СЪВЕТ НА ЕВРОПЕЙСКИЯ СЪЮЗ

Брюксел, 12 февруари 2013 г. (OR. en)

6342/13

Междуинституционално досие: 2013/0027 (COD)

TELECOM	**24**
DATAPROTECT	**14**
CYBER	**2**
MI	**104**
CODEC	**313**

ПРЕДЛОЖЕНИЕ

От:	Комисията
Дата:	7 февруари 2013 г.
№ док. Ком.:	COM(2013) 48 final
Относно:	Предложение за директива на Европейския парламент и на Съвета относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза

Приложено се изпраща на делегациите предложение на Комисията, предоставено с придружително писмо от г-н Jordi AYET PUIGARNAU до г-н Uwe CORSEPIUS, генерален секретар на Съвета на Европейския съюз.

Приложение: COM(2013) 48 final

ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

Предложение за

ДИРЕКТИВА НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза

{SWD(2013) 31 final}
{SWD(2013) 32 final}

ОБЯСНИТЕЛЕН МЕМОРАНДУМ

Целта на предлаганата директива е да гарантира високо общо ниво на мрежова и информационна сигурност (МИС). Това означава повишаване на сигурността на интернет и на частните мрежи и информационни системи, които са в основата на функционирането на нашите общества и икономики. За постигането на тази цел от държавите членки ще се изисква да повишат своята готовност и да подобрят сътрудничеството помежду си, а от операторите на критична инфраструктура, като енергетика и транспорт, от ключовите доставчици на услуги на информационното общество (платформи за електронна търговия, социални мрежи и др.), а също така от публичните администрации — да предприемат подходящи стъпки за управление на рисковете пред сигурността и да докладват на националните органи за сериозните инциденти.

Настоящото предложение се представя във връзка със съвместното съобщение на Комисията и на върховния представител на Съюза по въпросите на външните работи и политиката на сигурност относно европейската стратегия за киберсигурност. Целта на стратегията е да гарантира сигурна и надеждна цифрова среда и същевременно да утвърди и защити основните права на ЕС и другите му основни ценности. Настоящото предложение е основното действие по стратегията. Другите действия по стратегията в тази сфера са насочени към повишаване на осведомеността, развитие на вътрешен пазар за продукти и услуги на киберсигурността и насърчаване на инвестициите в НИРД. Тези действия ще бъдат допълнени от други, насочени към засилване на борбата с киберпрестъпността и изграждане на международна политика на ЕС за киберсигурност.

1.1. Мотиви и цели на предложението

МИС е от все по-голямо значение за нашата икономика и нашето общество. МИС е важна предпоставка и за създаването на надеждна среда за глобална търговия с услуги. Информационните системи обаче могат да бъдат засегнати от инциденти по отношение на сигурността, например човешки грешки, природни явления, технически повреди или злонамерени атаки. Тези инциденти стават все по-мащабни, по-чести и по-сложни. От проведената от Комисията обществена консултация онлайн „Подобряване на мрежовата и информационната сигурност в ЕС“[1] става ясно, че през изминалата година 57 % от респондентите са имали случаи на инциденти във връзка с МИС, които са се отразили сериозно на техните дейности. Липсата на МИС може да компрометира основни услуги, които зависят от целостта на мрежовите и информационните системи. Това може да стане причина за спиране на стопански дейности, да доведе до значителни финансови загуби за икономиката на ЕС и да се отрази отрицателно на благосъстоянието на обществото.

Освен това като комуникационен инструмент без граници цифровите информационни системи и най-вече интернет са взаимосвързани в различните държави членки и играят основна роля за улесняването на трансграничното движение на стоки, услуги и хора. Значителните нарушения в дейността на тези системи в една държава членка могат да засегнат и други държави членки, както и Съюза като цяло. Устойчивостта и стабилността на мрежите и информационните системи е поради това от основно

[1] Обществената консултация онлайн на тема „Подобряване на МИС в ЕС“ беше проведена от 23 юли до 15 октомври 2012 г.

значение за завършването на цифровия единен пазар и за безпроблемното функциониране на вътрешния пазар. Вероятността и честотата на инцидентите и неспособността да се гарантира ефикасна защита вредят и на обществено доверие в мрежовите и информационните услуги: например проведеното през 2012 г. изследване на Евробарометър показва, че 38 % от ползвателите на интернет в ЕС имат притеснения относно сигурността на плащанията онлайн и са променили поведението си поради притеснения във връзка със сигурността — 18% са по-малко склонни да пазаруват онлайн, а 15% са по-малко склонни да използват услуги за интернет банкиране[2].

Сегашната ситуация в ЕС, която е отражение на следвания дотук изцяло доброволен подход, не осигурява достатъчна защита в ЕС срещу инциденти и рискове във връзка с МИС. Съществуващият капацитет за МИС и съществуващите механизми определено не са достатъчни, за да бъдем в крак с бързите промени при заплахите и да гарантираме високо общо ниво на защита във всички държави членки.

Въпреки предприетите инициативи равнището на капацитета и готовността на различните държави членки е твърде различно, което води до фрагментираност на подходите в различните части на Съюза. Като се има предвид, че мрежите и информационните системи са взаимосвързани, общата МИС на ЕС се отслабва от онези държави членки, чието ниво на защита е недостатъчно. Това положение на нещата е пречка и за това между партньорите да възникне доверието, явяващо се предварително условие за сътрудничеството и обмена на информация. Поради това сътрудничество съществува само между държави членки с високо ниво на капацитета, а те са малцинство.

Поради това в момента на равнище ЕС няма ефективен механизъм за сътрудничество и за надежден обмен на информация между държавите членки относно инциденти и рискове във връзка с МИС. Това може да доведе до некоординирани регулаторни интервенции, несъгласувани стратегии и различни стандарти, водещи до недостатъчна защита на МИС в целия ЕС. Могат също така да възникнат и бариери на вътрешния пазар, което ще предизвика разходи за съвместимост за предприятията, работещи в повече от една държава членка.

На последно място, на субектите, управляващи критична инфраструктура или предоставящи услуги от основно значение за функционирането на нашите общества, не са определени съответните задължения да приемат мерки за управление на риска и за обмен на информация със съответните органи. Поради това, от една страна, бизнесът не получава ефективни стимули да осъществява сериозно управление на риска, включващо оценка на риска, и да предприема подходящи стъпки за гарантиране на МИС. От друга страна, компетентните органи не научават за голяма част от инцидентите, или те остават незабелязани от тях. Същевременно информацията за инцидентите е от основно значение, за да могат публичните органи да реагират, да предприемат подходящите мерки за тяхното ограничаване и да определят адекватните стратегически приоритети за МИС.

Съгласно настоящата регулаторна рамка само предприятията, работещи в сферата на далекосъобщенията, са длъжни да предприемат стъпки за управление на риска и да докладват за инциденти, свързани с МИС. Много други сектори обаче разчитат на ИКТ като на основен за тях фактор, и поради това също следва да проявяват загриженост по отношение на МИС. Някои конкретни доставчици на услуги и оператори на

[2] Евробарометър 390/2012.

инфраструктура са особено уязвими поради това, че зависят в голяма степен от добре работещите мрежови и информационни системи. Тези отрасли играят основна роля при предоставянето на ключови за нашата икономика и общество услуги и сигурността на техните системи е от особен интерес за функционирането на вътрешния пазар. Сред тези сектори са банковото дело, фондовите борси, производството, преносът и разпределението на енергия, транспортът (въздушен, железопътен, морски), здравеопазването, интернет услугите и публичните администрации.

Поради това е необходима радикална промяна в начина, по който се работи по МИС в ЕС. За да бъдат осигурени еднакви условия и да бъдат затворени „вратичките“ в законодателството, са необходими законово регламентирани задължения. За да разреши тези проблеми и да повиши нивото на МИС в Европейския съюз, настоящата директива си поставя следните цели.

На първо място, в предложението се изисква всички държави членки да гарантират, че са постигнали минимално ниво на национален капацитет, като са определили компетентни органи, сформирали са екипи за незабавно реагиране при компютърни инциденти (CERT) и са приели национални стратегии за МИС и национални планове за сътрудничество за МИС.

На второ място, националните компетентни органи следва да си сътрудничат в рамките на мрежа, която дава възможност за сигурна и ефективна координация, включително за координиран обмен на информация, както и за откриване и отговор на равнището на ЕС. Чрез тази мрежа държавите членки следва да обменят информация и да си сътрудничат в борбата срещу заплахите и инцидентите в сферата на МИС съгласно европейски план за сътрудничество за МИС.

На трето място, въз основа на модела на Рамковата директива за електронните съобщения предложението се стреми да гарантира развитието на култура на управление на риска и на обмен на информация между частния и публичния сектор. От предприятията в конкретните критични сектори, посочени по-горе, и от публичните администрации ще се изисква да оценяват рисковете, пред които са изправени, и да приемат подходящи и пропорционални мерки за гарантиране на МИС. От тези субекти ще се изисква да докладват на компетентните органи за инцидентите, които компрометират в голяма степен техните мрежи и информационни системи и оказват значително въздействие върху непрекъснатостта на критичните услуги и доставката на стоки.

1.2. Общ контекст

Още през 2001 г. в съобщението си „Мрежова и информационна сигурност: предложение за създаване на европейска политика“ Комисията очерта засилващото се значение на МИС[3]. Това съобщение беше последвано през 2006 г. от приемането на Стратегия за сигурно информационно общество[4], поставяща си за цел да създаде култура на МИС в Европа. Основните елементи на тази стратегия бяха потвърдени в резолюция на Съвета[5].

---

3 COM(2001) 298.

4 COM(2006) 251 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf.

5 2007/068/01.

Освен това на 30 март 2009 г. Комисията прие Съобщение относно защитата на критичната информационна инфраструктура (CIIP)[6], посветено основно на защитата на Европа от кибернетични смущения чрез подобрена сигурност. Със съобщението беше обявен план за действие, който да подпомага усилията на държавите членки да гарантират превенция и отговор. Планът за действие беше приет в заключенията на председателството на министерската конференция относно CIIP, провела се в Талин през 2009 г. На 18 декември 2009 г. Съветът прие резолюция относно европейски подход на сътрудничество по отношение на мрежовата и информационната сигурност[7].

Програмата в областта на цифровите технологии за Европа (DAE)[8], приета през май 2010 г., и свързаните с нея заключения на Съвета[9] откроиха общото разбиране, че доверието и сигурността са основни предпоставки за широкото използване на ИКТ, а оттам и за постигане на целите по измерението „Интелигентен растеж“ на стратегията „Европа 2020“[10]. В глава „Доверие и сигурност“ на DAE се акцентира върху необходимостта всички заинтересовани страни да обединят силите си в едно цялостно усилие за гарантиране на сигурността и устойчивостта на инфраструктурата на ИКТ, като се съсредоточат върху превенцията, готовността и осведомеността, и разработят също така ефективни и координирани механизми за сигурност. В основно действие 6 на DAE по-специално се призовава за мерки, насочени към укрепване на политиката за МИС от високо ниво.

В своето съобщение относно CIIP от март 2011 г. „Постижения и предстоящи стъпки за постигане на сигурност в световното кибернетично пространство“[11] Комисията направи преглед на постигнатите резултати от приемането на плана за действие за CIIP през 2009 г. и стигна до заключението, че изпълнението на плана показва, че само национални подходи за справяне с предизвикателствата пред сигурността и устойчивостта не са достатъчни и че Европа следва да продължи да полага усиля да изгради последователен и кооперативен подход на територията на целия ЕС. В съобщението за CIIP от 2011 г. бяха обявени редица действия, като Комисията призова държавите членки да изградят капацитет за МИС и трансгранично сътрудничество. Повечето от тези действия следваше да бъдат изпълнени до 2012 г., но все още не са факт.

В своите заключения от 27 май 2011 г. относно CIIP Съветът на Европейския съюз наблегна на належащата необходимост ИКТ мрежите и системите да станат устойчиви и сигурни спрямо всякакви възможни нарушения в дейността им, били те случайни или нарочни, в целия ЕС да се постигне високо ниво на готовност, капацитет за сигурност и устойчивост, да се актуализират техническите компетенции с цел да се осигури възможност Европа да посрещне предизвикателствата на защитата на мрежовата и информационна инфраструктура и да се насърчи сътрудничеството между държавите членки, като се създадат механизми за сътрудничество между тях при инциденти.

---

6 COM(2009) 149.
7 2009/C 321/01.
8 COM(2010) 245.
9 Заключения на Съвета от 31 май 2010 г. относно европейската програма за цифровите технологии (10130/10).
10 COM(2010) 2020 и заключения на Европейския съвет от 25/26 март 2010 г. (EUCO 7/10).
11 COM(2011) 163.

