



2022/0272(COD)

30.6.2023

СТАНОВИЩЕ

на комисията по вътрешния пазар и защита на потребителите

на вниманието на комисията по промишленост, изследвания и енергетика

относно предложението за регламент на Европейския парламент и на Съвета относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на Регламент (ЕС) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))

Докладчик по становище (*): Мортен Льокегор

(*) Процедура с асоциирана комисия – член 57 от Правилника за дейността

PA_Legam

КРАТКА ОБОСНОВКА

Като бивш докладчик по становище в комисията IMCO относно Директивата за мрежовата и информационна сигурност 2 (МИС 2), докладчикът счита, че Законодателният акт за киберустойчивост е решаваща и естествена следваща стъпка за подобряване на киберсигурността на Европейския съюз. Считайки, че по определение киберсигурността никога няма да бъде стопроцентово осигурена, докладчикът е на мнение, че е важно да направим всичко, което е по силите ни, за да се намали броят на слабите звена в нашия Съюз, и че за тази цел Законодателният акт за киберустойчивост е приветствана следваща стъпка. Трябва да повишим киберсигурността на продуктите с цифрови елементи и други нови продукти, като например устройствата от вида „интернет на нещата“, които са се превърнали в естествена част от ежедневието на европейските потребители и предприятия.

Тъй като комисията IMCO отговаря за функционирането и прилагането на единния пазар, включително цифровия единен пазар, и правилата за защита на потребителите, стремежът на докладчика беше да въведе изменения, които имат за цел да подобрят функционирането на вътрешния пазар, като същевременно осигуряват високо равнище на защита на потребителите в рамките на приложното поле на предложението, по-специално по отношение на изискванията за киберсигурност за продуктите с цифрови елементи.

В допълнение докладчикът счита, че се налага подобряване на някои аспекти на предложения регламент, за да се осигури правна яснота и съгласуваност между относимите разпоредби на предложения регламент и други законодателни актове. Това е свързано по-специално с Директивата за МИС 2, наскоро приетия Регламент относно общата безопасност на продуктите, Регламента за изкуствения интелект и Регламента относно машиностроителните изделия, както и с редица съответни делегирани актове и актове за изпълнение. Поради това докладчикът предложи изменения, които имат за цел да подобрят правната яснота и да спомогнат за осигуряването на съгласувано, ефективно и последователно тълкуване и прилагане на посочените законодателни актове.

Освен това, тъй като микро-, малките и средните предприятия са икономически участници от решаващо значение на цифровия пазар, докладчикът внесе редица изменения с цел опростяване на административните процедури и ограничаване на административната тежест за малките предприятия, без да се понижава равнището на безопасност. Докладчикът въведе също така изменения, които гарантират, че на микропредприятията и МСП ще бъдат предоставени конкретни насоки и съвети за спазване на изискванията на Законодателния акт за киберустойчивост.

И накрая, докладчикът въведе изменения с цел осигуряване на по-ефективна комуникация с компетентните органи (националните органи за надзор на пазара, ENISA), както и засилване на разпоредбите за задълженията и правомощията на съответните органи по отношение на жалбите, инспекциите и съвместните дейности. В допълнение към това някои изменения на докладчика се съсредоточават върху подобряването на изискванията за киберсигурност за компонентите, интегрирани в крайни продукти с цифрови елементи, като се уточняват задълженията на икономическите оператори, като например производителите и упълномощените представители.

Докладчикът отново изразява позицията, че въвеждането на Законодателния акт за киберустойчивост е навременна и естествена следваща стъпка за засилване на борбата срещу заплахите за киберсигурността в нашия Съюз. С предложените изменения докладчикът се стреми да намери правилния баланс между гарантирането на повишено ниво на киберсигурност в полза на европейските потребители и пропорционална тежест за бизнес общността. Амбицията на докладчика е киберсигурността да се превърне в естествен параметър на конкуренцията на вътрешния пазар. С оглед на това докладчикът се стреми да коригира предложението.

ИЗМЕНЕНИЯ

Комисията по вътрешния пазар и защита на потребителите приканва водещата комисия по промишленост, изследвания и енергетика да вземе предвид следните изменения:

Изменение 1

Предложение за регламент Съображение 1

Текст, предложен от Комисията

(1) Необходимо е да се подобри функционирането на вътрешния пазар, като се установи единна правна рамка за съществените изисквания за киберсигурност при пускането на продукти с цифрови елементи на пазара на Съюза. Следва да бъдат решени два основни проблема, които увеличават разходите за ползвателите и обществото: ниското ниво на киберсигурност на продуктите с цифрови елементи, което се изразява в широко разпространени уязвимости и недостатъчно и непоследователно предоставяне на актуализации на защитата за справяне с тях, и недостатъчно разбиране и достъп до информация от страна на ползвателите, което им пречи да избират продукти с подходящи характеристики за киберсигурност или да ги използват по защитен начин.

Изменение

(1) Необходимо е да се подобри функционирането на вътрешния пазар, като **същевременно се предоставя високо равнище на защита на потребителите и киберсигурност**, като се установи единна правна рамка за съществените изисквания за киберсигурност при пускането на продукти с цифрови елементи на пазара на Съюза. Следва да бъдат решени два основни проблема, които увеличават разходите за ползвателите и обществото: ниското ниво на киберсигурност на продуктите с цифрови елементи, което се изразява в широко разпространени уязвимости и недостатъчно и непоследователно предоставяне на актуализации на защитата за справяне с тях, и недостатъчно разбиране и достъп до информация от страна на ползвателите, което им пречи да избират продукти с подходящи характеристики за киберсигурност или да ги използват по защитен начин.

Изменение 2

Предложение за регламент Съображение 7

Текст, предложен от Комисията

(7) При определени условия всички

Изменение

(7) При определени условия всички

продукти с цифрови елементи, интегрирани в по-голяма електронна информационна система или свързани с нея, могат да послужат като вектор на атака за злонамерени участници. В резултат на това дори хардуерът и софтуерът, считани за по-малко критични, могат да улеснят първоначалното компрометиране на дадено устройство или мрежа, като позволят на злонамерените участници да получат привилегирован достъп до дадена система или да се придвижат странично между системите. Поради това производителите следва да гарантират, че всички **свързващи се** продукти с цифрови елементи са проектирани и разработени в съответствие със съществените изисквания, определени в настоящия регламент. Това включва както продукти, които могат да бъдат свързани физически чрез хардуерни интерфейси, така и продукти, които са свързани логически, например чрез сокет, канали, файлове, приложно-програмен интерфейс или други видове софтуерни интерфейси. Тъй като киберзаплахите могат да се разпространяват чрез различни продукти с цифрови елементи преди да достигнат до определена цел, например чрез верижно използване на множество уязвимости, производителите следва да гарантират киберсигурността и на тези продукти, които са само непряко свързани с други устройства или мрежи.

продукти с цифрови елементи, интегрирани в по-голяма електронна информационна система или свързани с нея, могат да послужат като вектор на атака за злонамерени участници. В резултат на това дори хардуерът и софтуерът, считани за по-малко критични, могат да улеснят първоначалното компрометиране на дадено устройство или мрежа, като позволят на злонамерените участници да получат привилегирован достъп до дадена система или да се придвижат странично между системите. Поради това производителите следва да гарантират, че всички продукти с цифрови елементи, **свързани с външна мрежа или устройство**, са проектирани и разработени в съответствие със съществените изисквания, определени в настоящия регламент. Това включва както продукти, които могат да бъдат свързани **с външни мрежи или устройство** физически чрез хардуерни интерфейси, така и продукти, които са свързани логически, например чрез сокет, канали, файлове, приложно-програмен интерфейс или други видове софтуерни интерфейси. Тъй като киберзаплахите могат да се разпространяват чрез различни продукти с цифрови елементи преди да достигнат до определена цел, например чрез верижно използване на множество уязвимости, производителите следва да гарантират киберсигурността и на тези продукти, които са само непряко свързани с други устройства или мрежи.

Изменение 3

Предложение за регламент Съображение 7 а (ново)

Текст, предложен от Комисията

Изменение

(7 а) Настоящият регламент не следва да се прилага за вътрешните мрежи на продукт с цифрови елементи, ако тези мрежи имат специални крайни точки и са напълно изолирани и защитени от външна връзка на данни.

Изменение 4

Предложение за регламент Съображение 7 б (ново)

Текст, предложен от Комисията

Изменение

(7 б) Настоящият регламент не следва да се прилага за резервни части, предназначени единствено за замяна на дефектни части на продукти с цифрови елементи с цел възстановяване на тяхната функционалност.

Изменение 5

Предложение за регламент Съображение 9

Текст, предложен от Комисията

Изменение

(9) С настоящия регламент се гарантира високо равнище на киберсигурност на продуктите с цифрови елементи. С него не се уреждат услуги, като например софтуер като услуга (SaaS), с изключение на решенията за дистанционна обработка на данни, свързани с продукт с цифрови елементи, разбирани като всяка обработка на данни от разстояние, за която софтуерът е проектиран и разработен от производителя на

(9) С настоящия регламент се гарантира високо равнище на киберсигурност на продуктите с цифрови елементи. С него не се уреждат услуги, като например софтуер като услуга (SaaS). С [Директива XXX/XXXX (МИС 2)] се въвеждат изисквания за киберсигурност и докладване на инциденти за съществени и важни субекти, като например критична инфраструктура, с оглед повишаване на устойчивостта на предоставяните от тях услуги.

съответния продукт или на негова отговорност, и липсата на която би попречила на такъв продукт с цифрови елементи да изпълнява някоя от функциите си. С

[Директива XXX/XXXX (МИС 2)] се въвеждат изисквания за киберсигурност и докладване на инциденти за съществени и важни субекти, като например критична инфраструктура, с оглед повишаване на устойчивостта на предоставяните от тях услуги.

[Директива XXX/XXXX (МИС 2)] се прилага за облачни услуги и модели на облачни услуги, като например SaaS. Всички субекти, предоставящи облачни услуги в Съюза, които отговарят на или надвишават прага за средни предприятия, попадат в обхвата на тази директива.

[Директива XXX/XXXX (МИС 2)] се прилага за облачни услуги и модели на облачни услуги, като например SaaS. Всички субекти, предоставящи облачни услуги в Съюза, които отговарят на или надвишават прага за средни предприятия, попадат в обхвата на тази директива.

Изменение 6

Предложение за регламент Съображение 10

Текст, предложен от Комисията

(10) С оглед да не се възпрепятстват иновациите или научните изследвания, свободният софтуер с отворен код, разработен или предоставян извън рамките на търговска дейност, не следва да бъде обхванат от настоящия регламент. Това се отнася по-специално за софтуер, включително неговия изходен код и модифицирани версии, който е свободно споделян и свободно достъпен, използваем, модифицируем и преразпределяем. В **контекста на софтуера търговската дейност** може да се характеризира **не само** с начисляване на цена за **продукт**, но и с начисляване на цена за услуги по техническа поддръжка, с предоставяне на софтуерна платформа, чрез която производителят печели от други услуги, или с използване на лични данни по

Изменение

(10) **Софтуерът и данните, които се споделят открито и до които ползвателите имат свободен достъп и свободно могат да използват, променят и разпространяват същите или техни модифицирани версии, могат да допринесат за научните изследвания и иновациите на пазара. Изследванията на Комисията показват също, че свободният софтуер с отворен код може да допринесе с между 65 и 95 млрд. евро за БВП на Съюза и че може да предостави значителни възможности за растеж на европейската икономика.** С оглед да не се възпрепятстват иновациите или научните изследвания, свободният софтуер с отворен код, разработен или предоставян извън рамките на търговска

причини, различни от такива, свързани изключително с подобряване на сигурността, съвместимостта или оперативната съвместимост на софтуера.

