	5	Административни разходи
--	---	-------------------------

	1 януари— 13 март 2012 г.	14 март— 31 декември 2012 г.	2013 г.	2014 г.	2015 г.	2016 г.	1 януари— 13 март 2017 г.	Общо
Човешки ресурси	0,085	0,342	0,427	--	--	--	--	--
Други административни разходи	0,002	0,013	0,015	--	--	--	--	--
ОБЩО ГД „Информационно общество и медии“	0,087	0,355	0,442	--	--	--	--	--
Бюджетни кредити								

ОБЩО бюджетни кредити по ФУНКЦИЯ 5 от многогодишната финансова рамка	(Общо поети задължения = общо плащания)	0,087	0,355	0,442	--	--	--	--	--
---	---	-------	-------	-------	----	----	----	----	----

	1 януари- 13 март 2012 г.	14 март- 31 декември 2012 г.	2013 г.	2014 г.	2015 г.	2016 г.	1 януари-13 март 2017 г.	Общо
ОБЩО бюджетни кредити по ФУНКЦИИ 1—5 от многогодишната финансова рамка								
Поети задължения	1,834	7,028	9,032	--	--	--	--	--
Плащания	1,834	7,028	9,032	--	--	--	--	--

3.2.2. *Прогнозирано отражение върху бюджетните кредити за оперативни разходи*

- Предложението/инициативата не води до използване на бюджетни кредити за оперативни разходи
- Предложението/инициативата налага използването на бюджетни кредити за оперативни разходи съгласно обяснението по-долу:

Бюджетни кредити за поети задължения в млн. EUR (до 3 знака след десетичната запетая)

Да се посочат целите и резултатите ↓	1 януари — 13 март 2012 г.	14 март — 31 декември 2012 г.	2013 г.	2014 г.	2015 г.	2016 г.	1 януари — 13 март 2017 г.	ОБЩО 14 март 2012 г. — 13 март 2017 г.
Съгласуваност на регулаторните подходи	0,114	0,494	0,620	--	--	--	--	--
Предотвратяване, установяване и реагиране	0,114	0,494	0,620	--	--	--	--	--
Повишаване на познанията на лицата, разработващи политики	0,068	0,297	0,370	--	--	--	--	--
Упълномощаване на заинтересованите страни	0,050	0,218	0,270	--	--	--	--	--
Предпазване на Европа от международни заплахи	0,023	0,099	0,120	--	--	--	--	--
Стремеж към съвместно прилагане	0,064	0,276	0,340	--	--	--	--	--
Борба срещу кибернетичните престъпления	0,023	0,098	0,120	--	--	--	--	--

ОБЩО РАЗХОДИ	0,454	1,976	2,460	--	--	--	--	--
---------------------	-------	-------	-------	----	----	----	----	----

3.2.3. Прогнозирано отражение върху бюджетните кредити с административен характер⁴⁸

3.2.3.1. Обобщение

- Предложението/инициативата не води до използване на бюджетни кредити за административни разходи
- Предложението/инициативата налага използването на бюджетни кредити за административни разходи съгласно обяснението по-долу:

а) административни разходи по функция 5 от многогодишната финансова рамка

в млн. EUR (до третия знак след десетичната запетая)

ФУНКЦИЯ 5 от многогодишната финансова рамка	1 януари — 13 март 2012 г.	14 март — 31 декември 2012 г.	2013 г.	2014 г.	2015 г.	2016 г.	1 януари — 13 март 2017 г.	Общо 14 март 2012 г. — 13 март 2017 г.
--	----------------------------	-------------------------------	---------	---------	---------	---------	----------------------------	---

Човешки ресурси	0,085	0,342	0,427	--	--	--	--	--
Други административни разходи	0,002	0,013	0,015	--	--	--	--	--

ОБЩО	0,087	0,355	0,442	--	--	--	--	--
-------------	-------	-------	-------	----	----	----	----	----

б) административни разходи, свързани с ENISA — обхванати от бюджетен ред „09.020301 Европейска мрежова и информационна сигурност: дял 1 – Персонал и дял 2 — Функциониране на Агенцията“.

в млн. EUR (до третия знак след десетичната запетая)

	1 януари — 13 март 2012 г.	14 март — 31 декември 2012 г.	2013 г.	2014 г.	2015 г.	2016 г.	1 януари — 13 март 2017 г.	Общо 14 март 2012 г. — 13 март 2017 г.
--	----------------------------	-------------------------------	---------	---------	---------	---------	----------------------------	---

Човешки ресурси - дял 1 — Персонал	1,153	4,329	5,607	--	--	--	--	--
Други разходи с административен характер – дял 2 – Функциониране на	0,140	0,368	0,513	--	--	--	--	--

⁴⁸ Приложението към законодателната финансова обосновка не е попълнено, тъй като не е приложимо за настоящото предложение.