1.3. Съществуващи разпоредби на ЕС и международни разпоредби в тази област

В съответствие с Регламент (ЕО) № 460/2004 Европейската общност създаде Европейската агенция за мрежова и информационна сигурност (ENISA)[12] с цел да допринесе за осигуряването на високо ниво и култура на МИС в ЕС. На 30 септември 2010 г.[13] беше прието предложение за модернизиране на ENISA, което в момента се обсъжда в Съвета и в Европейския парламент. Ревизираната регулаторна рамка за електронните съобщения[14], която е в сила от ноември 2009 г., налага задължения за сигурност на доставчиците на електронни съобщения[15]. Тези задължения трябваше да бъдат транспонирани на национално равнище до май 2011 г.

Всички участници, които работят с данни (напр. банки или болници), са задължени от регулаторната рамка за защита на данните[16] да въведат мерки за сигурност за защита на личните данни. Също така съгласно предложението на Комисията от 2012 г. за Общ регламент относно защитата на данните[17] работещите с данни ще са длъжни да докладват за нарушения на сигурността на личните данни на национални надзорни органи. Това означава, че нарушение на МИС, което се отразява на предоставянето на услуга, но не компрометира лични данни (например неналичност на ИКТ система в енергоснабдително дружество, довела до спиране на тока) няма да трябва да бъде докладвано.

Директива 2008/114/ЕО на Съвета от 8 декември 2008 г. относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита Европейската програма за защита на критичната инфраструктура (EPCIP)[18] определя общия, генерален подход към защитата на критичните инфраструктури в ЕС. Целите на EPCIP съответстват напълно на настоящото предложение и директивата следва да се прилага, без да се засяга Директива 2008/114. EPCIP не задължава операторите да докладват за значителни нарушения на сигурността и не предвижда механизми, чрез които държавите членки да си сътрудничат и да отговарят на инциденти.

Съзаконодателите понастоящем обсъждат предложението на Комисията за директива относно атаките срещу информационните системи[19], чиято цел е да се хармонизира инкриминирането на определени видове поведение. Предложението се отнася само до инкриминирането на определени видове поведение и не се занимава с предотвратяването на рисковете и инцидентите по отношение на МИС, отговора на инциденти, свързани с МИС, и ограничаването на тяхното въздействие. Настоящата директива следва да се прилага, без да се засяга Директивата относно атаките срещу информационните системи.

---

12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML.

13 COM(2010) 521.

14 Вж. http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

15 Членове 13а и 13б от Рамковата директива.

16 Директива 2002/58 от 12 юли 2002 г.

17 COM(2012) 11.

18 COM(2006) 786 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.

19 COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF.

На 28 март 2012 г. Комисията прие съобщение относно създаването на Европейски център по киберпрестъпност (ЕС3)[20]. Центърът, който беше създаден на 11 януари 2013 г., е част от Европейската полицейска служба (Европол) и служи като координационно звено в борбата срещу киберпрестъпността в ЕС. Замисълът е ЕС3 да обединява европейските познания във връзка с киберпрестъпността, да оказва подкрепа на държавите членки в изграждането на капацитет, да съдейства на разследванията на киберпрестъпления в държавите членки и в тясно сътрудничество с Евроюст да бъде колективният говорител на европейските правоприлагащи и съдебни органи, разследващи киберпрестъпността.

Европейските институции, агенции и органи сформираха свой собствен екип за незабавно реагиране при компютърни инциденти, известен като CERT-EU.

На международно ниво ЕС работи по киберсигурността както на двустранно, така и на многостранно равнище. Проведената през 2010 г. среща на върха[21] между ЕС и САЩ доведе до сформирането на работна група ЕС—САЩ за киберсигурността и киберпрестъпността. ЕС участва активно и в други имащи отношение международни форуми, като Организацията за икономическо сътрудничество и развитие (ОИСР), общото събрание на ООН, Международния съюз по далекосъобщения (МСД), Организацията за сигурност и сътрудничество в Европа (ОССЕ), Световната среща на високо равнище по въпросите на информационното общество (WSIS) и Форума за управление на интернет (IGF).

2. РЕЗУЛТАТИ ОТ КОНСУЛТАЦИИТЕ СЪС ЗАИНТЕРЕСОВАНИТЕ СТРАНИ И ОЦЕНКИ НА ВЪЗДЕЙСТВИЯТА

2.1. Консултации със заинтересованите страни и използване на експертни становища

От 23 юли до 15 октомври 2012 г. се проведе обществена консултация онлайн на тема „Подобряване на МИС в ЕС“. Комисията получи общо 160 отговора на онлайн въпросника.

Основният извод беше, че заинтересованите страни като цяло подкрепят необходимостта от подобряване на МИС в ЕС. По-специално: 82,8 % от респондентите са на мнение, че държавното управление в ЕС следва да прави повече за осигуряването на високо равнище на МИС; 82,8 % са на мнение, че ползвателите на информация и системи не са наясно със съществуването на заплахи и инциденти в МИС; 66,3 % по принцип биха били „за“ въвеждането на регулаторно изискване за управление на рисковете в МИС; 84,8 % заявяват, че подобни изисквания следва да се определят на равнище ЕС. Голяма част от респондентите са на мнение, че е важно да бъдат приети изисквания за МИС, по-специално в следните сектори: банково дело и финанси (91,1 %), енергетика (89,4 %), транспорт (81,7 %), здравеопазване (89,4 %), интернет услуги (89,1 %), публични администрации (87,5 %). Респондентите считат също така, че ако се въведе изискване за докладване на нарушенията на сигурността пред национални компетентни органи, то трябва да бъде определено на равнище ЕС (65,1 %), и заявяват, че изискването трябва да се отнася и за публичните администрации (93,5 %). На

[20] COM(2012) 140 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF.

[21] http://europa.eu/rapid/press-release_MEMO-10-597_en.htm.

последно място, респондентите заявяват, че изискването за провеждане на управление на риска за МИС в съответствие с последните постижения в тази сфера няма да предизвика значителни допълнителни разходи за тях (63,4 %), като значителни допълнителни разходи няма да предизвика и изискването за докладване на нарушенията на сигурността (72,3 %).

Обсъжданията с държавите членки протекоха в рамките на съответните състави на Съвета, в контекста на Европейския форум за държавите членки (ЕФДЧ), по време на конференцията на ЕС за киберсигурността, организирана от Комисията и Европейската служба за външна дейност на 6 юли 2012 г., както и по време на нарочни двустранни срещи, свикани по искане на отделни държави членки.

Обсъжданията с частния сектор също се проведоха в рамките на Европейското публично-частно партньорство за устойчивост[22] и на двустранни срещи. Що се отнася до публичния сектор, Комисията проведе обсъждания с ENISA и CERT за институциите на ЕС.

2.2. Оценка на въздействието

Комисията направи оценка на въздействието на три варианта на политиката:

Вариант 1: Запазване на обичайната практика („базисен вариант“); запазване на сегашния подход

Вариант 2: Регулаторен подход, състоящ се от законодателно предложение, с което се създава обща правна рамка на ЕС за МИС по отношение на капацитета на държавите членки, механизмите за сътрудничество на равнище ЕС и изискванията по отношение на частните участници и публичните администрации, имащи ключова роля

Вариант 3: Смесен подход, при който се съчетават доброволни инициативи по отношение на капацитета за МИС на държавите членки, механизми за сътрудничество на равнище ЕС и регулаторни изисквания по отношение на частните участници и публичните администрации, имащи ключова роля

Комисията заключи, че вариант 2 би имал най-голямо положително въздействие, тъй като би подобрил значително защитата на потребителите, предприятията и държавното управление в ЕС срещу инциденти, заплахи и рискове, свързани с МИС. По-специално задълженията, вменени на държавите членки, ще гарантират адекватна готовност на национално равнище и ще допринесат за създаването на климат на взаимно доверие, което е предпоставка за ефективно сътрудничество на равнище ЕС. С изграждането на механизми за сътрудничество на равнище ЕС чрез мрежата ще се постигне последователна и координирана превенция и отговор на трансграничните инциденти и рискове в МИС. Въвеждането на изисквания за управление на риска в областта на МИС за публичните администрации и основните частни участници ще създаде силен стимул за ефективно управление на рисковете, свързани със сигурността. Задължението да се докладва за инцидентите в МИС, оказали съществено значение, ще подобри способността за отговор на инциденти и ще стимулира прозрачността. Освен това с решаването на собствените си проблеми ЕС ще бъде в състояние да разшири своето международно влияние и да се превърне в още по-надежден партньор за двустранно и многостранно сътрудничество. Също така ЕС ще бъде в по-добра позиция да насърчава

[22] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

съблюдаването на основните права и да популяризира своите основни ценности зад граница.

Количествената оценка показа, че вариант 2 няма да предизвика прекомерна тежест за държавите членки. Разходите за частния сектор също ще бъдат ограничени, тъй като много от съответните субекти вече трябва да изпълняват съществуващи изисквания във връзка със сигурността (а именно задължението на работещите с данни да предприемат технически и организационни мерки за защита на личните данни, включително мерки от сферата на МИС). Заделените за сигурност средства в частния сектор също са взети предвид.

Настоящото предложение спазва принципите, признати от Хартата на основните права на Европейския съюз, и по-специално правото на зачитане на личния живот и личната кореспонденция, защитата на личните данни, свободата на стопанската инициатива, правото на собственост, правото на ефективни правни средства за защита и на съдебен процес. Настоящата директива трябва да бъде изпълнена в съответствие с тези права и принципи.

3. ПРАВНИ ЕЛЕМЕНТИ НА ПРЕДЛОЖЕНИЕТО

3.1. Правно основание

Европейският съюз е оправомощен да приема мерки с цел създаване на вътрешен пазар или гарантиране на неговото функциониране в съответствие с приложимите разпоредби на договорите (член 26 от Договора за функционирането на Европейския съюз — ДФЕС). В съответствие с член 114 от ДФЕС ЕС може да приема „мерките за *сближаване на законовите, подзаконовите или административните разпоредби на държавите членки,* които имат за цел създаването или функционирането на вътрешния пазар“.

Като беше посочено по-горе, мрежовите и информационните системи играят основна роля в улесняването на трансграничното движение на стоки, услуги и хора. В много случаи те са взаимосвързани, а интернет е глобален по своята природа. Поради това вътрешно присъщо транснационално измерение на системите нарушенията в тяхното функциониране в една държава членка могат да засегнат и други държави членки, както и Съюза като цяло. Устойчивостта и стабилността на мрежите и информационните системи е поради това от основното значение за безпроблемното функциониране на вътрешния пазар.

Европейските законодатели вече признаха необходимостта от хармонизиране на правилата за МИС с цел да се гарантира развитието на вътрешния пазар. Това вече е направено по-специално в Регламент (ЕО) № 460/2004 относно създаване на ENISA[23], чието правно основание е член 114 от ДФЕС.

Неравнопоставеността, произтичаща от разликите в националния капацитет за МИС, политиките и равнището на готовност на държавите членки, водят до появата на бариери на вътрешния пазар и са основание за действие на равнище ЕС.

[23] 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).

3.2. Субсидиарност

Европейската намеса в сферата на МИС е оправдана с оглед на принципа на субсидиарност.

На първо място, като се има предвид трансграничният характер на МИС, отсъствието на интервенция на равнище ЕС би довело до ситуация, при която всяка държава членка действа самостоятелно, като не се съобразява с взаимозависимостта на мрежовите и информационните системи в ЕС. Едно подходящо ниво на сътрудничество между държавите членки би било гаранция, че рисковете по отношение на МИС могат да се управляват добре в трансграничните условия, при които възникват те. Разликите в регламентирането на МИС са бариера пред дружествата, които желаят да работят в няколко държави, и пред постигането на общи икономии от мащаба.

На второ място, законово регламентираните задължения на равнище ЕС са необходими с оглед осигуряването на еднакви условия и затварянето на „вратичките“ в законодателството. Изцяло доброволният подход доведе до сътрудничество, част от което са само държави членки с високо ниво на капацитета, а те са малцинство. За да бъдат включени всички държави членки, е необходимо да се гарантира, че капацитетът на всяка една от тях е на изискваното минимално равнище. Мерките за МИС, приети от правителствата, трябва да бъдат последователни и координирани с оглед ограничаването и намаляването до минимум на последиците от инцидентите във връзка с МИС. В рамките на мрежата чрез обмен на най-добри практики и постоянно участие на ENISA компетентните органи и Комисията ще си сътрудничат с цел да бъде улеснено уеднаквяването на изпълнението на директивата в целия ЕС. Освен това съгласуваните политически действия в сферата на МИС могат да окажат изключително благоприятно влияние върху ефективната защита на основните права, и по-специално на правото на защита на личните данни и неприкосновеността на личния живот. Поради това действието на равнище ЕС би подобрило ефективността на съществуващите национални политики и би улеснило тяхното разгръщане.