дейност, не следва да бъде обхванат от настоящия регламент. Това се отнася по-специално за софтуер, включително неговия изходен код и модифицирани версии, който е свободно споделян и свободно достъпен, използваем, модифицируем и преразпределяем.

Търговска дейност в смисъл на предоставяне на пазара обаче може да се характеризира с начисляване на цена за **компонент на свободен софтуер с отворен код**, но и с **извличане на парична печалба, като например** начисляване на цена за услуги по техническа поддръжка **или платени актуализации на софтуер, освен ако това служи само за възстановяване на действителни разходи**, с предоставяне на софтуерна платформа, чрез която производителят печели от други услуги, или с използване на лични данни по причини, различни от такива, свързани изключително с подобряване на сигурността, съвместимостта или оперативната съвместимост на софтуера. **Нито съвместното разработване на компоненти на свободен софтуер с отворен код, нито предоставянето им в хранилища със свободен достъп не следва да представлява пускане на пазара или въвеждане в експлоатация.**

Обстоятелствата, при които е разработен продуктът, или начинът, по който е финансирана разработката, не следва да се вземат предвид при определяне на търговския или нетърговския характер на тази дейност. Когато софтуер с отворен код е интегриран в краен продукт с цифрови елементи, който се пуска на пазара, икономическият оператор, който е пуснал на пазара крайния продукт с цифрови елементи, следва да носи отговорност за съответствието на продукта, включително на компонентите на свободния софтуер с отворен код.

Изменение 7

Предложение за регламент Съображение 11

Текст, предложен от Комисията

(11) Сигурният интернет е незаменим за функционирането на критичните инфраструктури и за обществото като цяло. [Директива XXX/XXXX (МИС 2)] има за цел да осигури високо ниво на киберсигурност на услугите, предоставяни от съществени и важни субекти, включително доставчици на цифрова инфраструктура, които поддържат основните функции на отворения интернет, осигуряват достъп до интернет и интернет услуги. Поради това е важно продуктите с цифрови елементи, необходими на доставчиците на цифрова инфраструктура за осигуряване на функционирането на интернет, да се разработват по сигурен начин и да отговарят на утвърдените стандарти за сигурност в интернет. Настоящият регламент, който се прилага за всички **свързващи се** хардуерни и софтуерни продукти, има за цел също така да улесни доставчиците на цифрова инфраструктура при спазването на изискванията за веригата на доставките съгласно [Директива XXX/XXXX (МИС 2)], като се гарантира, че продуктите с цифрови елементи, които те използват за предоставяне на своите услуги, са разработени по сигурен начин и че те имат достъп до своевременни актуализации на защитата на тези продукти.

Изменение 8

Изменение

(11) Сигурният интернет е незаменим за функционирането на критичните инфраструктури и за обществото като цяло. [Директива XXX/XXXX (МИС 2)] има за цел да осигури високо ниво на киберсигурност на услугите, предоставяни от съществени и важни субекти, включително доставчици на цифрова инфраструктура, които поддържат основните функции на отворения интернет, осигуряват достъп до интернет и интернет услуги. Поради това е важно продуктите с цифрови елементи, необходими на доставчиците на цифрова инфраструктура за осигуряване на функционирането на интернет, да се разработват по сигурен начин и да отговарят на утвърдените стандарти за сигурност в интернет. Настоящият регламент, който се прилага за всички хардуерни и софтуерни продукти, **свързани с външна мрежа или устройство**, има за цел също така да улесни доставчиците на цифрова инфраструктура при спазването на изискванията за веригата на доставките съгласно [Директива XXX/XXXX (МИС 2)], като се гарантира, че продуктите с цифрови елементи, които те използват за предоставяне на своите услуги, са разработени по сигурен начин и че те имат достъп до своевременни актуализации на защитата на тези продукти.

Предложение за регламент Съображение 15

Текст, предложен от Комисията

(15) В Делегиран Регламент (ЕС) 2022/30 се уточнява, че съществените изисквания, определени в член 3, параграф 3, буква г) (вреди за мрежата и неправилна употреба на мрежови ресурси), буква д) (лични данни и неприкосновеност на личния живот) и буква е) (измами) от Директива 2014/53/ЕС, се прилагат за определени радиосъоръжения. В [Решение за изпълнение XXX/2022 на Комисията относно искане за стандартизация, отправено до европейските организации за стандартизация] се определят изисквания за разработване на специфични стандарти, в които допълнително се уточнява как следва да се отговори на тези три съществени изисквания. Съществените изисквания, определени с настоящия регламент, включват всички елементи на съществените изисквания по член 3, параграф 3, букви г), д) и е) от Директива 2014/53/ЕС. Освен това съществените изисквания, определени в настоящия регламент, са съгласувани с целите на изискванията за специфични стандарти, включени в посоченото искане за стандартизация. Поради това, **ако** Комисията отмени **или измени** Делегиран регламент (ЕС) 2022/30, вследствие на което той престане да се прилага за някои продукти, предмет на настоящия регламент, при изготвянето и разработването на хармонизирани стандарти за улесняване на прилагането на настоящия регламент, Комисията и европейските организации за стандартизация следва да вземат предвид работата по стандартизацията, извършена в контекста на Решение за изпълнение C(2022)5637 на Комисията относно искане за стандартизация за

Изменение

(15) В Делегиран регламент (ЕС) 2022/30 се уточнява, че съществените изисквания, определени в член 3, параграф 3, буква г) (вреди за мрежата и неправилна употреба на мрежови ресурси), буква д) (лични данни и неприкосновеност на личния живот) и буква е) (измами) от Директива 2014/53/ЕС, се прилагат за определени радиосъоръжения. В [Решение за изпълнение XXX/2022 на Комисията относно искане за стандартизация, отправено до европейските организации за стандартизация] се определят изисквания за разработване на специфични стандарти, в които допълнително се уточнява как следва да се отговори на тези три съществени изисквания. Съществените изисквания, определени с настоящия регламент, включват всички елементи на съществените изисквания по член 3, параграф 3, букви г), д) и е) от Директива 2014/53/ЕС. Освен това съществените изисквания, определени в настоящия регламент, са съгласувани с целите на изискванията за специфични стандарти, включени в посоченото искане за стандартизация. Поради това, **когато** Комисията отмени Делегиран регламент (ЕС) 2022/30, вследствие на което той престане да се прилага за някои продукти, предмет на настоящия регламент, при изготвянето и разработването на хармонизирани стандарти за улесняване на прилагането на настоящия регламент, Комисията и европейските организации за стандартизация следва да вземат предвид работата по стандартизацията, извършена в контекста на Решение за изпълнение C(2022)5637 на Комисията относно искане за стандартизация за

Делегиран регламент 2022/30 относно радиосъоръженията.

Делегиран регламент 2022/30 относно радиосъоръженията.

Изменение 9

Предложение за регламент Съображение 18 а (ново)

Текст, предложен от Комисията

Изменение

(18 а) За да се гарантира, че разработчиците на софтуер, които са физически лица или микропредприятия, както са определени в Препоръка 2003/361/ЕО на Комисията, не се сблъскват с големи финансови пречки и не са възпрепятствани да изпитат на пазара концепцията, както и икономическата обосновка, от тези субекти следва да се изисква да положат максимални усилия, за да спазят изискванията в настоящото предложение през 6-те месеца от пускането на софтуера на пазара. Този специален режим следва да предотврати възпиращото въздействие, което високите разходи за привездане в съответствие и за навлизане на пазара биха могли да оказат върху предприемачите или квалифицираните лица, обмислящи разработването на софтуер в Съюза. Въпреки това този специален режим не следва да се прилага за продуктите с цифрови елементи с висока степен на критичност.

Изменение 10

Предложение за регламент Съображение 19

Текст, предложен от Комисията

Изменение

(19) Някои задачи, предвидени в

(19) Някои задачи, предвидени в

настоящия регламент, следва да се изпълняват от ENISA в съответствие с член 3, параграф 2 от Регламент (ЕС) 2019/881. По-специално ENISA следва да получава уведомления от производителите за активно експлоатирани уязвимости, съдържащи се в продукти с цифрови елементи, както и за инциденти, които оказват въздействие върху сигурността на тези продукти. ENISA следва също така да препраща тези уведомления до съответните екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС) или съответно до съответните единни звена за контакт на държавите членки, определени в съответствие с [член X] от [Директива XXX/XXXX (МИС 2)], и да информира съответните органи за надзор на пазара за уязвимостта, за която е получено уведомление. Въз основа на събраната информация ENISA следва да изготвя двугодишен технически доклад за нововъзникващите тенденции по отношение на киберрисковете в продуктите с цифрови елементи и да го представя на групата за сътрудничество за МИС, посочена в [Директива XXX/XXXX (МИС 2)]. Освен това, като се имат предвид нейният експертен опит и мандат, ENISA следва да може да подкрепя процеса по правоприлагането на настоящия регламент. По-специално, тя следва да може да предлага съвместни дейности, които да бъдат провеждани от органите за надзор на пазара въз основа на признаци или информация относно потенциално несъответствие с настоящия регламент на продукти с цифрови елементи в няколко държави членки, или да определя категориите продукти, за които следва да се организират едновременни координирани контролни действия. При извънредни обстоятелства по искане на Комисията ENISA следва да може да извършва оценки по отношение на

настоящия регламент, следва да се изпълняват от ENISA в съответствие с член 3, параграф 2 от Регламент (ЕС) 2019/881. По-специално ENISA следва да получава уведомления от производителите **чрез ранно предупреждение** за активно експлоатирани уязвимости, съдържащи се в продукти с цифрови елементи, както и за инциденти, които оказват **значително** въздействие върху сигурността на тези продукти. ENISA следва също така да препраща тези уведомления до съответните екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС) или съответно до съответните единни звена за контакт на държавите членки, определени в съответствие с [член X] от [Директива XXX/XXXX (МИС 2)], и **незабавно** да информира съответните органи за надзор на пазара за **съществуването на уязвимост и когато е приложимо – за възможните мерки за смекчаване на риска. Когато за уязвимостта, за която е получено уведомление, няма налични корективни или смекчаващи мерки, ENISA следва да гарантира, че информацията за тази съобщена уязвимост се споделя в съответствие със строги протоколи за сигурност и въз основа на принципа „необходимост да се знае“**. Въз основа на събраната информация ENISA следва да изготвя двугодишен технически доклад за нововъзникващите тенденции по отношение на киберрисковете в продуктите с цифрови елементи и да го представя на групата за сътрудничество за МИС, посочена в [Директива XXX/XXXX (МИС 2)]. Освен това, като се имат предвид нейният експертен опит и мандат, ENISA следва да може да подкрепя процеса по правоприлагането на настоящия регламент. По-специално, тя следва да може да предлага съвместни дейности, които да бъдат провеждани от

конкретни продукти с цифрови елементи, които представляват значителен киберриск, когато е необходима незабавна намеса за запазване на доброто функциониране на вътрешния пазар.