Агенцията								
-----------	--	--	--	--	--	--	--	--

ОБЩО	1,293	4,697	6,120	--	--	--	--	--
-------------	--------------	--------------	--------------	----	----	----	----	----

3.2.3.2. Прогнозирани изисквания за човешки ресурси

Всяка година се изготвя документ, наречен План за политиката относно персонала, който се представя на бюджетния орган и съдържа обяснение и обосновка на щатното разписание на Агенцията.

- Предложението/инициативата не води до използване на човешки ресурси
- Предложението/инициативата налага използването на човешки ресурси съгласно обяснението по-долу:

а) човешки ресурси в рамките на Комисията

	1 януари— 13 март 2012 г.	14 март— 31 декември 2012 г.	2013 г.	2014 г.	2015 г.	2016 г.	1 януари— 13 март 2017 г.
Позиции в щатното разписание (длъжностни лица и временно наети лица)							
XX 01 01 01 (централа и представителства на Комисията)	3,5	3,5	3,5	--	--	--	--
ОБЩО	3,5	3,5	3,5	--	--	--	--

б) човешки ресурси на ENISA

	1 януари— 13 март 2012 г.	14 март— 31 декември 2012 г.	2013 г.	2014 г.	2015 г.	2016 г.	1 януари— 13 март 2017 г.
Щатно разписание на ENISA (позиции, приравнени към щатни длъжности на пълно работно време)							
Длъжностни лица или временно нает персонал	Степен AD	29	31	31	--	--	--
	Степен AST	15	16	16	--	--	--
ОБЩО длъжностни лица или временно нает персонал	44	47	47	--	--	--	--
Друг персонал (позиции, приравнени към щатни длъжности на пълно работно време)							

Договорно наети служители	13	14	14	--	--	--	--
Командировани национални експерти	5	5	5	--	--	--	--
Общо друг персонал	18	19	19	--	--	--	--
ОБЩО	62	66	66	--	--	--	--

Описание на задачите, които да бъдат извършвани от персонала на Агенцията:

Длъжностни лица и временно нает персонал	<p>Агенцията ще продължи да:</p> <ul style="list-style-type: none"> – изпълнява консултантски и координационни функции, като събира и анализира данни за информационната сигурност. Понастоящем както държавни, така и частни организации събират с различна цел информация за инциденти в областта на ИКТ и други данни, свързани с информационната сигурност. Не съществува обаче централизирана единица на европейско ниво, която подробно да може да събира и анализира данните и да предоставя мнения и съвети в подкрепа на работата на Съюза в областта на политиката за мрежова и информационна сигурност; – служи като център за експертно знание, към който държавите членки и Общността могат да се обръщат за мнение и съвет по техническите въпроси на сигурността; – допринася за разширено сътрудничество между различните действащи лица в областта на информационната сигурност, като например подпомага последващите дейности в подкрепа на сигурността на търговската дейност, осъществявана по електронен път. Подобно сътрудничество е жизнено важно условие за сигурността на функциониране на мрежовите и информационни системи в Европа. Необходимо е участието и включването на всички заинтересовани страни; – допринася за координиран подход към информационната сигурност, като осигурява подкрепа на държавите-членки, например чрез насърчаване на оценката на риска и дейности за повишаване на обществената осведоменост; – гарантира оперативната съвместимост на мрежовите и информационни системи, когато държавите-членки прилагат технически изисквания, които влияят на сигурността; – определя съответната нужда от стандартизация и оценява съществуващите стандарти за сигурност и схемите за сертифициране и насърчава тяхната възможно най-широка употреба в подкрепа на европейското законодателство; – подкрепя международното сътрудничество в тази област, което се оказва все по-необходимо, тъй като проблемите на мрежовата и информационна сигурност са глобални.
Външен персонал	Вж. по-горе.

3.2.4. Съвместимост с настоящата многогодишна финансова рамка

- Предложението/инициативата е съвместимо(а) с настоящата многогодишна финансова рамка.
- Предложението/инициативата изисква повторно планиране на съответната функция от многогодишната финансова рамка.
- Предложението/инициативата изисква прилагане на гъвкав инструмент или преразглеждане на многогодишната финансова рамка⁴⁹.

Финансирането от страна на ЕС след 2013 г. ще бъде проверено в рамките на дискусия на Комисията по всички предложения за периода след 2013 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.

3.2.5. Вноски на трети страни

- Предложението/инициативата не предвижда съфинансиране от трети страни
- Предложението/инициативата предвижда прогнозираното по-долу съфинансиране:

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

	1 януари— 13 март 2012 г.	14 март— 31 декември 2012 г.	2013 г.	2014 г.	2015 г.	2016 г.	1 януари— 13 март 2017 г.	Общо 14 март 2012 г.— 13 март 2017 г.
EFTA	0,042	0,160	0,206	--	--	--	--	--

3.3. Прогнозирано отражение върху приходите

- Предложението/инициативата няма финансово отражение върху приходите.
- Предложението/инициативата има следното финансово отражение:
 - върху собствените ресурси

⁴⁹ Вж. точки 19 и 24 от Междуйнституционалното споразумение.

– върху други приходи