Предлаганите мерки са оправдани и от гледна точка на пропорционалността. Изискванията за държавите членки са определени на минимално необходимото равнище за постигане на адекватна готовност и гарантиране на сътрудничество, почиващо но доверие. Това дава възможност държавите членки да отчитат надлежно националната си специфика и да гарантират, че общите принципи на ЕС се прилагат съразмерно. Широкото приложно поле ще даде възможност на държавите членки да изпълнят директивата с оглед на действителните рискове, с които се сблъскват на национално равнище и които са посочили в националната си стратегия за МИС. Изискванията за осъществяване на управление на риска са насочени само към критичните субекти и налагат меки, които са пропорционални на рисковете. По време на обществената консултация беше подчертана необходимостта да се гарантира сигурността на тези критични субекти. Изискванията за докладване ще засегнат само инциденти със значително отражение. Както беше посочено по-горе, мерките няма да причинят непропорционални разходи, тъй като от много от субектите, например от работещите с лични данни, вече се изисква съгласно сега действащите правила в сферата да гарантират защитата на личните данни.

С цел да се избегне налагането на несъразмерна тежест върху малките участници, и по-специално върху МСП, изискванията са съразмерни с риска, който съществува по отношение на съответната мрежова или информационна система, и не се прилагат за

микропредприятия. Рисковете ще трябва да бъдат идентифицирани най-напред от субектите, които следва да изпълнят тези задължения и които ще трябва да решат и какви да бъдат мерките, с които да ограничат тези рискове.

Обявените цели могат да бъдат постигнати по-успешно на равнище ЕС, отколкото от държави членки поотделно с оглед на трансграничните аспекти на инцидентите и рисковете в МИС. Поради това ЕС може да приеме мерки в съответствие с принципа на субсидиарност, посочен в член 5 от Договора за Европейски съюз. В съответствие с принципа на пропорционалност, предлаганата директива не надхвърля необходимото за постигането на тези цели.

С оглед постигане на целите Комисията следва да бъде оправомощена да приема делегирани актове в съответствие с член 290 от ДФЕС за допълването или изменението на определени несъществени елементи на основния акт. Предложението на Комисията има за цел също така да се подпомогне съразмерността в изпълнението на задълженията, възложени на частни и публични участници.

С цел осигуряване на еднакви условия за изпълнението на основния акт Комисията следва да бъде оправомощена да приема актове за изпълнение в съответствие с член 291 от ДФЕС.

Като се има предвид по-специално широкият обхват на предлаганата директива, това, че тя засяга силно регулирани сфери, както и правните задължения, произтичащи от глава IV от нея, нотификациите относно мерките за транспониране следва да се придружават от обяснителни документи. В съответствие със Съвместната политическа декларация от 28 септември 2011 г. на държавите членки и Комисията относно обяснителните документи държавите членки се ангажират в случаите, когато това е оправдано, да прилагат към нотификацията за мерките си за транспониране един или повече документи, поясняващи връзката между компонентите на дадена директива и съответните части от националните инструменти за транспониране. Законодателят счита, че по отношение на настоящата директива, предаването на такива документи е оправдано.

4. ОТРАЖЕНИЕ ВЪРХУ БЮДЖЕТА

Сътрудничеството и обменът на информация между държавите членки следва да се подкрепят от сигурна инфраструктура. Предложението има отражение върху бюджета на ЕС само ако държавите членки изберат да адаптират съществуващата инфраструктура (напр. sTESTA) и възложат това на Комисията в рамките на МФР 2014-2020 г. Очаква се, че еднократните разходи ще бъдат в размер на 1 250 000 EUR и ще бъдат понесени от бюджета на ЕС, бюджетен ред 09.03.02 (Насърчаване на взаимосвързаността и оперативната съвместимост на националните публични услуги онлайн, както и на достъпа до тези мрежи — Раздел 09.03, Механизъм за свързване на Европа — далекосъобщителни мрежи), при условие че са налични достатъчно средства по МСЕ. Като алтернатива държавите членки могат или да си поделят еднократните разходи за адаптирането на съществуващата инфраструктура, или да решат да изградят нова инфраструктура и да поемат разходите, които се оценяват на приблизително 10 млн. евро годишно.

2013/0027 (COD)

Предложение за

ДИРЕКТИВА НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

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

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейския икономически и социален комитет[1],

след консултация с Европейския надзорен орган по защита на данните,

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

(1) Мрежовите и информационните системи и услуги имат изключително важна роля в нашето общество. Тяхната надеждност и сигурност са от основно значение за стопанските дейности и общественото благополучие и особено за функционирането на вътрешния пазар.

(2) Мащабите на нарочно предизвиканите или случайно настъпили инциденти в сигурността и честотата, с която се появяват те, се увеличават и представляват крупна заплаха пред функционирането на мрежите и информационните системи. Подобни инциденти могат да попречат на осъществяването на стопански дейности, да причинят значителни финансови загуби, да подкопаят доверието на потребителите и да причинят големи вреди на икономиката на Съюза.

(3) Като комуникационен инструмент без граници цифровите информационни системи и най-вече интернет играят основна роля за улесняването на трансграничното движение на стоки, услуги и хора. Поради транснационалния характер на тези системи значителните нарушения в дейността им в една държава членка могат да засегнат и други държави членки, както и Съюза като цяло. Устойчивостта и стабилността на мрежите и информационните системи е поради това от основно значение за безпроблемното функциониране на вътрешния пазар.

[1] ОВ С […], […], стр. […].

(4) На равнище Съюза следва да бъде изграден механизъм за сътрудничество, който да дава възможност за обмен на информация и координирано откриване и отговор във връзка с мрежовата и информационна сигурност („МИС“). За да бъде ефективен и приобщаващ този механизъм, е от основно значение всички държави членки да разполагат с минимален капацитет и със стратегия, гарантираща високо равнище на МИС на тяхна територия. Към публичните администрации и операторите на критична информационна инфраструктура следва да се прилагат и минимални изисквания по отношение на сигурността с цел да се насърчава култура на управление на риска и да се гарантира докладването на най-сериозните инциденти.

(5) С цел да бъдат обхванати всички имащи отношение инциденти и рискове настоящата директива следва да се прилага за всички мрежови и информационни системи. Задълженията за публичните администрации и участниците на пазара обаче не следва да се прилагат за предприятията, предоставящи обществени съобщителни мрежи или обществено достъпни електронни съобщителни услуги по смисъла на 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)[2], които са обект на конкретните изисквания за сигурност и цялост, определени в член 13а от посочената Директива, нито към доставчиците на удостоверителни услуги.

(6) Съществуващият капацитет не е достатъчен, за да гарантира високо равнище на МИС в Съюза. Равнището на готовност на различните държави членки е твърде различно, което води до фрагментираност на подходите в различните части на Съюза. Това от своя страна е причина за нееднаква степен на защита на потребителите и стопанските субекти и подкопава общото ниво на МИС в Съюза. Отсъствието на общи минимални изисквания за публичните администрации и участниците на пазара от своя страна прави невъзможно изграждането на глобален и ефективен механизъм за сътрудничество на равнище Съюза.

(7) Поради това ефективният отговор на предизвикателствата пред сигурността на мрежовите и информационните системи изисква глобален подход на равнище Съюза, който да включва общи минимални изисквания за изграждане на капацитет и планиране, обмен на информация и координиране на действията и общи минимални изисквания по отношение на сигурността за всички имащи отношение участници на пазара и публични администрации.

(8) Разпоредбите на настоящата директива следва да не засягат възможността всяка държава членка да предприема необходимите мерки, с които да гарантира сигурността на защитата на своите основни интереси в сферата на сигурността, да опазва публичната политика и публичната сигурност и да дава възможност за разследването, разкриването и преследването на престъпления. В съответствие с член 346 от ДФЕС нито една държава членка не може да бъде задължавана да предоставя информация, чието разкриване тя счита за противоречащо на основните интереси на нейната сигурност.

---

[2] ОВ L 108, 24.4.2002 г., стр. 33.

(9) С цел постигане и поддържане на общо високо равнище на сигурност на мрежовите и информационните системи всяка държава членка следва да има национална стратегия за МИС, в която да са определени стратегическите цели и конкретните действия на политиката, които ще бъдат изпълнявани. На национално ниво следва да бъдат разработени планове за сътрудничество за МИС, които да отговарят на основните изисквания, с цел да бъдат постигнати нива на капацитет на отговора, даващи възможност в случай на инциденти за ефективно и ефикасно сътрудничество на национално равнище и на равнище Съюза.

(10) С цел да се осигури възможност за ефективно изпълнение на разпоредбите, приети в съответствие с настоящата директива, във всяка държава членка следва да бъде създаден или определен орган, който да отговоря за координацията на въпросите във връзка с МИС и да бъде център за трансгранично сътрудничество. Тези органи следва да получат достатъчно технически, финансови и човешки ресурси, за да се гарантира, че са в състояние да изпълняват ефективно и ефикасно определените им задачи и по този начин да постигат целите на настоящата директива.

(11) Всички държави членки следва да бъдат достатъчно добре подготвени и като технически, и като организационен капацитет да предотвратяват, реагират на и ограничават инциденти и рискове в мрежовите и информационните системи. За целта във всички държави членки следва да бъдат създадени добре функциониращи екипи за незабавно реагиране при компютърни инциденти, отговарящи на основни изисквания, които да гарантират наличието на ефективен и съвместим капацитет за справяне с инциденти и рискове и да осигуряват ефикасно сътрудничество на равнище Съюза.

(12) Като използват значителния напредък, постигнат в рамките на Европейския форум за държавите членки (ЕФДЧ) при насърчаването на дискусиите и обмена на добри практики в политиките, включително разработването на принципи на европейското сътрудничество при киберкризи, държавите членки и Комисията следва да създадат мрежа, която да им осигурява постоянна комуникация и да оказва подкрепа на тяхното сътрудничество. Този сигурен и ефикасен механизъм за сътрудничество следва да дава възможност за структуриран и координиран обмен на информация, откриване и отговор на равнище Съюза.

(13) Европейската агенция за мрежова и информационна сигурност („ENISA“) следва да оказва подкрепа на държавите членки и на Комисията, като предоставя на разположение своите експертни познания и консултации и улеснява обмена на най-добри практики. Комисията по-специално следва да се консултира с ENISA при прилагането на настоящата директива. За да се осигури навременна и ефикасна информация за държавите членки и Комисията, в рамките на мрежата за сътрудничество следва да се подават ранни предупреждения за инциденти и рискове. С цел у държавите членки да бъдат натрупани познания и изграден капацитет мрежата за сътрудничество следва да служи и като инструмент за обмен на най-добри практики, които да подпомагат нейните членове в изграждането на капацитет и да направляват организирането на партньорски проверки и учения за МИС.

(14) Следва да се създаде сигурна инфраструктура за обмен на информация, която да дава възможност за предаване на чувствителна и поверителна информация в мрежата за сътрудничество**.** Без да се засяга задължението на държавите членки да уведомяват в мрежата за сътрудничество за инциденти и рискове, чието измерение е от мащабите на Съюза, достъпът до поверителна информация от други държави членки следва да се предоставя само на държави членки, които са доказали, че техните технически, финансови и човешки ресурси и процедури, както и тяхната комуникационна инфраструктура гарантират тяхното ефикасно, ефективно и сигурно участие в мрежата.

(15) Тъй като повечето мрежови и информационни системи се експлоатират от частни субекти, сътрудничеството между публичния и частния сектор е от основно значение. Участниците на пазара следва да бъдат насърчавани да развиват свои собствени механизми за неофициално сътрудничество за гарантиране на МИС. Те следва също така да си сътрудничат с публичния сектор и да обменят информация и най-добри практики в размяна на оперативна подкрепа в случай на инциденти.

(16) С цел да се гарантира прозрачност и надлежно информиране на гражданите на ЕС и участниците на пазара компетентните органи следва да създадат общ уебсайт, на който да публикуват неповерителна информация относно инциденти и рискове.

(17) В случаите, когато информация се счита за поверителна в съответствие с националните разпоредби и тези на Съюза относно търговската тайна, се гарантира поверителност при провеждането на дейностите и изпълнението на целите, определени в настоящата директива.

(18) Въз основа по-специално на националния опит в управлението на кризи и в сътрудничество с ENISA Комисията и държавите членки следва да разработят план на Съюза за сътрудничество за МИС, в който да бъдат определени механизми за сътрудничество за противопоставяне на рискове и инциденти. Този план следва да бъде надлежно отчитан при работата с ранни предупреждения в мрежата за сътрудничество.