органите за надзор на пазара въз основа на признаци или информация относно потенциално несъответствие с настоящия регламент на продукти с цифрови елементи в няколко държави членки, или да определя категориите продукти, за които следва да се организират едновременни координирани контролни действия. При извънредни обстоятелства по искане на Комисията ENISA следва да може да извършва оценки по отношение на конкретни продукти с цифрови елементи, които представляват значителен киберриск, когато е необходима незабавна намеса за запазване на доброто функциониране на вътрешния пазар.

Изменение 11

Предложение за регламент Съображение 20

Текст, предложен от Комисията

(20) Продуктите с цифрови елементи следва да носят маркировката „СЕ“, указваща тяхното съответствие с настоящия регламент с цел свободно движение в рамките на вътрешния пазар. Държавите членки следва да не създават необосновани пречки пред пускането на пазара на продукти с цифрови елементи, които съответстват на изискванията, предвидени в настоящия регламент, и носят маркировката „СЕ“.

Изменение

(20) Продуктите с цифрови елементи следва да носят маркировката „СЕ“, указваща **по видим, четлив и незаличим начин** тяхното съответствие с настоящия регламент с цел свободно движение в рамките на вътрешния пазар. Държавите членки следва да не създават необосновани пречки пред пускането на пазара на продукти с цифрови елементи, които съответстват на изискванията, предвидени в настоящия регламент, и носят маркировката „СЕ“.

Изменение 12

Предложение за регламент Съображение 22

(22) С цел да се гарантира, че когато се пускат на пазара, продуктите с цифрови елементи не създават киберрискове за хората и организациите, следва да се определят съществени изисквания за такива продукти. Когато продуктите впоследствие бъдат изменени с физически или цифрови средства по начин, който не е предвиден от производителя, и това може да означава, че те вече не отговарят на съответните съществени изисквания, изменението следва да се смята за съществено. Например актуализациите на софтуера или ремонтите биха могли да бъдат приравнени към операциите по поддръжка, при условие че те не променят вече пуснатия на пазара продукт по начин, по който може да бъде засегнато съответствието с приложимите изисквания или да бъде променена предвидената употреба, за която продуктът е бил оценен. Както и в случая с физическите ремонти или изменения, даден продукт с цифрови елементи следва да се счита за съществено изменен чрез промяна на софтуера, когато актуализацията на софтуера променя първоначално предвидените функции, типа или експлоатационните характеристики на продукта и тези промени не са били предвидени в първоначалната оценка на риска, или естеството на опасността се е променило, или нивото на риска се е увеличило поради актуализацията на софтуера.

(22) С цел да се гарантира, че когато се пускат на пазара, продуктите с цифрови елементи не създават киберрискове за хората и организациите, следва да се определят съществени изисквания за такива продукти. Когато продуктите впоследствие бъдат изменени с физически или цифрови средства по начин, който не е предвиден от производителя, и това може да означава, че те вече не отговарят на съответните съществени изисквания, изменението следва да се смята за съществено. Например актуализациите на софтуера или ремонтите, **като незначителни корекции на изходния код, които могат да подобрят сигурността и функционирането**, биха могли да бъдат приравнени към операциите по поддръжка, при условие че те не променят вече пуснатия на пазара продукт по начин, по който може да бъде засегнато съответствието с приложимите изисквания или да бъде променена предвидената употреба, за която продуктът е бил оценен. Както и в случая с физическите ремонти или изменения, даден продукт с цифрови елементи следва да се счита за съществено изменен чрез промяна на софтуера, когато актуализацията на софтуера променя първоначално предвидените функции, типа или експлоатационните характеристики на продукта и тези промени не са били предвидени в първоначалната оценка на риска, или естеството на опасността се е променило, или нивото на риска се е увеличило поради актуализацията на софтуера.

Изменение 13

Предложение за регламент Съображение 23

Текст, предложен от Комисията

(23) В съответствие с общоприетото понятие за съществено изменение за продукти, регулирани от законодателството на Съюза за хармонизация, когато настъпи съществено изменение, което може да повлияе на съответствието на даден продукт с настоящия регламент, или когато се промени предназначението на този продукт, е целесъобразно да се провери съответствието на продукта с цифровите елементи и, когато е приложимо, **той да бъде подложен на ново оценяване** на съответствието. Когато е приложимо, ако производителят извършва оценяване на съответствието с участието на трета страна, за промените, които могат да доведат до съществени изменения, следва да се уведоми третата страна.

Изменение

(23) В съответствие с общоприетото понятие за съществено изменение за продукти, регулирани от законодателството на Съюза за хармонизация, когато настъпи съществено изменение, което може да повлияе на съответствието на даден продукт с настоящия регламент, или когато се промени предназначението на този продукт, е целесъобразно да се провери съответствието на продукта с цифровите елементи и, когато е приложимо, **да се актуализира оценяването** на съответствието. Когато е приложимо, ако производителят извършва оценяване на съответствието с участието на трета страна, за промените, които могат да доведат до съществени изменения, следва да се уведоми третата страна. **Последващото оценяване на съответствието следва да бъде насочено към промените, които водят до новото оценяване, освен ако тези промени оказват значително въздействие върху съответствието на други части на продукта. Когато се въвеждат актуализации на софтуера, от производителя следва да не се изисква да извършва друга оценка на съответствието на продукта с цифрови елементи, освен ако актуализацията на софтуера води до съществено изменение на продукта с цифрови елементи.**

Изменение 14

Предложение за регламент Съображение 24 а (ново)

(24 а) Производителите на продукти с цифрови елементи следва да гарантират, че актуализациите на софтуера се предоставят по ясен и прозрачен начин с ясно разграничение между актуализациите на защитата и актуализациите на функционалността. Въпреки че актуализациите на защитата имат за цел да намалят нивото на риска на даден продукт с цифрови елементи, използването на актуализации на функционалността, предоставени от производителя, следва винаги да остане избор на ползвателя. Поради това производителите следва да предоставят тези актуализации отделно, освен ако това е технически невъзможно. Производителите следва да предоставят на потребителите подходяща информация за причините за всяка актуализация и за предвиденото ѝ въздействие върху продукта, както и ясен и лесен за използване механизъм за отказ.

Изменение 15

Предложение за регламент Съображение 25

Текст, предложен от Комисията

Изменение

(25) Продуктите с цифрови елементи следва да се считат за критични, ако отрицателното въздействие от използването на потенциални уязвимости в киберсигурността на продукта може да бъде сериозно поради, наред с другото, функционалните възможности, свързани с киберсигурността или предвидената употреба. По-специално, уязвимостите в продуктите с цифрови елементи, които имат свързани с киберсигурността

(25) Продуктите с цифрови елементи следва да се считат за критични, ако отрицателното въздействие от използването на потенциални уязвимости в киберсигурността на продукта може да бъде сериозно поради, наред с другото, функционалните възможности, свързани с киберсигурността или предвидената употреба. По-специално, уязвимостите в продуктите с цифрови елементи, които имат свързани с киберсигурността

функционални възможности, като например защитени елементи, могат да доведат до разпространение на проблеми със сигурността по цялата верига на доставките. Сериозността на въздействието на киберинцидент може да се увеличи и когато се вземе предвид предвидената употреба на продукта, например в промишлена среда или в контекста на основен субект от вида, посочен в [приложение I] към [Директива XXX/XXXX (МИС 2)], или за изпълнението на критични или чувствителни функции, като например обработването на лични данни.

функционални възможности, като например защитени елементи, могат да доведат до разпространение на проблеми със сигурността по цялата верига на доставките. Сериозността на въздействието на киберинцидент може да се увеличи и когато се вземе предвид предвидената употреба на продукта **в критични приложения в чувствителна среда**, например в промишлена среда или в контекста на основен субект от вида, посочен в [приложение I] към [Директива XXX/XXXX (МИС 2)], или за изпълнението на критични или чувствителни функции, като например обработването на лични данни.

Изменение 16

Предложение за регламент Съображение 26

Текст, предложен от Комисията

(26) Критичните продукти с цифрови елементи следва да подлежат на по-строги процедури за оценяване на съответствието, като се запази пропорционален подход. За тази цел критичните продукти с цифрови елементи следва да бъдат разделени на два класа, които отразяват нивото на киберриска, свързан с тези категории продукти. Потенциален киберинцидент, свързан с продукти от клас II, може да доведе до по-големи отрицателни въздействия, отколкото инцидент, свързан с продукти от клас I, например поради естеството на тяхната функция, свързана с киберсигурността, или предвидената им употреба в чувствителна среда, и поради това следва да се подложи на по-строга процедура за оценяване на съответствието.

Изменение

(26) Критичните продукти с цифрови елементи следва да подлежат на по-строги процедури за оценяване на съответствието, като се запази пропорционален подход. За тази цел критичните продукти с цифрови елементи следва да бъдат разделени на два класа, които отразяват нивото на киберриска, свързан с тези категории продукти. Потенциален киберинцидент, свързан с продукти от клас II, може да доведе до по-големи отрицателни въздействия, отколкото инцидент, свързан с продукти от клас I, например поради естеството на тяхната функция, свързана с киберсигурността, или предвидената им употреба в чувствителна среда, и поради това следва да се подложи на по-строга процедура за оценяване на съответствието. **По изключение малките и микропредприятията следва да могат да използват**

Изменение 17

Предложение за регламент Съображение 29

Текст, предложен от Комисията

(29) Продуктите с цифрови елементи, класифицирани като високорискови системи с ИИ съгласно член 6 от Регламент²⁷ [Регламента относно ИИ], които попадат в обхвата на настоящия регламент, следва да отговарят на съществените изисквания, определени в настоящия регламент. Когато тези високорискови системи с ИИ отговарят на съществените изисквания на настоящия регламент, те следва да се считат за съответстващи на изискванията за киберсигурност, определени в [член 15] от Регламент [Регламента относно ИИ], доколкото тези изисквания са обхванати от ЕС декларацията за съответствие или части от нея, издадена съгласно настоящия регламент. По отношение на процедурите за оценяване на съответствието, свързани със съществените изисквания за киберсигурност на даден продукт с цифрови елементи, обхванат от настоящия регламент и класифициран като високорискова система с ИИ, по правило следва да се прилагат съответните разпоредби на **член 43** от Регламент [Регламента относно ИИ] вместо съответните разпоредби на настоящия регламент. Това правило **обаче** следва да **не води до намаляване на необходимото** ниво на увереност за критичните продукти с цифрови елементи, обхванати от настоящия регламент. **Поради това, като изключение от това правило**, високорисковите системи с ИИ, които попадат в обхвата на Регламента

Изменение

(29) Продуктите с цифрови елементи **или частично комплектваните продукти с цифрови елементи**, класифицирани като високорискови системи с ИИ съгласно член 6 от Регламент²⁷ [Регламента относно ИИ], които попадат в обхвата на настоящия регламент, следва да отговарят на съществените изисквания, определени в настоящия регламент. Когато тези високорискови системи с ИИ отговарят на съществените изисквания на настоящия регламент, те следва да се считат за съответстващи на изискванията за киберсигурност, определени в [член 15] от Регламент [Регламента относно ИИ], доколкото тези изисквания са обхванати от ЕС декларацията за съответствие или части от нея, издадена съгласно настоящия регламент. По отношение на процедурите за оценяване на съответствието, свързани със съществените изисквания за киберсигурност на даден продукт с цифрови елементи, обхванат от настоящия регламент и класифициран като високорискова система с ИИ, по правило следва да се прилагат съответните разпоредби на **[приложимите разпоредби]** от Регламент [Регламента относно ИИ] вместо съответните разпоредби на настоящия регламент. Това правило следва да **създаде високо** ниво на увереност за критичните продукти с цифрови елементи, обхванати от настоящия регламент. **За** високорисковите системи с ИИ, които

[Регламента относно ИИ] и са определени също като критични продукти с цифрови елементи съгласно настоящия регламент **и за които се прилага процедурата за оценяване на съответствието въз основа на вътрешен контрол, посочена в приложение VI към Регламент [Регламента относно ИИ]**, следва да бъдат предмет на разпоредбите за оценяване на съответствието на настоящия регламент, доколкото това се отнася до съществените изисквания на настоящия регламент. **В този случай за всички останали аспекти, обхванати от Регламент [Регламента относно ИИ]**, следва да се прилагат съответните разпоредби за оценяване на съответствието въз основа на вътрешен контрол, посочени в приложение VI към Регламент [Регламента относно ИИ].