(19) Подаването на ранно предупреждение в мрежата следва да се изисква единствено когато мащабът и тежестта на инцидента или риска са или могат да бъдат от такова значение, че е необходима информация или координация на отговора на равнище Съюза. Ранните предупреждения следва поради това да бъдат ограничени до действителни или потенциални инциденти и рискове, които се разрастват бързо, превишават националния капацитет за отговор или засягат повече от една държава членка. С цел да се осигури възможност за добра оценка в мрежата за сътрудничество следва да се предава всичката информация, имаща отношение към оценката на риска или инцидента**.**

(20) При получаване на ранно предупреждение и след оценката му компетентните органи следва да постигат съгласие за координиран отговор съгласно плана на Съюза за сътрудничество за МИС. Компетентните органи както и Комисията следва да бъдат информирани за мерките, предприети на национално ниво вследствие на координирания отговор.

(21) С оглед на глобалния характер на проблемите в МИС е необходимо по-тясно международно сътрудничество за повишаване на стандартите за сигурност и обмен на информация и насърчаване на общ глобален подход към въпросите на МИС.

(22) Отговорностите за гарантиране на МИС до голяма степен се носят от публичните администрации и участниците на пазара. Следва да се насърчава културата на управление на риска, част от която са оценката на риска и изпълнението на мерки за сигурност, отговарящи на срещаните рискове, и тази култура да се развива чрез подходящи регулаторни изисквания и доброволни практики от страна на сектора. Постигането на еднакви условия също е от основно значение за ефективното функциониране на мрежата за сътрудничество при гарантирането на ефективно сътрудничество от страна на всички държави членки.

(23) В Директива 2002/21/ЕО се изисква предприятията, предоставящи обществени съобщителни мрежи или обществено достъпни електронни съобщителни услуги, да предприемат подходящи мерки за опазване на своята цялост и сигурност и се въвеждат изисквания за уведомяване в случай на нарушаване на сигурността или компрометиране на целостта. 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)[3] се изисква доставчиците на обществено достъпни електронни съобщителни услуги да предприемат подходящи технически и организационни мерки за опазване на сигурността на своите услуги.

(24) Обхватът на тези задължения следва да бъде разширен извън сектора на електронните съобщения и да обхване ключовите доставчици на услуги на информационното общество, определени 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[4], които са в основата на услуги на информационното общество надолу по веригата или на онлайн дейности, като платформи за електронна търговия, портали за плащания в интернет, социални мрежи, машини за търсене, услуги за изчисления в облак, магазини за приложни програми. Нарушеното предоставяне на тези основни услуги на информационното общество прави невъзможно предоставянето на други услуги на информационното общество, за които те са основен фактор. Разработващите софтуер и производителите на хардуер не са доставчици на услуги на информационното общество и поради това са изключени. Тези задължения трябва да обхванат и публичните администрации, и операторите на критична инфраструктура, които разчитат в голяма степен на информационни и комуникационни технологии и са от съществено значение за поддържането на основни икономически или обществени функции, като електро- и газоснабдяване, транспорт, кредитни институции, фондови борси и здравеопазване. Нарушаването на дейността на тези мрежови и информационни системи би засегнало вътрешния пазар.

---

[3] ОВ L 201, 31.7.2002 г., стр. 37.

[4] ОВ L 204, 21.7.1998 г., стр. 37.

(25) Техническите и организационните мерки, наложени на публичните администрации и участниците на пазара, следва да не изискват проектирането, разработването или производство по определен начин на конкретен търговски продукт на информационните и комуникационните технологии.

(26) Публичните администрации и участниците на пазара следва да гарантират сигурността на мрежите и системите, които контролират. Това са предимно частни мрежи и системи, управлявани или от вътрешен ИТ персонал, или чиято сигурност е възложена на външни изпълнители. Задълженията във връзка със сигурността и уведомяването следва да се прилагат за съответния участник на пазара и за съответната публична администрация без оглед на това дали те извършват вътрешно поддръжката на своите мрежови и информационни системи или я възлагат на външни изпълнители.

(27) С цел да се избегне налагането на несъразмерна финансова и административна тежест върху малките участници и потребители изискванията следва да бъдат съразмерни с риска, който съществува по отношение на съответната мрежова или информационна система, като се отчитат последните постижения по отношение на подобни мерки. Тези изисквания следва да не се прилагат за микропредприятията.

(28) Компетентните органи следва да обръщат необходимото внимание на запазването на неофициалните и ползващи се с доверие канали за споделяне на информация между участниците на пазара и между публичния и частния сектор. При даването на публичност на докладваните инциденти компетентните органи следва да постигат нужния баланс между интереса на обществеността да бъде информирана за заплахите и възможните търговски щети и накърняването на репутацията на публичните администрации и участниците на пазара, които докладват за инцидентите. При изпълнението на задълженията за уведомяване компетентните органи следва да обръщат особено внимание на необходимостта информацията за уязвимите аспекти на продуктите да бъде запазвана строго поверителна до извършването на съответните корекции по отношение на сигурността.

(29) Компетентните органи следва да разполагат с необходимите средства за изпълнението на своите задължения, включително с правомощия да получават достатъчно информация от участниците на пазара и публичните администрации с цел оценка на нивото на сигурност на мрежовите и информационните системи, както и надеждни и комплексни данни за действителните инциденти, които са имали отражение върху работата на мрежовите и информационните системи.

(30) В много случаи инцидентите са предизвикани от престъпни деяния. Престъпният характер на инцидентите може да бъде обект на подозрение, дори ако доказателствата в подкрепа на подобно твърдение не са достатъчно убедителни в самото начало. В подобни случаи съответното сътрудничество между компетентните органи и правоприлагащите органи следва да бъде част от един ефикасен и комплексен отговор на заплахата от инциденти в сигурността. Утвърждаването на безопасна, сигурна и по-устойчива среда изисква по-специално системно докладване на инцидентите с предполагаем сериозен престъпен характер на правоприлагащите органи. Сериозният престъпен

характер на инцидентите следва да се оценява в светлината на законодателството на ЕС относно киберпрестъпността.

(31) В много случаи вследствие на инциденти се компрометират лични данни. В този контекст компетентните органи и органите за защита на данните следва да си сътрудничат и да обменят информация относно всички имащи отношение въпроси с цел справяне с нарушенията на сигурността на лични данни, предизвикани от инциденти. Държавите членки изпълняват задължението да уведомяват за инциденти по отношение на сигурността по начин, при който се намалява до минимум административната тежест, в случай че инцидентът във връзка със сигурността представлява и нарушение на сигурността на лични данни съгласно Регламента на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни[5]. Като поддържа връзка с компетентните органи и органите за защита на данните, ENISA би могла да оказва съдействие, като разработва механизми за обмен на информация и образци, чрез които се избягва необходимостта от два образеца за уведомленията. Единният образец за уведомленията ще улесни докладването на инцидентите, при които са компрометирани лични данни, и по този начин ще облекчи административната тежест върху бизнеса и публичните администрации.

(32) Стандартизацията на изискванията относно сигурността е процес, движен от пазарни сили. С цел да гарантират последователно прилагане на стандартите за сигурност държавите членки следва да насърчават съответствието или спазването на посочените стандарти с оглед осигуряването на високо ниво на сигурност на равнище Съюза. За тази цел може да бъде необходимо да бъдат изготвени хармонизирани стандарти, чиято разработка следва да бъде в съответствие с Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета от 25 октомври 2012 г. относно европейската стандартизация, за изменение на директиви 89/686/ЕИО и 93/15/ЕИО на Съвета и на директиви 94/9/ЕО, 94/25/ЕО, 95/16/ЕО, 97/23/ЕО, 98/34/ЕО, 2004/22/ЕО, 2007/23/ЕО, 2009/23/ЕО и 2009/105/ЕО на Европейския парламент и на Съвета и за отмяна на Решение 87/95/ЕИО на Съвета и на Решение № 1673/2006/ЕО на Европейския парламент и на Съвета[6].

(33) Комисията следва периодично да прави преглед на настоящата директива, по-специално с оглед да определя необходимостта от изменения в светлината на променящите се технологични или пазарни условия.

(34) С цел да се даде възможност за правилното функциониране на мрежата за сътрудничество на Комисията следва да бъде делегирано правомощието да приема актове в съответствие с член 290 от Договора за функционирането на Европейския съюз по отношение на определянето на критериите, на които трябва да отговорят държавите членки, за да им бъде разрешено да участват в сигурната система за обмен на информация, относно по-подробното специфициране на началните събития, водещи до ранни предупреждения, и относно определянето на обстоятелствата, при които се изисква участниците на пазара и публичните администрации да изпращат уведомления за инцидентите.

---

5 SEC(2012) 72 final.

6 ОВ L 316, 14.11.2012 г., стр. 12.

(35) От особено значение е Комисията да провежда надлежни консултации по време на своята подготвителна дейност, включително на експертно ниво. При подготовката и съставянето на делегираните актове Комисията следва да гарантира едновременното, навременно и надлежно предаване на съответните документи на Европейския парламент и Съвета.

(36) С цел да се осигурят еднакви условия за изпълнението на настоящата директива на Комисията следва да бъдат предоставени правомощия за изпълнение по отношение на сътрудничеството между компетентните органи и Комисията в рамките на мрежата за сътрудничество, достъпа до сигурната инфраструктура за обмен на информация, плана на Съюза за сътрудничество, форматите и процедурите, приложими при информирането на обществеността за инциденти, и стандартите и/или техническите спецификации, имащи отношение към МИС. Тези правомощия следва да се изпълняват в съответствие с Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета от 16 февруари 2011 г. за установяване на общите правила и принципи относно реда и условията за контрол от страна на държавите членки върху упражняването на изпълнителните правомощия от страна на Комисията[7].

(37) При прилагането на настоящата директива Комисията следва да поддържа според необходимостта връзка със съответните секторни комитети и със съответните органи, създадени на равнище ЕС, по-специално в сферата на енергетиката, транспорта и здравеопазването.

(38) Информацията, която даден компетентен орган счита за поверителна, следва да бъде обменяна с Комисията и останалите компетентни органи в съответствие с националните разпоредби и тези на Съюза относно търговската тайна само ако подобен обмен е абсолютно необходим за прилагането на настоящата директива. Обменената информация следва да се ограничава до имащата отношение информация и да бъде пропорционална на целите на подобен обмен.

(39) Обменът на информация относно рисковете и инцидентите в рамките на мрежата за сътрудничество и изпълнението на изискванията за уведомяване на националните компетентни органи за инциденти може да изисква обработката на лични данни. Подобна обработка на лични данни е необходима, за да се изпълнят целите на обществения интерес, преследвани от настоящата директива, и следователно е законосъобразна съгласно член 7 от Директива 95/46/ЕО. По отношение на тези законни цели тя не представлява непропорционално и неприемливо вмешателство, нарушаващо в същината му правото на защита на личните данни, гарантирано от член 8 от Хартата на основните права. При прилагането на настоящата директива следва да се прилага 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[8], както е целесъобразно. Когато институции и органи на Съюза обработват данни, обработката с цел изпълнение на настоящата директива следва да съответства на Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на

[7] ОВ L 55, 28.2.2011 г., стр.13.
[8] ОВ L 145, 31.5.2001 г., стр. 43.

обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни.

(40) Тъй като целите на настоящата директива, а именно да гарантира високо равнище на МИС в Съюза, не могат да бъдат постигнати в достатъчна степен от държавите членки поотделно и следователно на равнище Съюза може да бъде постигнат по добър ефект от действията, Съюзът може да приема мерки в съответствие с принципа на субсидиарност, определен в член 5 от Договора за Европейски съюз. В съответствие с принципа на пропорционалност, определен в същия член, настоящата директива не надхвърля необходимото за постигане на посочените цели.

(41) Настоящата директива зачита основните права и спазва принципите, признати в Хартата на основните права на Европейския съюз, и по-специално правото на зачитане на личния живот и личната кореспонденция, защитата на личните данни, свободата на стопанската инициатива, правото на собственост, правото на ефективни правни средства за защита и на съдебен процес. Настоящата директива трябва да бъде изпълнена в съответствие с тези правила и принципи,

ПРИЕХА НАСТОЯЩАТА ДИРЕКТИВА:

ГЛАВА I

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет и приложно поле

1. С настоящата директива се определят мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност (наричана по-долу „МИС“) в Съюза.

2. За тази цел с настоящата директива се:

а) определят задължения на всички държави членки относно превенцията, действията и отговора във връзка с рискове и инциденти, засягащи мрежи и информационни системи;

б) създава се механизъм за сътрудничество между държавите членки с цел да се гарантира единното прилагане на настоящата директива в Съюза и, когато е необходимо, координираните и ефективни действия при рискове и инциденти, засягащи мрежи и информационни системи, и отговора на тях;

в) определят се изисквания за сигурност за участниците на пазара и публичните администрации.