²⁷ [Регламент относно ИИ].

Изменение 18

Предложение за регламент Съображение 32

Текст, предложен от Комисията

(32) За да се гарантира, че продуктите с цифрови елементи са безопасни както в момента на пускането им на пазара, така и по време на целия им жизнен цикъл, е необходимо да се определят съществени изисквания за отстраняване на уязвимостите и съществени изисквания за киберсигурността, свързани с характеристиките на продуктите с цифрови елементи. Въпреки че производителите следва да спазват всички съществени изисквания, свързани с отстраняването на уязвимостите, и да гарантират, че всички техни продукти се доставят без

попадат в обхвата на Регламента [Регламента относно ИИ] и са определени също като критични продукти с цифрови елементи съгласно настоящия регламент, **отговорният секторен нотифициран орган** следва да **отговаря** за **извършването** на **оценяването** на **съответствието** съгласно настоящия регламент **и да ръководи административния процес, така че икономическите оператори да могат да отправят искането си** за оценяване на съответствието **до единствен регулаторен орган**.

²⁷ [Регламент относно ИИ].

Изменение

(32) За да се гарантира, че продуктите с цифрови елементи са безопасни както в момента на пускането им на пазара, така и по време на целия им жизнен цикъл, е необходимо да се определят съществени изисквания за отстраняване на уязвимостите и съществени изисквания за киберсигурността, свързани с характеристиките на продуктите с цифрови елементи. Въпреки че производителите следва да спазват всички съществени изисквания, свързани с отстраняването на уязвимостите, и да гарантират, че всички техни продукти се доставят без

известни уязвимости, които могат да бъдат използвани, те следва да определят кои други съществени изисквания, свързани с характеристиките на продукта, са приложими за съответния вид продукт. За тази цел производителите следва да извършат оценка на киберрисковете, свързани с даден продукт с цифрови елементи, за да определят съответните рискове и съответните съществени изисквания, както и за да приложат по уместен начин подходящи хармонизирани стандарти *или общи спецификации*.

Изменение 19

Предложение за регламент Съображение 33 а (ново)

Текст, предложен от Комисията

известни уязвимости, които могат да бъдат използвани, те следва да определят кои други съществени изисквания, свързани с характеристиките на продукта, са приложими за съответния вид продукт. За тази цел производителите следва да извършат оценка на киберрисковете, свързани с даден продукт с цифрови елементи, за да определят съответните рискове и съответните съществени изисквания, както и за да приложат по уместен начин подходящи хармонизирани стандарти.

Изменение

(33 а) С цел да се гарантира, че продуктите са проектирани, разработени и произведени в съответствие със съществените изисквания, предвидени в приложение I, раздел I, производителите следва да полагат дължимата грижа, когато интегрират компоненти, доставени от трети страни, в продукти с цифрови елементи. Такъв е случаят при компоненти, които са съобразени с особеностите на продукта и са интегрирани в него, по-специално в случай на свободен софтуер с отворен код, който не е пуснат на пазара в замяна на финансова или друг вид печалба.

Изменение 20

Предложение за регламент Съображение 34

(34) За да се гарантира, че на националните ЕРИКС и на единното звено за контакт, определени в съответствие с член [член X] от [Директива XX/XXXX (МИС 2)], се предоставя необходимата информация за изпълнение на техните задачи и за повишаване на цялостното ниво на киберсигурност на съществените и важните субекти, както и за да се осигури ефективното функциониране на органите за надзор на пазара, производителите на продукти с цифрови елементи следва да уведомяват ENISA за уязвимости, които се използват активно. Тъй като повечето продукти с цифрови елементи се предлагат на целия вътрешен пазар, всяка използвана уязвимост в даден продукт с цифрови елементи следва да се счита за заплаха за функционирането на вътрешния пазар. Производителите следва също така да обмислят възможността за разкриване на фиксирани уязвимости в европейската база данни за уязвимости, създадена съгласно Директива [Директива XX/XXXX (МИС 2)] и управлявана от ENISA, или във всяка друга публично достъпна база данни за уязвимости.

(34) За да се гарантира, че на националните ЕРИКС и на единното звено за контакт, определени в съответствие с член [член X] от [Директива XX/XXXX (МИС 2)], се предоставя необходимата информация за изпълнение на техните задачи и за повишаване на цялостното ниво на киберсигурност на съществените и важните субекти, както и за да се осигури ефективното функциониране на органите за надзор на пазара, производителите на продукти с цифрови елементи следва да уведомяват ENISA **без неоправдано забавяне и във всички случаи в рамките на 48 часа от узнаването, чрез ранно предупреждение**, за уязвимости, които се използват активно. **След узнаването за активно използвана уязвимост, оказваща значително въздействие върху сигурността на продукта с цифрови елементи производителите следва да съобщават без неоправдано забавяне на ENISA допълнителни подробности относно използваната уязвимост. ENISA следва да бъде уведомена за всички други уязвимости, които не оказват значително въздействие върху сигурността на продукта с цифрови елементи, след като уязвимостта бъде отстранена.** Тъй като повечето продукти с цифрови елементи се предлагат на целия вътрешен пазар, всяка използвана уязвимост в даден продукт с цифрови елементи следва да се счита за заплаха за функционирането на вътрешния пазар. Производителите следва също така да обмислят възможността за разкриване на фиксирани уязвимости в европейската база данни за уязвимости, създадена съгласно Директива [Директива XX/XXXX (МИС 2)] и управлявана от ENISA, или във всяка друга публично достъпна база данни за

уязвимости.

Изменение 21

Предложение за регламент Съображение 34 а (ново)

Текст, предложен от Комисията

Изменение

(34 а) ENISA следва да отговаря за публикуването и поддържането на база данни с известни използвани уязвимости. Производителите следва да следят базата данни и да уведомяват за открити уязвимости в техните продукти.

Изменение 22

Предложение за регламент Съображение 35

Текст, предложен от Комисията

Изменение

(35) Производителите следва също така да докладват на ENISA за всеки инцидент, който оказва въздействие върху сигурността на продукта с цифрови елементи. Независимо от задълженията за докладване на инциденти в Директива [Директива XXX/XXXX (МИС 2)] за съществени и важни субекти, от решаващо значение за ENISA, единните звена за контакт, определени от държавите членки в съответствие с член [член X] от Директива [Директива XXX/XXXX (МИС 2)], и органите за надзор на пазара е да получават информация от производителите на продукти с цифрови елементи, която да им позволи да оценят сигурността на тези продукти. С цел да се гарантира, че ползвателите могат да реагират бързо на инциденти, които оказват въздействие върху

(35) Производителите следва също така да докладват на ENISA **чрез ранно предупреждение** за всеки инцидент, който оказва **значително** въздействие върху сигурността на продукта с цифрови елементи. **Производителите следва да уведомяват допълнително ENISA за повече подробности относно значителния инцидент, свързан с продукта с цифрови елементи, без неоправдано забавяне и във всички случаи в рамките на 72 часа след узнаването му.** Независимо от задълженията за докладване на инциденти в Директива [Директива XXX/XXXX (МИС 2)] за съществени и важни субекти, от решаващо значение за ENISA, единните звена за контакт, определени от държавите членки в съответствие с член [член X] от Директива [Директива XXX/XXXX (МИС 2)], и

сигурността на техните продукти с цифрови елементи, производителите следва също така да информират своите ползватели за всеки такъв инцидент и, когато е приложимо, за всички корективни мерки, които ползвателите могат да приложат, за да намалят въздействието на **инцидента**, например чрез публикуване на съответната информация на своите уебсайтове или, когато производителят е в състояние да се свърже с ползвателите и когато това е оправдано от рисковете, като се обърне директно към ползвателите.

органите за надзор на пазара е да получават информация от производителите на продукти с цифрови елементи, която да им позволи да оценят сигурността на тези продукти. С цел да се гарантира, че ползвателите могат да реагират бързо на инциденти, които оказват **значително** въздействие върху сигурността на техните продукти с цифрови елементи, производителите следва също така да информират своите ползватели за всеки такъв инцидент, **когато е целесъобразно и ако е вероятно те да бъдат засегнати неблагоприятно от него**, и когато е приложимо, за **смекчаването на риска** и всички корективни мерки, които ползвателите могат да приложат, за да намалят въздействието на **значителния инцидент**, например чрез публикуване на съответната информация на своите уебсайтове или, когато производителят е в състояние да се свърже с ползвателите и когато това е оправдано от рисковете, като се обърне директно към ползвателите. **Без да се засягат други задължения, производителите, които установят уязвимост в компонент, интегриран в продукт с цифрови елементи, включително в свободен компонент с отворен код, следва да докладват за уязвимостта на физическото или юридическото лице, което поддържа компонента, заедно с предприетата корективна мярка.**

Изменение 23

Предложение за регламент Съображение 37 а (ново)

Текст, предложен от Комисията

Изменение

(37 а) Съгласно Споразумението на СТО за техническите пречки пред търговията, когато са необходими технически правила и съществуват

съответни международни стандарти, членовете на СТО следва да използват тези стандарти като основа за своите технически правила. Важно е да се избягва дублирането на работата на организациите за стандартизация, тъй като международните стандарти имат за цел да улеснят хармонизирането на националните и регионалните технически регламенти и стандарти, като по този начин се намалят нетарифните технически пречки пред търговията. Като се има предвид, че киберсигурността е глобален проблем, Съюзът следва да се стреми към максимално съгласуване. За да се постигне тази цел, с искането за стандартизация за настоящия регламент, както е посочено в член 10 от Регламент 1025/2012, следва да се търси намаляване на пречките пред приемането на стандартите, като се публикуват данните за тях в Официален вестник на ЕС в съответствие с член 10, параграф 6 от Регламент 1025/2012.

Изменение 24

Предложение за регламент Съображение 37 б (ново)

Текст, предложен от Комисията

Изменение

(37 б) Като се има предвид широкият обхват на настоящия регламент, своевременното разработване на хармонизирани стандарти представлява сериозно предизвикателство. За да се повиши сигурността на продуктите с цифрови компоненти на пазара на Съюза във възможно най-кратък срок, Комисията следва да бъде оправомощена за ограничен период от време да обявява съществуващите

международни стандарти за киберсигурност на продуктите за отговарящи на изискванията на настоящия регламент. Тези стандарти следва да бъдат публикувани като стандарти, осигуряващи презумпция за съответствие.