3. Изискванията за сигурност, предвидени в член 14, не се прилагат за предприятията, предоставящи обществени съобщителни мрежи или обществено достъпни електронни съобщителни услуги по смисъла на Директива 2002/21/ЕО, които отговарят на специфичните изисквания за

сигурност и цялост, определени в членове 13а и 13б от посочената директива, нито към доставчиците на удостоверителни услуги.

4. Настоящата директива не засяга законодателството на ЕС относно киберпрестъпността и Директива 2008/114/ЕО на Съвета от 8 декември 2008 г. относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита[9].

5. Настоящата директива не засяга също така 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 данни[10], 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 и Регламента на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни[11].

6. Обменът на информация в рамките на мрежата за сътрудничество по глава III и уведомленията за инциденти във връзка с МИС съгласно член 14 могат да изискват обработка на лични данни. Подобна обработка, необходима с цел да бъдат изпълнени целите на обществения интерес, които настоящата директива преследва, се разрешава от държавата членка в съответствие с член 7 от Директива 95/46/ЕО и Директива 2002/58/ЕО, така както е въведен в националното законодателство.

Член 2

Минимална хармонизация

Държавите членки имат право да приемат или запазват разпоредби, които гарантират по-високо ниво на сигурност, без това да засяга техните задължения съгласно законодателството на Съюза.

Член 3

Определения

За целите на настоящата директива се прилагат следните определения:

(1) „мрежова и информационна система“ означава:

a) електронна съобщителна мрежа по смисъла на Директива 2002/21/ЕИО, както и

[9] ОВ L 345, 23.12.2008 г., стр. 75.
[10] ОВ L 281, 23.11.1995 г. стр. 31.
[11] SEC(2012) 72 final.

б) всяко устройство или всяка група взаимосвързани или имащи връзка помежду си устройства, едно или няколко от които, следвайки програма, извършват автоматична обработка на компютърни данни, както и

в) компютърни данни, записвани, обработвани, извличани или пренасяни от елементи, обхванати от букви а) и б), с цел обработка, използване, защита и поддръжка;

(2) „сигурност“ означава способността на мрежа или информационна система да издържа — при дадено равнище на увереност — на инциденти или злонамерени действия, които повлияват на наличността, автентичността, целостта и поверителността на съхранявани или пренасяни данни или на свързаните с тях услуги, предлагани от или достъпни посредством тази мрежова и информационна система;

(3) „риск“ означава обстоятелство или събитие, което има потенциално неблагоприятно отражение върху сигурността;

(4) „инцидент“ означава обстоятелство или събитие, което има действително неблагоприятно отражение върху сигурността;

(5) „услуга на информационното общество“ означава услуга по смисъла на член 1, точка 2 от Директива 98/34/ЕО;

(6) „план за сътрудничество за МИС“ означава план, в който се определя рамката на институционалните роли, отговорности и процедури с оглед поддържане или възстановяване на работата на мрежи и информационни системи в случай на риск или инцидент, който ги засяга;

(7) „действия при инцидент“ означава всички процедури в подкрепа на анализа, ограничаването и отговора на инцидента;

(8) „участник на пазара “ означава:

а) доставчик на услуги на информационното общество, които правят възможно предоставянето на други услуги на информационното общество, неизчерпателен списък на които е даден в приложение II;

б) оператор на критична инфраструктура, която е от основно значение за поддържането на особено важни икономически и обществени дейности в сферата на енергетиката, транспорта, банковото дело, фондовите борси и здравеопазването, неизчерпателен списък на които е даден в приложение II;

(9) „стандарт“ означава стандарт, посочен в Регламент (ЕО) № 1025/2012;

(10) „спецификация“ означава спецификация, посочена в Регламент (ЕО) № 1025/2012;

(11) „доставчик на удостоверителни услуги“ означава физическо или юридическо лице, което доставя каквато и да било електронна услуга, състояща се в създаване, проверка, валидиране, обработка и съхраняване на електронни

подписи, електронни печати, електронни времеви печати, електронни документи, услуги по електронно доставяне, удостоверяване на автентичността на уебсайтове, електронни удостоверения, включително удостоверения за електронен подпис и електронен печат.

ГЛАВА II

НАЦИОНАЛНИ РАМКИ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

Член 4

Принцип

Държавите членки гарантират високо ниво на сигурност на мрежовите и информационните системи на тяхна територия в съответствие с настоящата директива.

Член 5

Национална стратегия за МИС и национален план за сътрудничество за МИС

1. Всяка държава членка приема национална стратегия за МИС, в която са определени стратегически цели, конкретни мерки на политиката и регулаторни мерки за постигане и поддържане на високо равнище на мрежова и информационна сигурност. В националната стратегия за МИС се разглеждат по-специално следните въпроси:

а) определяне на целите и приоритетите на стратегията въз основа на анализ на актуалните рискове и инциденти;

б) управленска рамка за постигане на стратегическите цели и приоритети, включително ясно определени роли и отговорности на структурите на държавното управление и на останалите имащи отношение действащи лица;

в) набелязване на основните мерки във връзка с готовността, отговора и възстановяването, включително механизми за сътрудничество между публичния и частния сектор;

г) основна информация за образователните и обучителните програми и за програмите за повишаване на осведомеността;

д) планове за научноизследователска и развойна дейност и описание на начина, по който в тях са отразени набелязаните приоритети.

2. Националната стратегия за МИС съдържа национален план за сътрудничество за МИС, който отговаря най-малкото на следните изисквания:

а) план за оценка на риска с цел установяване на рисковете и оценка на въздействието на потенциалните инциденти;

б) определяне на ролите и отговорностите на различните действащи лица, участващи в изпълнението на плана;

в) определяне на процесите за сътрудничество и комуникация, чрез които се гарантират превенцията, откриването, отговорът, отстраняването на смущенията и възстановяването, с модификации в тях в зависимост от степента на тревога;

г) пътна карта за учения и обучения във връзка с МИС с цел подсилване, валидиране и тестване на плана. Извлечените поуки се документират и включват при актуализациите на плана.

3. Националната стратегия за МИС и националният план за сътрудничество за МИС се предоставят на Комисията в едномесечен срок след тяхното приемане.

Член 6

Национален компетентен орган по сигурността на мрежовите и информационните системи

1. Всяка държава членка определя национален компетентен орган по сигурността на мрежовите и информационните системи („компетентния орган“).

2. Компетентните органи следят за прилагането на настоящата директива на национално равнище и спомагат за последователното ѝ прилагане в целия Съюз.

3. Държавите членки гарантират, че компетентните органи разполагат с достатъчно технически, финансови и човешки ресурси, за да изпълняват ефективно и ефикасно определените им задачи и по този начин да постигат целите на настоящата директива. Държавите членки гарантират, че чрез мрежата, посочена в член 8, компетентните органи си сътрудничат ефективно, ефикасно и сигурно.

4. Държавите членки гарантират, че компетентните органи получават уведомленията за настъпили инциденти от публичните администрации и участниците на пазара, както е посочено в член 14, параграф 2, и разполагат с правомощията за прилагане и изпълнение, посочени в член 15.

5. Компетентните органи се консултират помежду си и си сътрудничат винаги, когато това е целесъобразно, със съответните национални правоприлагащи органи, включително с органите за защита на данните.

6. Всяка държава членка уведомява незабавно Комисията за определения от нея компетентен орган, неговите задачи и за всякакви последващи промени в тях. Всяка държава членка прави обществено достояние акта, с който определя компетентния орган.

Член 7

Екипи за незабавно реагиране при компютърни инциденти

1. Всяка държава членка сформира екип за незабавно реагиране при компютърни инциденти (наричан по-долу „CERT“), който отговаря за предприемането на действия при инциденти и рискове в съответствие с подробно определена процедура, която отговаря на изискванията, посочени в приложение I, точка 1. CERT може да бъде сформиран в рамките на компетентния орган.

2. Държавите членки гарантират, че CERT разполагат с достатъчно технически, финансови и човешки ресурси, за да изпълняват ефективно задачите, определени им в приложение I, точка 2.

3. Държавите членки гарантират, че на национално равнище CERT разчитат на сигурна и устойчива комуникационна и информационна инфраструктура, която има обща и оперативна съвместимост със сигурната система за обмен на информация, посочена в член 9.

4. Държавите членки информират Комисията за ресурсите и правомощията на CERT, както и за процедурата за предприемане на действия при инциденти, която CERT следва.

5. Дейността на CERT е обект на надзор от страна на компетентния орган, който прави редовно преглед на адекватността на неговите ресурси и правомощия и на ефективността на процедурата за предприемане на действия при инциденти, която той следва.

ГЛАВА III

СЪТРУДНИЧЕСТВО МЕЖДУ КОМПЕТЕНТНИТЕ ОРГАНИ

Член 8

Мрежа за сътрудничество

1. Компетентните органи и Комисията изграждат мрежа („мрежа за сътрудничество“) с цел да си сътрудничат в борбата с рисковете и инцидентите, засягащи мрежовите и информационните системи.

2. Мрежата за сътрудничество осигурява постоянна комуникация между Комисията и компетентните органи. При поискване Европейската агенция за мрежова и информационна сигурност („ENISA“) оказва съдействие на мрежата за сътрудничество, като ѝ предоставя експертни познания и консултации.

3. В рамките на мрежата за сътрудничество компетентните органи:

   а) разпространяват ранни предупреждения за рискове и инциденти в съответствие с член 10;

   б) гарантират наличието на координиран отговор в съответствие с член 11;

   в) редовно публикуват на общ уебсайт неповерителна информация относно актуални ранни предупреждения и координирани отговори;

г) съвместно обсъждат и оценяват по искане на някоя от държавите членки или на Комисията една или няколко национални стратегии за МИС и национални планове за сътрудничество за МИС, посочени в член 5, в рамките на приложното поле на настоящата директива;

д) съвместно обсъждат и оценяват по искане на някоя от държавите членки или на Комисията ефективността на CERT, по-специално когато на равнище Съюза се провеждат учения за МИС;

е) си сътрудничат и обменят информация по всички имащи отношение въпроси с Европейския център по киберпрестъпността към Европол и с всички останали имащи отношение европейски органи, по-специално в сферата на защитата на данни, енергетиката, транспорта, банковото дело, фондовите борси и здравеопазването;

ж) обменят информация и най-добри практики помежду си и с Комисията и се подпомагат взаимно при изграждането на капацитет за МИС;

з) организират редовно партньорски проверки на капацитета и готовността;

и) организират учения за МИС на равнище Съюза и участват, когато това е целесъобразно, в международни учения за МИС.

4. Чрез актове за изпълнение Комисията определя необходимата уредба, с която да улесни сътрудничеството между компетентните органи и Комисията, посочено в параграфи 2 и 3. Тези актове за изпълнение се приемат в съответствие с процедурата по консултиране, посочена в член 19, параграф 2.

Член 9

Сигурна система за обмен на информация

1. Обменът на чувствителна и поверителна информация в рамките на мрежата за сътрудничество се осъществява с помощта на сигурна инфраструктура.

2. Комисията е оправомощена да приема делегирани актове в съответствие с член 18 за определяне на критериите, които една държава членка трябва да изпълни, за да получи разрешение да участва в сигурната система за обмен на информация по отношение на:

а) наличието на сигурна и устойчива комуникационна и информационна инфраструктура на национално равнище, която има обща и оперативна съвместимост със сигурната система за обмен на информация, посочена в член 7, параграф 3, и

б) наличието на достатъчно технически, финансови и човешки ресурси и адекватни процедури за нейните компетентни органи и CERT, които да дават възможност за ефективно, ефикасно и сигурно участие в сигурната система за обмен на информация по член 6, параграф 3, член 7, параграф 2 и член 7, параграф 3.

3. Чрез актове за изпълнение Комисията приема решения относно достъпа на държавите членки до сигурната инфраструктура в съответствие с критериите, посочени в параграфи 2 и 3. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 19, параграф 3.

Член 10

Ранни предупреждения

1. Компетентните органи или Комисията изпращат ранни предупреждения в мрежата за сътрудничество относно онези рискове и инциденти, които отговорят поне на едно от следните условия:

   а) мащабът им се увеличава бързо или може да се увеличи бързо;

   б) превишават или може да превишат националния капацитет за отговор;

   в) засягат или може да засегнат повече от една държава членка.

2. В ранните предупреждения компетентните органи и Комисията съобщават всякаква имаща отношение информация, с която разполагат и която може да бъде от полза за оценката на риска или инцидента.