Изменение 25

Предложение за регламент Съображение 38

Текст, предложен от Комисията

(38) С цел да се улесни оценяването на съответствието с изискванията, определени в настоящия регламент, следва да има презумпция за съответствие за продукти с цифрови елементи, които са в съответствие с хармонизирани стандарти, които превръщат съществените изисквания на настоящия регламент в подробни технически спецификации и които са приети в съответствие с Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета²⁹. Регламент (ЕС) № 1025/2012 предвижда процедура за възражения срещу хармонизирани стандарти, когато тези стандарти не отговарят напълно на изискванията на настоящия регламент.

²⁹ 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

Изменение

(38) С цел да се улесни оценяването на съответствието с изискванията, определени в настоящия регламент, следва да има презумпция за съответствие за продукти с цифрови елементи, които са в съответствие с хармонизирани стандарти, които превръщат съществените изисквания на настоящия регламент в подробни технически спецификации и които са приети в съответствие с Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета²⁹. Регламент (ЕС) № 1025/2012 предвижда процедура за възражения срещу хармонизирани стандарти, когато тези стандарти не отговарят напълно на изискванията на настоящия регламент. ***Процесът на стандартизация следва да гарантира балансирано представяне на интересите и ефективно участие на заинтересованите страни от гражданското общество, включително организациите на потребителите.***

²⁹ 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 (ОВ L 316, 14.11.2012 г., стр. 12).

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 (ОВ L 316, 14.11.2012 г., стр. 12).

Изменение 26

Предложение за регламент Съображение 41

Текст, предложен от Комисията

(41) Когато не са **приети хармонизирани** стандарти **или когато хармонизираните стандарти не отговарят в достатъчна степен на съществените изисквания на настоящия регламент**, Комисията следва да може да приема общи спецификации чрез актове за изпълнение. Причините за разработване на такива общи спецификации, вместо да се разчита на хармонизирани стандарти, могат да включват отказ на искане за стандартизация от някоя от европейските организации за стандартизация, неоправдано забавяне при установяването на подходящи хармонизирани стандарти или липса на съответствие на разработените стандарти с изискванията на настоящия регламент или с искане на Комисията. С цел да се улесни оценяването на съответствието със съществените изисквания, определени в настоящия регламент, следва да има презумпция за съответствие за продукти с цифрови елементи, които са в съответствие с общите спецификации, приети от Комисията съгласно настоящия регламент за целите на представянето на подробни технически спецификации на

Изменение

(41) Когато **в съответствие с Регламент (ЕС) 1025/2012 в Официален вестник на Европейския съюз не са публикувани позовавания на хармонизираните стандарти, които обхващат посочените в приложение I изисквания, и не се очаква да бъдат публикувани подобни позовавания в разумен срок**, Комисията следва да може да приема общи спецификации чрез актове за изпълнение. Причините за разработване на такива общи спецификации, вместо да се разчита на хармонизирани стандарти, могат да включват отказ на искане за стандартизация от някоя от европейските организации за стандартизация, неоправдано забавяне при установяването на подходящи хармонизирани стандарти или липса на съответствие на разработените стандарти с изискванията на настоящия регламент или с искане на Комисията. С цел да се улесни оценяването на съответствието със съществените изисквания, определени в настоящия регламент, следва да има презумпция за съответствие за продукти с цифрови елементи, които са в съответствие с общите спецификации, приети от Комисията съгласно настоящия

тези изисквания.

регламент за целите на представянето на подробни технически спецификации на тези изисквания.

Изменение 27

Предложение за регламент Съображение 43

Текст, предложен от Комисията

(43) Маркировката „СЕ“, указваща съответствието на продукта, е видимата последица от цял един процес, включващ оценяване на съответствието в широк смисъл. Основните принципи относно маркировката „СЕ“ са установени в Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета³⁰. Правилата за нанасяне на маркировката „СЕ“ върху продукти с цифрови елементи следва да бъдат определени в настоящия регламент. Маркировката „СЕ“ следва да бъде единствената маркировка, гарантираща съответствието на продуктите с цифрови елементи с изискванията на настоящия регламент.

³⁰ Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. за определяне на изискванията за акредитация и за отмяна на Регламент (ЕИО) № 339/93 (ОВ L 218, 13.8.2008 г., стр. 30).

Изменение

(43) Маркировката „СЕ“, указваща съответствието на продукта, е видимата последица от цял един процес, включващ оценяване на съответствието в широк смисъл. Основните принципи относно маркировката „СЕ“ са установени в Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета³⁰. Правилата за нанасяне на маркировката „СЕ“ върху продукти с цифрови елементи следва да бъдат определени в настоящия регламент. Маркировката „СЕ“ следва да бъде единствената маркировка, гарантираща съответствието на продуктите с цифрови елементи с изискванията на настоящия регламент. ***Въпреки това частично комплектван продукт с цифрови елементи не се маркира с маркировката „СЕ“ съгласно настоящия регламент, без да се засягат разпоредбите за маркиране, произтичащи от друго приложимо законодателство на Съюза. За частично комплектван продукт с цифрови елементи производителите следва да изготвят ЕС декларация за вграждане.***

³⁰ Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. за определяне на изискванията за акредитация и за отмяна на Регламент (ЕИО) № 339/93 (ОВ L 218, 13.8.2008 г., стр. 30).

Изменение 28

Предложение за регламент Съображение 45

Текст, предложен от Комисията

(45) Като общо правило **оценяването** на съответствието на продукти с цифрови елементи следва да се извършва от производителя на негова отговорност, като се следва процедурата, основана на модул А от Решение 768/2008/ЕО. Производителят следва да запази гъвкавостта си да избере по-строга процедура за оценяване на съответствието с участието на трета страна. Ако продуктът е класифициран като критичен продукт от клас I, се изисква допълнителна гаранция за доказване на съответствието със съществените изисквания, определени в настоящия регламент. Производителят следва да прилага хармонизирани стандарти, **общи спецификации** или схеми за сертифициране на киберсигурността съгласно Регламент (ЕС) 2019/881, които са определени от Комисията в акт за изпълнение, ако иска да извърши оценяване на съответствието на своя отговорност (модул А). Ако производителят не прилага такива хармонизирани стандарти, **общи спецификации** или схеми за сертифициране на киберсигурността, той следва да извърши оценяване на съответствието с участието на трета страна. Като се има предвид административната тежест за производителите и фактът, че киберсигурността играе важна роля в етапа на проектиране и разработване на материални и нематериални продукти с цифрови елементи, процедурите за оценяване на съответствието, основани съответно на модули В+С или модул Н

Изменение

(45) Като общо правило **изискванията за оценяване** на съответствието на продукти с цифрови елементи следва **да се основават на риска и в тази връзка в много случаи оценяването може** да се извършва от производителя на негова отговорност, като се следва процедурата, основана на модул А от Решение 768/2008/ЕО. Производителят следва да запази гъвкавостта си да избере по-строга процедура за оценяване на съответствието с участието на трета страна. Ако продуктът е класифициран като критичен продукт от клас I, се изисква допълнителна гаранция за доказване на съответствието със съществените изисквания, определени в настоящия регламент. Производителят следва да прилага хармонизирани стандарти или схеми за сертифициране на киберсигурността съгласно Регламент (ЕС) 2019/881, които са определени от Комисията в акт за изпълнение, ако иска да извърши оценяване на съответствието на своя отговорност (модул А). Ако производителят не прилага такива хармонизирани стандарти или схеми за сертифициране на киберсигурността, той следва да извърши оценяване на съответствието с участието на трета страна. Като се има предвид административната тежест за производителите и фактът, че киберсигурността играе важна роля в етапа на проектиране и разработване на материални и нематериални продукти с цифрови елементи, процедурите за оценяване на съответствието, основани

от Решение 768/2008/ЕО, бяха избрани като най-подходящи за оценяване на съответствието на критични продукти с цифрови елементи по пропорционален и ефективен начин. Производителят, който извършва оценяване на съответствието от трета страна, може да избере процедурата, която най-добре отговаря на неговия процес по проектиране и производство. Предвид още по-големия киберриск, свързан с използването на продукти, класифицирани като критични продукти от клас II, в оценяването на съответствието винаги трябва да участва трета страна.

съответно на модули В+С или модул Н от Решение 768/2008/ЕО, бяха избрани като най-подходящи за оценяване на съответствието на критични продукти с цифрови елементи по пропорционален и ефективен начин. Производителят, който извършва оценяване на съответствието от трета страна, може да избере процедурата, която най-добре отговаря на неговия процес по проектиране и производство. Предвид още по-големия киберриск, свързан с използването на продукти, класифицирани като критични продукти от клас II, в оценяването на съответствието винаги трябва да участва трета страна.

Изменение 29

Предложение за регламент Съображение 46 а (ново)

Текст, предложен от Комисията

Изменение

(46 а) Когато продуктите с цифрови елементи са еквивалентни, един от тези продукти може да бъде приет като представителен за семейство или категория продукти за целите на определени процедури за оценяване на съответствието.

Изменение 30

Предложение за регламент Съображение 55

Текст, предложен от Комисията

Изменение

(55) В съответствие с Регламент (ЕС) 2019/1020 органите за надзор на пазара осъществяват надзор на пазара на територията на съответната държава членка. Настоящият регламент следва да не възпрепятства държавите

(55) В съответствие с Регламент (ЕС) 2019/1020 органите за надзор на пазара осъществяват надзор на пазара на територията на съответната държава членка. Настоящият регламент следва да не възпрепятства държавите

членки да избират компетентните органи, които да изпълняват тези задачи. Всяка държава членка следва да определи един или повече органи за надзор на пазара на своята територия. Държавите членки могат да изберат да определят всеки съществуващ или нов орган, който да действа като орган за надзор на пазара, включително националните компетентни органи съгласно член **[член X]** от Директива **[Директива XXX/XXXX (МИС 2)]**, или определените национални органи за сертифициране на киберсигурността, посочени в член 58 от Регламент (ЕС) 2019/881. Икономическите оператори следва да си сътрудничат изцяло с органите за надзор на пазара и с други компетентни органи. Всяка държава членка следва да информира Комисията и другите държави членки за своите органи за надзор на пазара и за областите на компетентност на всеки от тези органи, както и да осигури необходимите ресурси и умения за изпълнение на задачите по надзора, свързани с настоящия регламент. Съгласно член 10, параграфи 2 и 3 от Регламент (ЕС) 2019/1020 всяка държава членка следва да определи единна служба за връзка, което следва да отговаря, наред с другото, за представянето на съгласуваната позиция на органите за надзор на пазара и за подпомагането на сътрудничеството между органите за надзор на пазара в различните държави членки.

членки да избират компетентните органи, които да изпълняват тези задачи. Всяка държава членка следва да определи един или повече органи за надзор на пазара на своята територия. Държавите членки могат да изберат да определят всеки съществуващ или нов орган, който да действа като орган за надзор на пазара, включително националните компетентни органи съгласно член **8** от Директива **(ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директивата за МИС 2)**, или определените национални органи за сертифициране на киберсигурността, посочени в член 58 от Регламент (ЕС) 2019/881. Икономическите оператори следва да си сътрудничат изцяло с органите за надзор на пазара и с други компетентни органи. Всяка държава членка следва да информира Комисията и другите държави членки за своите органи за надзор на пазара и за областите на компетентност на всеки от тези органи, както и да осигури необходимите ресурси и умения за изпълнение на задачите по надзора, свързани с настоящия регламент. Съгласно член 10, параграфи 2 и 3 от Регламент (ЕС) 2019/1020 всяка държава членка следва да определи единна служба за връзка, което следва да отговаря, наред с другото, за представянето на съгласуваната позиция на органите за надзор на пазара и за подпомагането на сътрудничеството между органите за надзор на пазара в различните държави членки.