3. По искане на държава членка или по собствена инициатива Комисията може да поиска една държава членка да предостави всякаква имаща отношение информация по конкретен риск или инцидент.

4. Когато рискът или инцидентът, за който е изпратено ранно предупреждение, е с предполагаем престъпен характер, компетентните органи или Комисията уведомяват Европейския център по киберпрестъпността към Европол.

5. Комисията е оправомощена да приема делегирани актове в съответствие с член 18 за допълнително специфициране на рисковете и инцидентите, които са причина за изпращане на ранното предупреждение, посочено в параграф 1.

Член 11

Координиран отговор

1. След постъпването на ранното предупреждение, посочено в член 10, компетентните органи, след като направят оценка на имащата отношение информация, се споразумяват за координиран отговор в съответствие с плана на Съюза за сътрудничество за МИС, посочен в член 12.

2. Различните мерки, приети на национално равнище вследствие на координирания отговор, се съобщават на мрежата за сътрудничество.

Член 12

План на Съюза за сътрудничество за МИС

1. Комисията е оправомощена чрез делегирани актове да приема план на Съюза за сътрудничество за МИС. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 19, параграф 3.

2. В плана на Съюза за сътрудничество за МИС се предвиждат:

   а) за целите на член 10:

      – определение на формата и процедурата за събиране и обмен на съвместима и съпоставима информация относно рискове и инциденти от страна на компетентните органи;

      – определяне на процедурите и критериите за оценка на рисковете и инцидентите от страна на мрежата за сътрудничество;

   б) процедурата, която следва координираният отговор съгласно член 11, включително определяне на ролите и отговорностите и на процедурите за сътрудничество;

   в) пътна карта за учения и обучения във връзка с МИС с цел подсилване, валидиране и тестване на плана;

   г) програма за трансфер на знания между държавите членки във връзка с изграждането на капацитетите и ученето от партньорите;

   д) програма за повишаване на осведомеността и за обучение между държавите членки.

3. Планът на Съюза за МИС се приема не по-късно от една година след влизането в сила на настоящата директива и се преразглежда редовно.

Член 13

Международно сътрудничество

Без да се засяга възможността мрежата за сътрудничество да провежда неофициално международно сътрудничество, Съюзът може да сключва международни споразумения с трети държави или международни организации, които да дават възможност за участие в някои от дейностите на мрежата за сътрудничество и да ги организират. Подобни споразумения отчитат необходимостта да се гарантира надеждна защита на личните данни, които са в обращение в мрежата за сътрудничество.

ГЛАВА IV

СИГУРНОСТ НА МРЕЖИТЕ И ИНФОРМАЦИОННИТЕ СИСТЕМИ НА ПУБЛИЧНИТЕ АДМИНИСТРАЦИИ И НА УЧАСТНИЦИТЕ НА ПАЗАРА

Член 14

Изисквания за сигурност и уведомяване за инциденти

1. Държавите членки гарантират, че публичните администрации и участниците на пазара предприемат подходящи технически и организационни мерки за управление на рисковете, пред които е изправена сигурността на мрежите и информационните системи, които контролират и използват като част от дейността си. Тези мерки гарантират ниво на сигурност, съответстващо на съществуващия риск с оглед на последните постижения в тази сфера. Предприемат се по-специално мерки с цел предотвратяване и намаляване до минимум на отражението на инциденти, засягащи техните мрежи и информационни системи, върху основните услуги, които те предоставят, и по този начин за гарантиране на непрекъснатостта на услугите, които се поддържат от тези мрежи и информационни системи.

2. Държавите членки гарантират, че публичните администрации и участниците на пазара уведомяват компетентния орган за инцидентите, които са имали значително отражение върху сигурността на основните предоставяни от тях услуги.

3. Изискванията съгласно параграфи 1 и 2 се прилагат за всички участници на пазара, които предоставят услуги в Европейския съюз.

4. Компетентният орган може да информира обществеността или да изиска това да бъде направено от публичните администрации и участниците на пазара, в случай че прецени, че разкриването на инцидента е в интерес на обществото. Веднъж годишно компетентният орган предава обобщен доклад до мрежата за сътрудничество относно получените уведомления и предприетите действия в съответствие с настоящия параграф.

5. Комисията е оправомощена да приема делегирани актове в съответствие с член 18 относно определянето на обстоятелства, при които се изисква публичните администрации и участниците на пазара да информират за настъпилите инциденти.

6. В съответствие с евентуално приетите съгласно параграф 5 делегирани актове компетентните органи могат да приемат насоки и, когато е необходимо, да издават указания относно обстоятелствата, при които се изисква публичните администрации и участниците на пазара да информират за настъпилите инциденти.

7. Комисията е оправомощена чрез делегирани актове да определя форматите и процедурите, приложими за целите на параграф 2. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 19, параграф 3.

8. Параграфи 1 и 2 не се прилагат за микропредприятия, съгласно определението от Препоръка 2003/361/ЕО на Комисията от 6 май 2003 г. относно определението за микро-, малки и средни предприятия[12].

[12] ОВ L 124, 20.5.2003 г., стр. 36.

Член 15

Изпълнение и правоприлагане

1. Държавите членки гарантират, че компетентните органи получават всички необходими правомощия, за да разследват случаите на неизпълнение от страна на публичните администрации и участниците на пазара на техните задължения съгласно член 14 и на последиците от тях за сигурността на мрежовите и информационните системи.

2. Държавите членки гарантират, че компетентните органи разполагат с правомощието да изискват от публичните администрации и участниците на пазара да:

   а) предоставят информацията, необходима за оценка на сигурността на техните мрежови и информационни системи, включително документирани политики за сигурност;

   б) да преминават одит на сигурността, извършван от квалифицирана независима организация или национален орган, и да предоставят резултатите от него на компетентния орган.

3. Държавите членки гарантират, че компетентните органи разполагат с правомощието да издават задължителни инструкции за участниците на пазара и публичните администрации.

4. Компетентните органи уведомяват правоприлагащите органи за инцидентите от предполагаемо сериозно престъпно естество.

5. Компетентните органи работят в тясно сътрудничество с органите за защита на личните данни по инцидентите, които водят до нарушаване на сигурността на лични данни.

6. Държавите членки гарантират, че всички задължения, наложени на публичните администрации и участниците на пазара, могат да бъдат обект на съдебен контрол.

Член 16

Стандартизация

1. С цел да гарантират последователно прилагане на член 14, параграф 1 държавите членки насърчават използването на стандарти и/или спецификации, касаещи мрежовата и информационната сигурност.

2. Комисията изготвя чрез актове за изпълнение списък на стандартите, посочени в параграф 1. Списъкът се публикува в Официален вестник на Европейския съюз.

ГЛАВА V

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 17

Санкции

1. Държавите членки определят правила относно санкциите в случаи на нарушения на националните разпоредби, приети съгласно настоящата директива, и предприемат всички необходими мерки, за да гарантират тяхното изпълнение. Предвидените санкции трябва да бъдат ефикасни, съразмерни и възпиращи. Държавите членки нотифицират тези разпоредби на Комисията не по-късно от датата на транспониране на настоящата директива и нотифицират без забавяне всякакви последващи изменения, които засягат тези разпоредби.

2. Държавите членки гарантират, че в случаите когато инцидент засяга лични данни, предвидените санкции са съгласувани със санкциите, предвидени в Регламента на Европейския парламент и на Съвета относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни[13].

Член 18

Упражняване на делегирането

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

2. Правомощието да приема делегирани актове, посочено в член 9, параграф 2, член 10, параграф 5 и член 14, параграф 5 се предоставя на Комисията. Комисията изготвя доклад относно делегирането на правомощия не по-късно от девет месеца преди изтичането на петгодишния срок. Делегирането на правомощия се продължава мълчаливо за срокове с еднаква продължителност, освен ако Европейският парламент или Съветът не възразят срещу подобно продължаване не по-късно от три месеца преди изтичането на всеки срок.

3. Делегирането на правомощия, посочено в член 9, параграф 2, член 10, параграф 5 и член 14, параграф 5, може да бъде оттеглено по всяко време от Европейския парламент или от Съвета. С решението за оттегляне се прекратява посоченото в него делегиране на правомощия. То поражда действие в деня след публикуването на решението в *Официален вестник на Европейския съюз* или на по-късна, посочена в решението дата. То не засяга действителността на делегираните актове, които вече са в сила.

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

5. Делегиран акт, приет съгласно член 9, параграф 2, член 10, параграф 5 и член 14, параграф 5, влиза в сила единствено ако нито Европейският парламент, нито Съветът не са представили възражения в срок от два месеца след нотифицирането на акта на Европейския парламент и Съвета или ако преди изтичането на този срок и Европейският парламент, и Съветът са уведомили

[13] SEC(2012) 72 final.

Комисията, че няма да представят възражения. Този срок се удължава с два месеца по инициатива на Европейския парламент или на Съвета.

Член 19

Процедура на комитет

1. Комисията се подпомага от комитет (Комитет по мрежова и информационна сигурност). Посоченият комитет е комитет по смисъла на Регламент (ЕС) № 182/2011.

2. При позоваване на настоящия параграф се прилага член 4 от Регламент (ЕС) № 182/2011.

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

Член 20

Преразглеждане

Комисията периодично преразглежда действието на настоящата директива и докладва на Европейския парламент и Съвета. Първият доклад се предава не по-късно от три години след датата на транспониране, посочена в член 21. За тази цел Комисията може да поиска от държавите членки да предоставят информация без неоправдано забавяне.

Член 21

Транспониране

1. Държавите членки въвеждат в сила законовите, подзаконовите и административните разпоредби, необходими, за да се съобразят с настоящата директива не по-късно от [една година и половина след приемането] г. Те незабавно съобщават на Комисията текста на тези разпоредби.

   Те прилагат тези разпоредби от [една година и половина след приемането] г.

   Когато държавите членки приемат тези разпоредби, в тях се съдържа позоваване на настоящата директива или то се извършва при официалното им публикуване. Условията и редът на позоваване се определят от държавите членки.

2. Държавите членки съобщават на Комисията текста на основните разпоредби от националното законодателство, които те приемат в областта, уредена с настоящата директива.

Член 22

Влизане в сила

Настоящата директива влиза в сила на [двадесетия] ден след публикуването ѝ в *Официален вестник на Европейския съюз*.

Член 23

Адресати

Адресати на настоящата директива са държавите членки.

Съставено в Брюксел на […] година.

За Европейския парламент	*За Съвета*
Председател	*Председател*

ПРИЛОЖЕНИЕ I

Изисквания и задачи на екипите за незабавно реагиране при компютърни инциденти (CERT)

Изискванията към CERT и техните задачи се определят по подходящ начин и ясно, като в тяхна подкрепа има национални политики и/или законодателство. Те включват следните елементи:

(1) Изисквания към CERT

а) CERT гарантират много добра наличност на своите комуникационни услуги, като не допускат съществуването на точки, повредата в които може да доведе до общ срив, и разполагат с няколко канала, по които могат да установяват връзка и да бъдат търсени. Комуникационните канали трябва да бъдат също така ясно посочени и добре известни на заинтересованите страни и на партньорите от сътрудничеството.

б) CERT изпълняват и управляват мерки за сигурност, с които да гарантират поверителността, целостта, наличността и автентичността на информацията, която получават и с която работят.

в) Офисите на CERT и поддържащите дейността на CERT информационни системи се разполагат в помещения с гарантирана сигурност.

г) Създава се система за качествено управление на услугите с цел проследяване представянето на CERT и гарантиране на траен процес на усъвършенстване. Тя се основава на ясно определени параметри, които включват формалните равнища на услугите и основни показатели на представянето.

д) Непрекъснатост на дейността

- CERT разполага с подходяща система за управление и разпределяне на заявките с цел да улесни предаването на задачите от един на друг изпълнител,
- CERT разполага с достатъчен персонал, който да гарантира, че CERT е постоянно на разположение,
- CERT разчита на инфраструктура с гарантирана непрекъснатост на дейността. За тази цел за CERT се създават резервирани системи и резервно работно пространство, чрез които да се гарантира постоянен достъп до комуникационните средства.

(2) Задачи на CERT

а) Задачите на CERT включват поне следните елементи:

- Следене на инцидентите на национално равнище,

– Осигуряване на ранни предупреждения, сигнали за тревога, съобщения и разпространяване на информация за инциденти и рискове сред съответните заинтересовани страни,

– Отговор на инциденти,

– Осигуряване на динамичен анализ на рисковете и инцидентите и информация за текущата ситуация,

– Постигане на мащабна обществена осведоменост за рисковете, свързани с онлайн дейностите,

– Организиране на кампании за МИС.

б) CERT изграждат отношения на сътрудничество с частния сектор.