Изменение 31

Предложение за регламент Съображение 56 а (ново)

Текст, предложен от Комисията

Изменение

(56 а) За да могат икономическите оператори, които са МСП и микропредприятия, да се справят с наложените от настоящия регламент нови задължения, Комисията следва да им предостави лесни за разбиране насоки и съвети, например чрез пряк канал за връзка с експерти, в случай че имат въпроси, като се отчита необходимостта от опростяване и ограничаване на административните тежести. При разработването на такива насоки Комисията следва да вземе предвид потребностите на МСП, така че административната и финансовата тежест да се сведат до минимум, като същевременно се улесни спазването на настоящия регламент от страна на МСП. Комисията следва да се консултира със съответните заинтересовани страни с експертен опит в областта на киберсигурността.

Изменение 32

Предложение за регламент Съображение 58

Текст, предложен от Комисията

Изменение

(58) В определени случаи даден продукт с цифрови елементи, който е в съответствие с настоящия регламент, може въпреки това да представлява значителен киберриск или риск за здравето или безопасността на хората, за спазването на задълженията по правото на Съюза или националното право, предназначени за защита на основните

(58) В определени случаи даден продукт с цифрови елементи, който е в съответствие с настоящия регламент, може въпреки това да представлява значителен киберриск или риск за здравето или безопасността на хората, за спазването на задълженията по правото на Съюза или националното право, предназначени за защита на основните

права, за достъпността, автентичността, целостта или поверителността на услугите, предлагани чрез електронна информационна система от основни субекти от вида, посочен в **[приложение I към Директива XXX/XXXX (МИС 2)]**, или за други аспекти на опазването на обществения интерес. Поради това е необходимо да се установят правила, които да гарантират намаляването на тези рискове. В резултат на това органите за надзор на пазара следва да предприемат мерки, с които да изискат от икономическия оператор да гарантира, че продуктът вече не представлява този риск, да го изведе или да го изтегли, в зависимост от риска. След като орган за надзор на пазара ограничи или забрани свободното движение на продукта по такъв начин, държавата членка следва незабавно да уведоми Комисията и другите държави членки за временните мерки, като посочи причините и основанията за решението. Когато орган за надзор на пазара приема такива мерки срещу продукти, представляващи риск, Комисията следва незабавно да започне консултации с държавите членки и със съответния(те) икономически оператор(и) и да извърши оценка на националната мярка. Въз основа на резултатите от тази оценка Комисията следва да взема решение дали националната мярка е оправдана или не. Комисията следва да адресира решението си до всички държави членки, като го съобщава незабавно на тях и на съответния(те) икономически оператор(и). Ако мярката бъде счетена за обоснована, Комисията може също така да обмисли приемането на предложения за преразглеждане на съответното законодателство на Съюза.

права, за достъпността, автентичността, целостта или поверителността на услугите, предлагани чрез електронна информационна система от основни субекти от вида, посочен в **приложение I към Директива (ЕС) 2022/2555 (Директивата МИС 2)**, или за други аспекти на опазването на обществения интерес. Поради това е необходимо да се установят правила, които да гарантират намаляването на тези рискове. В резултат на това органите за надзор на пазара следва да предприемат мерки, с които да изискат от икономическия оператор да гарантира, че продуктът вече не представлява този риск, да го изведе или да го изтегли, в зависимост от риска. След като орган за надзор на пазара ограничи или забрани свободното движение на продукта по такъв начин, държавата членка следва незабавно да уведоми Комисията и другите държави членки за временните мерки, като посочи причините и основанията за решението. Когато орган за надзор на пазара приема такива мерки срещу продукти, представляващи риск, Комисията следва незабавно да започне консултации с държавите членки и със съответния(те) икономически оператор(и) и да извърши оценка на националната мярка. Въз основа на резултатите от тази оценка Комисията следва да взема решение дали националната мярка е оправдана или не. Комисията следва да адресира решението си до всички държави членки, като го съобщава незабавно на тях и на съответния(те) икономически оператор(и). Ако мярката бъде счетена за обоснована, Комисията може също така да обмисли приемането на предложения за преразглеждане на съответното законодателство на Съюза.

Изменение 33

Предложение за регламент Съображение 59

Текст, предложен от Комисията

(59) По отношение на продукти с цифрови елементи, представляващи значителен киберриск, и когато има основание да се смята, че те не са в съответствие с настоящия регламент, или по отношение на продукти, които са в съответствие с настоящия регламент, но представляват други съществени рискове, като например рискове за здравето или безопасността на хората, основните права или предоставянето на услуги от основни субекти от вида, посочен в *[приложение I към Директива XXX/XXXX (МИС 2)]*, Комисията може да поиска от ENISA да извърши оценка. Въз основа на тази оценка Комисията може да приеме чрез актове за изпълнение корективни или ограничителни мерки на равнището на Съюза, включително да разпореда изтегляне от пазара или изземване на съответните продукти в разумен срок, съобразен с естеството на риска. Комисията може да прибегне до такава намеса само при извънредни обстоятелства, които оправдават незабавна намеса за запазване на доброто функциониране на вътрешния пазар, и само когато органите за надзор не са предприели ефективни мерки за коригиране на ситуацията. Такива извънредни обстоятелства могат да бъдат извънредни ситуации, когато например несъответстващ на изискванията продукт е широко предлаган от производителя в няколко държави членки, използва се също така в ключови сектори от субекти, обхванати от *[Директива XXX/XXXX (МИС 2)]*, като същевременно съдържа известни уязвимости, които се използват от злонамерени участници и за които

Изменение

(59) По отношение на продукти с цифрови елементи, представляващи значителен киберриск, и когато има основание да се смята, че те не са в съответствие с настоящия регламент, или по отношение на продукти, които са в съответствие с настоящия регламент, но представляват други съществени рискове, като например рискове за здравето или безопасността на хората, основните права или предоставянето на услуги от основни субекти от вида, посочен в *приложение I към Директива (ЕС) 2022/2555 (Директивата МИС 2)*, Комисията може да поиска от ENISA да извърши оценка. Въз основа на тази оценка Комисията може да приеме чрез актове за изпълнение корективни или ограничителни мерки на равнището на Съюза, включително да разпореда изтегляне от пазара или изземване на съответните продукти в разумен срок, съобразен с естеството на риска. Комисията може да прибегне до такава намеса само при извънредни обстоятелства, които оправдават незабавна намеса за запазване на доброто функциониране на вътрешния пазар, и само когато органите за надзор не са предприели ефективни мерки за коригиране на ситуацията. Такива извънредни обстоятелства могат да бъдат извънредни ситуации, когато например несъответстващ на изискванията продукт е широко предлаган от производителя в няколко държави членки, използва се също така в ключови сектори от субекти, обхванати от *Директива (ЕС) 2022/2555 (Директивата МИС 2)*, като същевременно съдържа известни уязвимости, които се използват от

производителят не предоставя налични корекции. Комисията може да се намесва в такива извънредни ситуации само за периода на извънредните обстоятелства и ако несъответствието с настоящия регламент или наличните съществени рискове продължават да съществуват.

злонамерени участници и за които производителят не предоставя налични корекции. Комисията може да се намесва в такива извънредни ситуации само за периода на извънредните обстоятелства и ако несъответствието с настоящия регламент или наличните съществени рискове продължават да съществуват.

Изменение 34

Предложение за регламент Съображение 62

Текст, предложен от Комисията

(62) С цел да се гарантира, че регулаторната рамка може да бъде адаптирана, когато е необходимо, на Комисията следва да се предостави правомощието да приема актове в съответствие с член 290 от Договора по отношение на актуализирането на списъка с критични продукти в приложение III и уточняването на определенията на тези категории продукти. На Комисията следва да бъде предоставено правомощието да приема актове в съответствие с посочения член за определянето на продукти с цифрови елементи, обхванати от други правила на Съюза, които постигат същото ниво на защита като настоящия регламент, като се уточнява дали ще е необходимо ограничение или изключване от обхвата на настоящия регламент, както и обхватът на това ограничение, ако е приложимо. На Комисията следва също така да бъде предоставено правомощието да приема актове в съответствие с посочения член във връзка с евентуалното **въвеждане на задължение за** сертифициране на някои продукти с цифрови елементи с висока степен на критичност въз основа на критериите за критичност, посочени в настоящия регламент, както и за

Изменение

(62) С цел да се гарантира, че регулаторната рамка може да бъде адаптирана, когато е необходимо, на Комисията следва да се предостави правомощието да приема актове в съответствие с член 290 от Договора по отношение на актуализирането на списъка с критични продукти в приложение III и уточняването на определенията на тези категории продукти. На Комисията следва да бъде предоставено правомощието да приема актове в съответствие с посочения член за определянето на продукти с цифрови елементи, обхванати от други правила на Съюза, които постигат същото ниво на защита като настоящия регламент, като се уточнява дали ще е необходимо ограничение или изключване от обхвата на настоящия регламент, както и обхватът на това ограничение, ако е приложимо. На Комисията следва също така да бъде предоставено правомощието да приема актове в съответствие с посочения член във връзка с евентуалното **доброволно** сертифициране на някои продукти с цифрови елементи с висока степен на критичност въз основа на критериите за критичност, посочени в настоящия регламент, както и за определянето на

определянето на минималното съдържание на ЕС декларацията за съответствие и за допълване на елементите, които трябва да бъдат включени в техническата документация. От особена важност е по време на подготвителната си работа Комисията да проведе подходящи консултации, включително на експертно равнище, и тези консултации да се проведат в съответствие с принципите, залегнали в Междуинституционалното споразумение от 13 април 2016 г. за по-добро законотворчество³³. По-специално, с цел осигуряване на равно участие при подготовката на делегираните актове, Европейският парламент и Съветът получават всички документи едновременно с експертите от държавите членки, като техните експерти получават систематично достъп до заседанията на експертните групи на Комисията, занимаващи се с подготовката на делегираните актове.

³³ ОВ L 123, 12.5.2016 г., стр. 1.

минималното съдържание на ЕС декларацията за съответствие и за допълване на елементите, които трябва да бъдат включени в техническата документация. От особена важност е по време на подготвителната си работа Комисията да проведе подходящи консултации, включително на експертно равнище, и тези консултации да се проведат в съответствие с принципите, залегнали в Междуинституционалното споразумение от 13 април 2016 г. за по-добро законотворчество³³. По-специално, с цел осигуряване на равно участие при подготовката на делегираните актове, Европейският парламент и Съветът получават всички документи едновременно с експертите от държавите членки, като техните експерти получават систематично достъп до заседанията на експертните групи на Комисията, занимаващи се с подготовката на делегираните актове.

³³ ОВ L 123, 12.5.2016 г., стр. 1.

Изменение 35

Предложение за регламент Съображение 63

Текст, предложен от Комисията

(63) За да се гарантират еднакви условия за изпълнение на настоящия регламент, на Комисията следва да бъдат предоставени изпълнителни правомощия: да определя формата и елементите на описа на софтуерните компоненти, да определя допълнително вида на информацията, формата и процедурата за уведомяванията относно активно използвани уязвимости и инциденти, подавани до ENISA от производителите, да определя европейските схеми за сертифициране

Изменение

(63) За да се гарантират еднакви условия за изпълнение на настоящия регламент, на Комисията следва да бъдат предоставени изпълнителни правомощия: да определя формата и елементите на описа на софтуерните компоненти, да определя допълнително вида на информацията, формата и процедурата за уведомяванията относно активно използвани уязвимости и инциденти, подавани до ENISA от производителите, **въз основа на най-добрите практики в сектора**, да

на киберсигурността, приети съгласно Регламент (ЕС) 2019/881, които могат да се използват за доказване на съответствие със съществените изисквания или части от тях, както е посочено в приложение I към настоящия регламент, да приема общи спецификации по отношение на съществените изисквания, посочени в приложение I, да определя техническите спецификации за пиктограми или всякакви други знаци, свързани със сигурността на продуктите с цифрови елементи, и механизмите за насърчаване на тяхното използване, да взема решение за корективни или ограничителни мерки на равнището на Съюза при извънредни обстоятелства, които оправдават незабавна намеса за запазване на доброто функциониране на вътрешния пазар. Тези правомощия следва да бъдат упражнявани в съответствие с Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета³⁴.

³⁴ Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета от 16 февруари 2011 г. за установяване на общите правила и принципи относно реда и условията за контрол от страна на държавите членки върху упражняването на изпълнителните правомощия от страна на Комисията (ОВ L 55, 28.2.2011 г., стр. 13).

Изменение 36

Предложение за регламент Съображение 69

Текст, предложен от Комисията

(69) На икономическите оператори следва да се предостави достатъчно

определя европейските схеми за сертифициране на киберсигурността, приети съгласно Регламент (ЕС) 2019/881, които могат да се използват за доказване на съответствие със съществените изисквания или части от тях, както е посочено в приложение I към настоящия регламент, да приема общи спецификации по отношение на съществените изисквания, посочени в приложение I, да определя техническите спецификации за пиктограми или всякакви други знаци, свързани със сигурността на продуктите с цифрови елементи, и механизмите за насърчаване на тяхното използване, да взема решение за корективни или ограничителни мерки на равнището на Съюза при извънредни обстоятелства, които оправдават незабавна намеса за запазване на доброто функциониране на вътрешния пазар. Тези правомощия следва да бъдат упражнявани в съответствие с Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета³⁴.

³⁴ Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета от 16 февруари 2011 г. за установяване на общите правила и принципи относно реда и условията за контрол от страна на държавите членки върху упражняването на изпълнителните правомощия от страна на Комисията (ОВ L 55, 28.2.2011 г., стр. 13).

Изменение

(69) На икономическите оператори следва да се предостави достатъчно

време, за да се адаптират към изискванията на настоящия регламент. Настоящият регламент следва да се прилага [24 месеца] от влизането му в сила, **с изключение на задълженията за докладване относно активно използвани уязвимости и инциденти, които следва да се прилагат [12 месеца] от влизането в сила на настоящия регламент.**

Изменение 37

Предложение за регламент Член 1 – параграф 1 – уводна част

Текст, предложен от Комисията

С настоящия регламент се определят:

време, за да се адаптират към изискванията на настоящия регламент. Настоящият регламент следва да се прилага [36 месеца] от влизането му в сила.

Изменение

Целта на настоящия регламент е да се подобри функционирането на вътрешния пазар, като същевременно се осигури високо равнище на защита на потребителите и киберсигурност.

С настоящия регламент се определят хармонизирани правила относно:

Изменение 38

Предложение за регламент Член 1 – параграф 1 – буква а

Текст, предложен от Комисията

а) ***правила за*** пускането на пазара на продукти с цифрови елементи, за да се гарантира киберсигурността на тези продукти;

Изменение

а) пускането на пазара на продукти с цифрови елементи, за да се гарантира киберсигурността на тези продукти;

Изменение 39

Предложение за регламент Член 1 – параграф 1 – буква г

Текст, предложен от Комисията

г) **правила за** надзор на пазара и правоприлагане на горепосочените правила и изисквания.

Изменение

г) надзор на пазара и правоприлагане на горепосочените правила и изисквания.

Изменение 40

Предложение за регламент Член 2 – параграф 1

Текст, предложен от Комисията

1. Настоящият регламент се прилага за всички продукти с цифрови елементи, чиято планирана или разумно предвидима употреба включва пряка или непряка логическа или физическа връзка на данни с устройство или мрежа.

Изменение

1. Настоящият регламент се прилага за всички **пуснати на пазара** продукти с цифрови елементи, чиято планирана или разумно предвидима употреба включва пряка или непряка логическа или физическа връзка на данни с **външно** устройство или мрежа.

Изменение 41

Предложение за регламент Член 2 – параграф 5 а (нов)

Текст, предложен от Комисията

Изменение

5 а. *Настоящият регламент не се прилага за свободен софтуер с отворен код, включително за неговия изходен код и модифицирани версии, освен ако софтуерът се предоставя в хода на търговска дейност чрез:*

i) начисляване на цена за продукт; или
ii) предоставяне на софтуерна платформа, зависима от други услуги, от които производителят печели; или

iii) използване на лични данни, генерирани от софтуера, по причини, различни от тези, свързани изключително с подобряване на сигурността, съвместимостта или

оперативната съвместимост на софтуера; или

iv) начисляване на цена за услуги по техническа поддръжка.

Съответствието на свободните продуктови компоненти с отворен код се осигурява от производителя на продукта, в който те са включени.

Изменение 42

Предложение за регламент Член 2 – параграф 5 б (нов)

Текст, предложен от Комисията

Изменение

5 б. Настоящият регламент не се прилага за вътрешните мрежи на продукт с цифрови елементи, ако тези мрежи имат специални крайни точки и са напълно изолирани и защитени от външна връзка на данни.

Изменение 43

Предложение за регламент Член 2 – параграф 5 в (нов)

Текст, предложен от Комисията

Изменение

5 в. Настоящият регламент не се прилага за резервни части, предназначени единствено за замяна на дефектни части на продукти с цифрови елементи с цел възстановяване на тяхната функционалност.

Изменение 44

Предложение за регламент Член 3 – параграф 1 – точка 1

Текст, предложен от Комисията

(1) „продукт с цифрови елементи“ означава всеки софтуерен или хардуерен продукт **и неговите решения за обработване на данни от разстояние**, включително софтуерни или хардуерни компоненти, които ще бъдат пуснати на пазара поотделно;

Изменение

(1) „продукт с цифрови елементи“ означава всеки софтуерен или хардуерен продукт, включително софтуерни или хардуерни компоненти, които ще бъдат пуснати на пазара поотделно;

Изменение 45

Предложение за регламент Член 3 – параграф 1 – точка 2

Текст, предложен от Комисията

(2) „**обработване на данни от разстояние**“ означава всяко обработване на данни от разстояние, за което софтуерът е проектиран и разработен от производителя или за което производителят носи отговорност и липсата на което би попречила на продукта с цифрови елементи да изпълнява една от своите функции;

Изменение

заличава се

Изменение 46

Предложение за регламент Член 3 – параграф 1 – точка 6 а (нова)

Текст, предложен от Комисията

(6 а) „софтуер с отворен код“ означава софтуер, разпространяван с лиценз, който позволява на ползвателите да го използват, копират, разпространяват, изучават, променят и подобряват свободно, както и да го интегрират като компонент в други продукти, да го предоставят като услуга или да осигуряват търговска поддръжка за

Изменение

него;

Изменение 47

Предложение за регламент

Член 3 – параграф 1 – точка 18

Текст, предложен от Комисията

(18) „производител“ означава всяко физическо или юридическо лице, което разработва или произвежда продукти с цифрови елементи или възлага проектирането, разработването или производството на продукти с цифрови елементи и ги предлага на пазара под своето име или търговска марка, независимо дали срещу заплащане или безвъзмездно;

Изменение

(Не се отнася до българския текст.)

Изменение 48

Предложение за регламент

Член 3 – параграф 1 – точка 19

Текст, предложен от Комисията

(19) „упълномощен представител“ означава всяко физическо или юридическо лице, установено в Съюза, което е упълномощено писмено от производител да действа от негово име във връзка с определени задачи;

Изменение

(19) „упълномощен представител“ означава всяко физическо или юридическо лице, установено в Съюза, което е упълномощено писмено от производител да действа от негово име във връзка с определени задачи **по отношение на задълженията на производителя**;

Изменение 49

Предложение за регламент

Член 3 – параграф 1 – точка 23 а (нова)

Текст, предложен от Комисията

Изменение

(23 а) „изземване“ означава изземване съгласно определението в член 3,

Изменение 50

Предложение за регламент Член 3 – параграф 1 – точка 26

Текст, предложен от Комисията

Изменение

(26) „разумно предвидима неправилна експлоатация“ е използването на продукт с цифрови елементи по начин, който не е в съответствие с неговата предвидена употреба, но който е възможно да е резултат от разумно предвидимо човешко поведение или от взаимодействие с други системи;

заличава се

Изменение 51

Предложение за регламент Член 3 – параграф 1 – точка 31

Текст, предложен от Комисията

Изменение

(31) „съществено изменение“ означава промяна на продукта с цифрови елементи след пускането му на пазара, която засяга съответствието на продукта с цифрови елементи със съществените изисквания, определени в приложение I, раздел 1, или води до промяна на предвидената употреба, за която е оценен продуктът с цифрови елементи;

(31) „съществено изменение“ означава промяна на продукта с цифрови елементи, с изключение на актуализациите на защитата и поддръжката, след пускането му на пазара, която засяга съответствието на продукта с цифрови елементи със съществените изисквания, определени в приложение I, раздел 1, или води до промяна на предвидената употреба, за която е оценен продуктът с цифрови елементи;

Изменение 52

Предложение за регламент Член 3 – параграф 1 – точка 39

Текст, предложен от Комисията

(39) „активно използвана уязвимост“ означава уязвимост, за която има надеждни доказателства, че е извършено изпълнение на злонамерен код от участник в система без разрешението на собственика на системата;

Изменение

(39) „активно използвана уязвимост“ означава **коригирана** уязвимост, за която има надеждни доказателства, че е извършено изпълнение на злонамерен код от участник в система без разрешението на собственика на системата;

Изменение 53

Предложение за регламент

Член 3 – параграф 1 – точка 40 а (нова)

Текст, предложен от Комисията

Изменение

(40 а) „частично комплектовани продукти с цифрови елементи“ означава материално изделие, което не е в състояние да функционира самостоятелно и което е произведено единствено с цел да бъде включено или сглобено в продукт с цифрови елементи или друг частично комплектован продукт с цифрови елементи и чието съответствие може да бъде ефективно оценено единствено като се вземе предвид начинът, по който е включено в предвидения краен продукт с цифрови елементи;

Изменение 54

Предложение за регламент

Член 3 – параграф 1 – точка 40 б (нова)

Текст, предложен от Комисията

Изменение

(40 б) „жизнен цикъл“ означава периода от момента, в който продукт, попадащ в обхвата на настоящия регламент, е пуснат на пазара или въведен в експлоатация, до

момента, в който бъде изхвърлен, включително ефективното време, когато може да бъде използван, и етапите на транспортиране, монтаж, демонтаж, извеждане от експлоатация, бракуване или други физически или софтуерни промени, предвидени от производителя.