в) С цел улесняване на сътрудничеството CERT насърчава възприемането и използването на общи практики за стандартизация за:

– процедури за действия при инциденти и рискове,

– системи за класификация на инциденти, рискове и информация,

– таксономии на параметрите,

– формати за обмен на информация за рискове и инциденти и договореност за системно именуване.

ПРИЛОЖЕНИЕ II

Списък на участниците на пазара

Посочени в член 3, параграф 8, буква а):

1. Платформи за електронна търговия

2. Портали за плащания в интернет

3. Социални мрежи

4. Машини за търсене

5. Услуги за изчисления в облак

6. Магазини за приложни програми

Посочени в член 3, параграф 8, буква б):

1. Енергетика

- доставчици на електроенергия и природен газ
- оператори на системи за електро- и газоразпределение и търговци на дребно, работещи с крайните потребители
- оператори на газопреносни мрежи, оператори на хранилища, оператори на системи за съхранение и за ВПГ
- оператори на преносни мрежи за електроенергия
- нефтопроводи и нефтохранилища
- участници на пазара на електроенергия и природен газ
- оператори на съоръжения за добив, рафиниране и преработка на нефт и природен газ

2. Транспорт

- въздушни превозвачи (товарен и пътнически въздушен транспорт)
- морски превозвачи (компании за морски и крайбрежен воден транспорт на пътници и компании за морски и крайбрежен воден транспорт на товари)
- железопътен транспорт (управители на инфраструктура, интегрирани дружества и железопътни транспортни оператори)
- летища
- пристанища

– операторите ръководство на движението

– спомагателни логистични услуги (а) складове и съхранение, б) обработка на товари и в) други транспортни подпомагащи услуги)

3. Банково дело: кредитни институции в съответствие с член 4, точка 1 от Директива 2006/48/ЕО.

4. Инфраструктури на финансовия пазар: фондови борси и централни контрагенти клирингови къщи

5. Сектор на здравеопазването: здравни заведения (включително болници и частни клиники) и други субекти, участващи в предоставянето на здравни услуги.

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1. Наименование на предложението/инициативата

1.2. Съответни области на политиката в структурата на УД/БД

1.3. Естество на предложението/инициативата

1.4. Цели

1.5. Мотиви за предложението/инициативата

1.6. Срок на действие и финансово отражение

1.7. Предвидени методи на управление

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

2.2. Система за управление и контрол

2.3. Мерки за предотвратяване на измами и нередности

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

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

3.2. Очаквано отражение върху разходите

3.2.1. Обобщение на очакваното отражение върху разходите

3.2.2. Очаквано отражение върху бюджетните кредити за оперативни разходи

3.2.3. Очаквано отражение върху бюджетните кредити за административни разходи

3.2.4. Съвместимост с настоящата многогодишна финансова рамка

3.2.5. Участие на трети страни във финансирането

3.3. Очаквано отражение върху приходите

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1. Наименование на предложението/инициативата

Предложение за директива на Европейския парламент и на Съвета относно мерки за гарантиране на високо ниво на мрежова и информационна сигурност в Съюза

1.2. Съответна област на политиката в структурата на УД/БД[37]

- 09 – Съобщителни мрежи, съдържание и технологии

1.3. Естество на предложението/инициативата

☒ Предложението/инициативата е във връзка с **нова дейност**

☐ Предложението/инициативата е във връзка с **нова дейност след пилотен проект/подготвителна дейност**[38]

☐ Предложението/инициативата е във връзка с **продължаване на съществуваща дейност**

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

1.4. Цели

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

Целта на предлаганата директива е да гарантира високо общо ниво на мрежова и информационна сигурност (МИС) в целия ЕС.

1.4.2. Конкретни цели и съответни дейности във връзка с УД/БД

В предложението се определят мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза.

Конкретните цели са:

1. Да се въведе минимално ниво на МИС в държавите членки и по този начин да се повиши общото ниво на подготвеност и реагиране.

2. Да се подобри сътрудничеството относно МИС на равнище ЕС с цел да се противодейства ефективно на трансгранични инциденти и заплахи. Ще бъде създадена сигурна инфраструктура за обмен на информация, която да дава възможност за предаване на чувствителна и поверителна информация между компетентните органи**.**

3. Да се създаде култура на управление на риска и да се подобри обменът на информация между частния и публичния сектор.

[37] УД: управление по дейности; БД: бюджетиране по дейности.

[38] Съгласно член 49, параграф 6, буква а) или б) от Финансовия регламент.

Съответни дейности във връзка с УД/БД

Директивата обхваща субекти (дружества и организации, включително някои МСП) и публични администрации в редица сектори (енергетика, транспорт, кредитни институции и фондови борси, здравеопазване, субекти с фундаментална роля за ключовите интернет услуги). В нея за застъпени връзките с правоприлагащите органи и органите за защита на данните и аспектите на външните отношения, свързани с МИС.

- 09 – Съобщителни мрежи, съдържание и технологии

- 02 - Предприемачество

- 32 - Енергетика

- 06 – Мобилност и транспорт

- 17 – Здравеопазване и защита на потребителите

- 18 – Вътрешни работи

- 19 – Външни отношения

- 33 - Правосъдие

- 12- Вътрешен пазар

1.4.3. Очаквани резултати и отражение

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

Защитата на потребителите, предприятията и сектора на държавното управление в ЕС срещу инциденти, заплахи и рискове, свързани с МИС, ще се подобри значително.

Повече подробности са дадени в точка 8.2 (Въздействие на вариант 2 — регулаторен подход) от работния документ на службите на Комисията — Оценка на въздействието, който придружава настоящото законодателно предложение.

1.4.4. Показатели за резултатите и за отражението

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

Показателите за мониторинг и оценка могат да бъдат намерени в точка 10 от оценката на въздействието.

1.5. Мотиви за предложението/инициативата

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

От всяка държава членка ще се изисква да разполага със:

- национална стратегия за МИС;

- план за сътрудничество за МИС;

- национален компетентен орган за МИС;

- екип за незабавно реагиране при компютърни инциденти (CERT).

На равнище ЕС от държавите членки ще се изисква да си сътрудничат в мрежа.

От публичните администрации и основните частни участници ще се изисква да провеждат управление на риска за МИС и да докладват на компетентните органи инцидентите в МИС, които имат значителни последици.

1.5.2. Добавена стойност от намесата на ЕС

Като се има предвид трансграничния характер на МИС, разликите в съответното законодателство и политики представляват бариера пред дружествата, които желаят да работят в няколко държави, и пред постигането на общи икономии от мащаба. Отсъствието на интервенция на равнище ЕС би довело до ситуация, при която всяка държава членка действа самостоятелно, като не се съобразява с взаимозависимостта на мрежовите и информационните системи в ЕС.

Обявените цели могат следователно да бъдат постигнати по-успешно на равнище ЕС, отколкото от държавите членки самостоятелно.

1.5.3. Изводи от подобен опит в миналото

Настоящото предложение произтича от анализа, че са необходими законово регламентирани задължения, за да бъдат осигурени еднакви условия и да бъдат затворени част от „вратичките“ в законодателството. Изцяло доброволният подход в тази сфера доведе до сътрудничество, част от което са само държави членки с високо ниво на капацитета, а те са малцинство.

1.5.4. Съгласуваност и евентуална синергия с други актове

Предложението съответства изцяло на Програмата в областта на цифровите технологии за Европа, а оттам и на стратегията „Европа 2020“. То е в синхрон с регулаторната рамка на ЕС относно електронните съобщения, Директивата на ЕС относно европейските критични инфраструктури и Директивата на ЕС относно защитата на личните данни и ги допълва.

Настоящото предложение придружава съобщението на Комисията и на върховния представител на Съюза по въпросите на външните работи и политиката на сигурност относно европейска стратегия за киберсигурност и е основна част от него.

1.6. Срок на действие и финансово отражение

– ☐ Предложение/инициатива с ограничен срок на действие

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

– ☐ Финансово отражение от ГГГГ до ГГГГ

– ☒ Предложение/инициатива с неограничен срок на действие

– Периодът на транспониране ще започне веднага след приемането (очаквано през 2015 г.) и ще продължи 18 месеца. Изпълнението на директивата обаче ще започне след приемането ѝ и ще доведе до изграждането на сигурната инфраструктура в подкрепа на сътрудничеството между държавите членки.

– което ще бъде последвано от функциониране с пълен капацитет.

1.7. Предвидени методи на управление[39]

– ☒ Пряко централизирано управление от Комисията

– ☒ Непряко централизирано управление чрез делегиране на задачи по изпълнението на:

– ☐изпълнителни агенции

– ☒ органи, създадени от Общностите[40]

– ☐ национални органи от публичния сектор/организации, предоставящи обществени услуги

– ☐ 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

– ☐ Споделено управление с държавите членки

– ☐ Децентрализирано управление с трети държави

– ☐ Съвместно управление с международни организации, включително Европейската космическа агенция

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

Забележки:

ENISA, децентрализираната агенция, създадена от Общностите, може да оказва съдействие на държавите членки и Комисията при изпълнението на директивата на

[39] Подробности във връзка с методите на управление и позоваванията на Финансовия регламент могат да бъдат намерени на уебсайта BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.htmlhttp://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[40] Посочени в член 185 от Финансовия регламент.

основание мандата си и като преразпределя ресурси, предвидени за агенцията по МФР 2014-2020 г.

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

Да се посочат честотата и условията.

Комисията периодично ще преразглежда действието на настоящата директива и ще докладва на Европейския парламент и Съвета.

Комисията ще направи също така оценка на правилното транспониране на директивата от държавите членки.

В предложението за МСЕ е предвидена възможността също така да бъде извършена оценка на методите за изпълнение на проекти, както и на ефекта от тяхното изпълнение с цел оценка доколко са постигнати целите, включително отнасящите се до опазването на околната среда.

2.2. Система за управление и контрол

2.2.1. Установени рискове

- закъснение в изпълнението на проектите за изграждането на сигурната инфраструктура

2.2.2. Предвидени методи на контрол

В споразуменията и решенията за изпълнение на действията по МСЕ се предвижда надзор и финансов контрол от страна на Комисията или на нейни упълномощени представители, както и одити от страна на Сметната палата и проверки на място от страна на Службата за борба с измамите (OLAF).

2.2.3. Разходи за контрола и ползи от него и вероятен процент на нарушенията

Предварителните и последващите проверки въз основа на равнището на риск и възможността за одити на място ще гарантират разумни разходи за контрол.

2.3. Мерки за предотвратяване на измами и нередности

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

Комисията предприема подходящи мерки, за да гарантира, че при изпълнението на действието, финансирано съгласно настоящата директива, финансовите интереси на Съюза се опазват посредством прилагането на превантивни мерки срещу измами, корупция и всякакви други незаконни дейности и като част от тези мерки се извършват ефективни проверки, а при откриване на нередности, възстановяване на неправомерно изплатените суми и, когато е необходимо, налагане на ефективни, съразмерни и възпиращи санкции.

Комисията или нейни представители и Сметната палата имат правомощия за извършване на одити по документи и на място на всички бенефициери на

безвъзмездни средства, изпълнители и подизпълнители, които са получили средства от Съюза по силата на настоящата програма.

Европейската служба за борба с измамите (OLAF) може да извършва проверки и инспекции на място по отношение на икономически оператори, засегнати пряко или непряко от такова финансиране, в съответствие с процедурите, предвидени в Регламент (Евратом, ЕО) № 2185/96, с оглед установяване дали е налице измама, корупция или каквато и да било друга незаконна дейност, накърняваща финансовите интереси на Съюза във връзка със споразумение или решение за отпускане на безвъзмездни средства или договор за финансиране от страна на Съюза.

Без да се засягат разпоредбите на предходните параграфи, в споразуменията за сътрудничество с трети държави и международни организации, в споразуменията и решенията за отпускане на безвъзмездни средства и в договорите, произтичащи от прилагането на настоящия регламент, се предвижда изрично оправомощаване на Комисията, Сметната палата и OLAF да провеждат такива одити, проверки и инспекции на място.

В МСЕ е предвидено договорите за обществени поръчки и споразуменията за отпускане на безвъзмездни средства да се изготвят по стандартни образци, в които са определени общоприложимите мерки за борба с измамите.

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

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

- Съществуващи бюджетни редове

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

Функция от многогодишната финансова рамка	Бюджетен ред	Вид на разхода	Вноска			
	Номер [Наименование……...……]	Многогод./ едногод.[41]	от държави от ЕАСТ[42]	от държави кандидатки[43]	от трети държави	по смисъла на член 18, параграф 1, буква аа) от Финансовия регламент
	09 03 02 Насърчаване на взаимосвързаността и оперативната съвместимост на националните публични услуги онлайн, както и на достъпа до тези мрежи	Многогод.	НЕ	НЕ	НЕ	НЕ

- Поискани нови бюджетни редове (неприложимо)

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

Функция от многогодишната финансова рамка	Бюджетен ред	Вид на разхода	Вноска			
	Номер [Наименование……...……]	Многогод./ едногод.	от държави от ЕАСТ	от държави кандидатки	от трети държави	по смисъла на член 18, параграф 1, буква аа) от Финансовия регламент
	[XX.YY.YY.YY]		ДА/НЕ	ДА/НЕ	ДА/НЕ	ДА/НЕ

41 Многогод. = многогодишни бюджетни кредити / Едногод. = едногодишни бюджетни кредити.

42 ЕАСТ: Европейска асоциация за свободна търговия.

43 Държави кандидатки и, ако е приложимо, държави потенциални кандидатки от Западните Балкани.

3.2. Очаквано отражение върху разходите

3.2.1. Обобщение на очакваното отражение върху разходите

млн. евро (до третия знак след десетичната запетая)

Функция от многогодишната финансова рамка:	1	Интелигентен и приобщаващ растеж

ГД: <…….>			2015 г. *[44]	2016 г.	2017 г.	2018 г.	Следващи години (2019-2021)и след това			**ОБЩО**
• Бюджетни кредити за оперативни разходи										
09 03 02	Поети задължения	(1)	1,250**	0,000						**1,250**
	Плащания	(2)	0,750	0,250	0,250					**1,250**
Бюджетни кредити за административни разходи, финансирани от пакета за определени програми[45]			**0,000**							**0,000**
Номер на бюджетния ред		(3)	**0,000**							**0,000**
ОБЩО бюджетни кредити за ГД <…….>	Поети задължения	=1+1a +3	1,250	0,000						**1,250**
	Плащания	=2+2a +3	0,750	0,250	0,250					**1,250**

[44] Година N е годината, през която започва да се осъществява предложението/инициативата.

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

• ОБЩО бюджетни кредити за оперативни разходи	Поети задължения	(4)	1,250	0,000						**1,250**
	Плащания	(5)	0,750	0,250	0,250					**1,250**
• ОБЩО бюджетни кредити за административни разходи, финансирани от пакета за определени програми		(6)	**0,000**							
БЩО бюджетни кредити по ФУНКЦИЯ 1 от многогодишната финансова рамка	Поети задължения	=4+ 6	1,250	0,000						**1,250**
	Плащания	=5+ 6	0,750	0,250	0,250					**1,250**

* Точният момент ще зависи от датата, на която бъде прието предложението от законодателния орган (т.е., ако директивата бъде одобрена през 2014 г., адаптирането на съществуващата инфраструктура ще започне през 2015 г., а в противен случай — една година по-късно).

** Ако държавите членки предпочетат да използват съществуващата инфраструктура и да покрият еднократните разходи за адаптацията ѝ от бюджета на ЕС, както е обяснено в точки 1.4.3 и 1.7, се очаква, че разходите за приспособяването на мрежата, за да поддържа сътрудничеството между държавите членки съгласно глава III от директивата (ранни предупреждения, координиран отговор и др.) ще възлязат на 1 250 000 EUR. Тази сума е малко по-висока от посочената в оценката на въздействието („приблизително 1 млн. евро“), тъй като се базира на по-точна оценка на необходимите компоненти на подобна инфраструктура. Необходимите компоненти и разходите за тях са на база оценка на JRC, произтичаща от неговия опит в разработването на сходни системи за други сфери, например публично здраве, и включват: система за бързо предупреждение и уведомяване за МИС (275 000 EUR); платформа за обмен на информация (400 000 EUR); система за ранно предупреждение и отговор (275 000 EUR); ситуационен център (300 000 EUR) — или общо 1 250 000 EUR. По-подробен план за изпълнение ще бъде представен в проучването за осъществимост, които предстои да бъде проведено в рамките на договор SMART 2012/0010: „Проучване за осъществимост и подготвителни действия за изпълнението на европейска система за ранно предупреждение и отговор на кибератаки и нарушения на функционалността“.

Ако предложението/инициативата има отражение върху повече от една функция:

• ОБЩО бюджетни кредити за оперативни разходи	Поети задължения	(4)	0,000	0,000						
	Плащания	(5)	0,000	0,000						
• ОБЩО бюджетни кредити за административни разходи, финансирани от пакета за определени програми		(6)	**0,000**	**0,000**						

БЩО бюджетни кредити по ФУНКЦИИ 1—4 от многогодишната финансова рамка (Референтна стойност)	Поети задължения	=4+ 6	1,250	0,000						1,250
	Плащания	=5+ 6	0,750	0,250	0,250					1,250

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

млн. евро (до третия знак след десетичната запетая)

		2015 г.	**2016 г.**	**2017 г.**	**2018 г.**	Следващи години (2019-2021)и след това			**ОБЩО**
ГД: CNECT									
• Човешки ресурси		0,572	0,572	0,572	0,572	0,572	0,572	**0,572**	**4,004**
• Други административни разходи		0,318	0,118	0,318	0,118	0,318	0,118	**0,118**	**1,426**
ОБЩО за ГД CNECT	Бюджетни кредити	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

БЩО бюджетни кредити по ФУНКЦИЯ 5 от многогодишната финансова рамка	(Общо поети задължения = общо плащания)	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

млн. евро (до третия знак след десетичната запетая)

		2015 г.[46]	**2016 г.**	**2017 г.**	**2018 г.**	Следващи години (2019-2021)и след това			**ОБЩО**
БЩО бюджетни кредити по ФУНКЦИЯ 5 от многогодишната финансова рамка	Поети задължения	2,140	0,690	0,890	0,690	0,890	0,690	0,690	**6,680**
	Плащания	1,640	0,940	1,140	0,690	0,890	0,690	0,690	**6,680**

[46] Година N е годината, през която започва да се осъществява предложението/инициативата.

3.2.2. Очаквано отражение върху бюджетните кредити за оперативни разходи

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

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

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

Да се посочат целите и резултатите ⇩			**2015 г. ***		**2016 г.**		**2017 г.**		**2018 г.**		Следващи години (2019-2021)и след това						**ОБЩО**	
	РЕЗУЛТАТИ																	
	Вид[47]	Среден разход	Брой	Разходи	Брой	Разходи	Брой	Разходи	Брой	Разходи	Брой	Разходи	Брой	Разходи	Брой	Разходи	Общ брой	Общо разходи
КОНКРЕТНА ЦЕЛ № 2[48] Сигурна система за обмен на информация																		
- Резултат	Адаптиране на инфра																	
Междинен сбор за конкретна цел № 2…			1	1,250**													1	1,250
ОБЩО РАЗХОДИ				1,250														1,250

47 Резултатите са продуктите и услугите, които ще бъдат доставени (напр. брой финансирани обмени на учащи се, дължина на построените пътища в километри и т.н.).

48 Съгласно описанието в част 1.4.2. „Конкретни цели…“.

* Точният момент ще зависи от датата, на която бъде прието предложението от законодателния орган (т.е., ако директивата бъде одобрена през 2014 г., адаптирането на съществуващата инфраструктура ще започне през 2015 г., а в противен случай — една година по-късно).

** Вж. точка 3.2.1.

3.2.3. Очаквано отражение върху бюджетните кредити за административни разходи

3.2.3.1. Обобщение

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

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

млн. евро (до третия знак след десетичната запетая)

	2015 г.[49]	**2016 г.**	**2017 г.**	**2018 г.**	Следващи години (2019-2021)и след това			**ОБЩО**
ФУНКЦИЯ 5 от многогодишната финансова рамка								
Човешки ресурси	0,572	0,572	0,572	0,572	0,572	0,572	0,572	**4,004**
Други административни разходи	0,318	0,118	0,318	0,118	0,318	0,118	0,118	**1,426**
Междинен сбор за ФУНКЦИЯ 5 от многогодишната финансова рамка	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
Извън ФУНКЦИЯ 5[50] **от многогодишната финансова рамка**								
Човешки ресурси	0,000	0,000						**0,000**
Други разходи с административен характер								
Междинен сбор извън ФУНКЦИЯ 5 от многогодишната финансова рамка	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
ОБЩО	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

[49] Година N е годината, през която започва да се осъществява предложението/инициативата.

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

Необходимите бюджетни кредити ще бъдат покрити от бюджетни кредити на ГД CNECT, които вече са предвидени за управлението на дейността и/или които са преразпределени в рамките на генералната дирекция, при необходимост заедно с всички допълнителни отпуснати ресурси, които могат да бъдат предоставени на управляващата генералната дирекция в рамките на годишната процедура за отпускане на средства и като се имат предвид бюджетните ограничения.

Европейската агенция за мрежова и информационна сигурност (ENISA) може да оказва съдействие на държавите членки и Комисията при изпълнението на директивата на основание мандата си и като преразпределя ресурси, предвидени за нея по МФР 2014-2020 г., т.е. без допълнителни бюджетни средства или заделени човешки ресурси.

3.2.3.2. Очаквани нужди от човешки ресурси

– ☐ Предложението/инициативата не налага използване на човешки ресурси

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

По принцип няма да бъдат необходими допълнителни човешки ресурси. Ще бъдат необходими много ограничени човешки ресурси, които ще бъдат набрани от персонал на генералната дирекция, който вече е разпределен за управлението на това действие.

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

		2015 г.	2016 г.	2017 г.	2018 г.	Следващи години (2019-2021)и след това		
• Длъжности в щатното разписание (длъжностни лица и временно наети лица)								
09 01 01 01 (Централа и представителства на Комисията)		4	4	4	4	4	4	4
XX 01 01 02 (Делегации)								
XX 01 05 01 (Непреки научни изследвания)								
10 01 05 01 (Преки научни изследвания)								
• Външен персонал (в еквивалент на пълно работно време — ЕПРВ)[51]								
09 01 02 01 (ДНП, ПНА, КНЕ от общия финансов пакет)		1	1	1	1	1	1	1
XX 01 02 02 (ДНП, ПНА, МЕД, МП и КНЕ в делегациите)								
XX 01 04 yy[52]	- в централата[53]							
	- в делегациите							
XX 01 05 02 (ДНП, ПНА, КНЕ — Непреки научни изследвания)								
10 01 05 02 (ДНП, ПНА, КНЕ — Преки научни изследвания)								
Други бюджетни редове (да се посочат)								

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

[52] Под тавана за външния персонал от бюджетните кредити за оперативни разходи (предишни редове „ВА“).

[53] Основно за структурните фондове, Европейския земеделски фонд за развитие на селските райони (ЕЗФРСР) и Европейския фонд за рибарство (ЕФР).

ОБЩО	**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX е съответната област на политиката или бюджетен дял.

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

Европейската агенция за мрежова и информационна сигурност (ENISA) може да оказва съдействие на държавите членки и Комисията при изпълнението на директивата на основание сегашния си мандат и като преразпределя ресурси, предвидени за нея по МФР 2014-2020 г., т.е. без допълнителни бюджетни средства или заделени човешки ресурси.

Описание на задачите, които трябва да се изпълнят:

Длъжностни лица и временно нает персонал	- Изготвяне на делегирани актове в съответствие с член 14, параграф 3 - Изготвяне на актове за изпълнение в съответствие с член 8, член 9, параграф 2, член 12, член 14, параграф 5 и член 16 - Принос към сътрудничеството чрез мрежата както на политическо, така и на оперативно ниво - Участие в международни преговори и в евентуалното сключване на международни споразумения
Външен персонал	Подкрепа според необходимостта за осъществяването на горните задачи

3.2.4. Съвместимост с настоящата многогодишна финансова рамка

– ☑ Предложението/инициативата е съвместимо(а) с настоящата многогодишна финансова рамка.

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

До очакваното финансово въздействие на предложението върху оперативните разходи ще се стигне, ако държавите членки решат да адаптират съществуващата инфраструктура и възложат осъществяването на адаптацията на Комисията в рамките на МФР 2014-2020 г. Свързаните с това еднократни разходи ще бъдат поети по МСЕ, при условие че са налични достатъчно средства. Като алтернатива държавите членки могат да си поделят разходите за адаптирането на инфраструктурата или за изграждането на нова инфраструктура.

– ☐ Предложението/инициативата налага да се използва Инструментът за гъвкавост или да се преразгледа многогодишната финансова рамка.[54]

Неприложимо.

3.2.5. Участие на трети страни във финансирането

– Предложението/инициативата не предвижда съфинансиране от трети страни

3.3. Очаквано отражение върху приходите

– ☑ Предложението/инициативата няма финансово отражение върху приходите.

[54] Вж. точки 19 и 24 от Междуинституционалното споразумение.