Изменение 55

Предложение за регламент Член 4 – параграф 1

Текст, предложен от Комисията

1. Държавите членки не възпрепятстват по отношение на областите, обхванати от настоящия регламент, предоставянето на пазара на продукти с цифрови елементи, които отговарят на изискванията на настоящия регламент.

Изменение

1. Държавите членки не възпрепятстват по отношение на областите, обхванати от настоящия регламент, предоставянето на пазара на продукти с цифрови елементи **или на частично комплектовани продукти с цифрови елементи**, които отговарят на изискванията на настоящия регламент.

Изменение 56

Предложение за регламент Член 4 – параграф 2

Текст, предложен от Комисията

2. По време на търговски панаири, изложения и демонстрации или други подобни събития държавите членки не възпрепятстват представянето и използването на даден продукт с цифрови елементи, който не отговаря на изискванията на настоящия регламент.

Изменение

2. По време на търговски панаири, изложения и демонстрации или други подобни събития държавите членки не възпрепятстват представянето и използването на даден продукт с цифрови елементи, **прототип на даден продукт с цифрови елементи или частично комплектован продукт с цифрови елементи**, който не отговаря на изискванията **на настоящия регламент, при условие че продуктът с цифрови елементи се използва изключително за целите на представянето в хода на събитието и**

*че видим знак ясно показва, че
въпросният продукт не съответства
на настоящия регламент.*

Изменение 57

Предложение за регламент Член 4 – параграф 3

Текст, предложен от Комисията

3. Държавите членки не възпрепятстват предоставянето на незавършен *софтуер*, който не съответства на настоящия регламент, при условие че *софтуерът* се предоставя само **за ограничен период от време, необходим** за целите на изпитването, и че видим знак ясно показва, че той не съответства на настоящия регламент и няма да се предоставя на пазара за цели, различни от тестване.

Изменение

3. Държавите членки не възпрепятстват предоставянето на незавършен *продукт с цифрови елементи или прототип на продукт с цифрови елементи*, който не съответства на настоящия регламент, при условие че *той* се предоставя само **в непроизводствена версия** за целите на изпитването, и че видим знак ясно показва, че той не съответства на настоящия регламент и няма да се предоставя на пазара за цели, различни от тестване.

Изменение 58

Предложение за регламент Член 4 – параграф 3 а (нов)

Текст, предложен от Комисията

Изменение

3 а. Настоящият регламент не възпрепятства държавите членки да прилагат допълнителни мерки по отношение на продуктите с цифрови елементи, когато тези конкретни продукти ще бъдат използвани за военни цели, за цели в областта на отбраната или за цели в областта на националната сигурност в съответствие с националното законодателство и правото на Съюза и такива мерки са необходими и пропорционални за постигането на въпросните цели.

Изменение 59

Предложение за регламент Член 5 – параграф 1 – точка 1

Текст, предложен от Комисията

(1) при правилно инсталиране, извършване на техническа поддръжка и използване по предназначение или при разумно предвидими условия, и, когато е приложимо, **актуализиране**, отговарят на съществените изисквания, посочени в приложение I, раздел 1; и

Изменение

(1) при правилно инсталиране, извършване на техническа поддръжка и използване по предназначение или при разумно предвидими условия, и, когато е приложимо, **предоставяне на необходимите актуализации на защитата**, отговарят на съществените изисквания, посочени в приложение I, раздел 1; и

Изменение 60

Предложение за регламент Член 6 – параграф 1

Текст, предложен от Комисията

1. Продуктите с цифрови елементи, които принадлежат към категория, посочена в приложение III, се считат за критични продукти с цифрови елементи. Счита се, че продуктите, които притежават основните функционални възможности на категория, която е посочена в приложение III към настоящия регламент, попадат в тази категория. Категориите критични продукти с цифрови елементи се разделят на клас I и клас II, както е посочено в приложение III, като отразяват нивото на киберриска, свързан с тези продукти.

Изменение

1. Продуктите с цифрови елементи, които принадлежат към категория, посочена в приложение III, се считат за критични продукти с цифрови елементи. Счита се, че **само** продуктите, които притежават основните функционални възможности на категория, която е посочена в приложение III към настоящия регламент, попадат в тази категория. Категориите критични продукти с цифрови елементи се разделят на клас I и клас II, както е посочено в приложение III, като отразяват нивото на киберриска, свързан с тези продукти.

Интегрирането на компонент с по-висока степен на критичност в продукт с по-ниска степен на критичност не променя задължително нивото на критичност за продукта, в който е

Изменение 61

Предложение за регламент Член 6 – параграф 2 – буква б

Текст, предложен от Комисията

б) предвидената употреба в чувствителна среда, **включително** в **промишлени условия** или от основни субекти от вида, посочен в приложение [приложение I] към Директива [Директива XXX/XXXX (МИС 2)];

Изменение

б) предвидената употреба в **критични приложения** в чувствителна среда или от основни субекти от вида, посочен в приложение [приложение I] към Директива [Директива XXX/XXXX (МИС 2)];

Изменение 62

Предложение за регламент Член 6 – параграф 2 – буква в

Текст, предложен от Комисията

в) предвидената употреба за изпълнение на критични или чувствителни функции, като например обработване на лични данни;

Изменение

в) предвидената употреба **и мащаба** за изпълнение на критични или чувствителни функции, като например обработване на лични данни;

Изменение 63

Предложение за регламент Член 6 – параграф 4

Текст, предложен от Комисията

4. Критичните продукти с цифрови елементи подлежат на процедурите за оценяване на съответствието, посочени в член 24, параграфи 2 и 3.

Изменение

4. Критичните продукти с цифрови елементи подлежат на процедурите за оценяване на съответствието, посочени в член 24, параграфи 2 и 3. **По изключение малките и микропредприятията могат да използват процедурата, посочена в член 24, параграф 2.**

Изменение 64

Предложение за регламент Член 6 – параграф 5 – уводна част

Текст, предложен от Комисията

5. Комисията има правомощието да приема делегирани актове в съответствие с член 50 за допълване на настоящия регламент чрез определяне на категориите продукти с цифрови елементи с висока степен на критичност, за които *от* производителите *се изисква* да получат европейски сертификат за киберсигурност в съответствие с европейска схема за сертифициране на киберсигурността съгласно Регламент (ЕС) 2019/881, за да докажат съответствието си със съществените изисквания, посочени в приложение I, или с части от него. При определянето на такива категории продукти с цифрови елементи с висока степен на критичност Комисията взема предвид нивото на киберриска, свързан с категорията продукти с цифрови елементи, като се отчитат един или няколко от критериите, посочени в параграф 2, както и с оглед на оценката дали тази категория продукти:

Изменение

5. Комисията има правомощието да приема делегирани актове в съответствие с член 50 за допълване на настоящия регламент чрез определяне на категориите продукти с цифрови елементи с висока степен на критичност, за които производителите *могат* да получат европейски сертификат за киберсигурност в съответствие с европейска схема за сертифициране на киберсигурността съгласно Регламент (ЕС) 2019/881, за да докажат съответствието си със съществените изисквания, посочени в приложение I, или с части от него. При определянето на такива категории продукти с цифрови елементи с висока степен на критичност Комисията взема предвид нивото на киберриска, свързан с категорията продукти с цифрови елементи, като се отчитат един или няколко от критериите, посочени в параграф 2, както и с оглед на оценката дали тази категория продукти:

Изменение 65

Предложение за регламент Член 8 – параграф 1

Текст, предложен от Комисията

1. Продукти с цифрови елементи, класифицирани като високорискови системи с ИИ в съответствие с член [член 6] от Регламент [Регламента относно ИИ], които попадат в обхвата на настоящия регламент и отговарят на съществените изисквания, посочени в раздел 1 от приложение I към

Изменение

1. **Продукти с цифрови елементи или частично комплектовани** продукти с цифрови елементи, класифицирани като високорискови системи с ИИ в съответствие с член [член 6] от Регламент [Регламента относно ИИ], които попадат в обхвата на настоящия регламент и отговарят на

настоящия регламент, и при които въведените от производителя процеси са в съответствие със съществените изисквания, посочени в приложение I, раздел 2, се считат за съответстващи на изискванията, свързани с киберсигурността, посочени в член [член 15] от Регламент [Регламента относно ИИ], без да се засягат другите изисквания, свързани с точността и надеждността, включени в посочения член, и доколкото постигането на нивото на защита, наложено от тези изисквания, е доказано с ЕС декларацията за съответствие, издадена съгласно настоящия регламент.

съществените изисквания, посочени в раздел 1 от приложение I към настоящия регламент, и при които въведените от производителя процеси са в съответствие със съществените изисквания, посочени в приложение I, раздел 2, се считат за съответстващи на изискванията, свързани с киберсигурността, посочени в член [член 15] от Регламент [Регламента относно ИИ], без да се засягат другите изисквания, свързани с точността и надеждността, включени в посочения член, и доколкото постигането на нивото на защита, наложено от тези изисквания, е доказано с ЕС декларацията за съответствие, издадена съгласно настоящия регламент.

Изменение 66

Предложение за регламент Член 8 – параграф 2

Текст, предложен от Комисията

2. По отношение на продуктите и изискванията за киберсигурност, посочени в параграф 1, се прилага съответната процедура за оценяване на съответствието съгласно изискванията на **член [член 43]** от Регламент [Регламент относно ИИ]. За целите на това оценяване нотифицираните органи, които имат право да проверяват съответствието на високорисковите системи с ИИ съгласно Регламента [Регламент относно ИИ], имат право също така да проверяват съответствието на високорисковите системи с ИИ в обхвата на настоящия регламент с изискванията, посочени в приложение I към настоящия регламент, **при условие че съответствието на тези нотифицирани органи с изискванията, определени в член 29 от настоящия регламент, е било оценено в контекста на процедурата**

Изменение

2. По отношение на продуктите и изискванията за киберсигурност, посочени в параграф 1, се прилага съответната процедура за оценяване на съответствието съгласно изискванията на **[приложимите разпоредби]** от Регламент [Регламент относно ИИ]. За целите на това оценяване нотифицираните органи, които имат право да проверяват съответствието на високорисковите системи с ИИ съгласно Регламента [Регламент относно ИИ], имат право също така да проверяват съответствието на високорисковите системи с ИИ в обхвата на настоящия регламент с изискванията, посочени в приложение I към настоящия регламент.

за нотифициране съгласно Регламент
[Регламент относно ИИ].

Изменение 67

Предложение за регламент Член 8 – параграф 3

Текст, предложен от Комисията

Изменение

3. Като изключение от параграф 2, критичните продукти с цифрови елементи, изброени в приложение III към настоящия регламент, за които трябва да се прилагат процедурите за оценяване на съответствието, посочени в член 24, параграф 2, букви а) и б), член 24, параграф 3, букви а) и б) съгласно настоящия регламент, и които също така са класифицирани като високорискови системи с ИИ по член [член 6] от Регламента [Регламент относно ИИ] и за които се прилага процедурата за оценяване на съответствието, основана на вътрешен контрол, посочена в приложение [приложение VI] към Регламент [Регламента относно ИИ], подлежат на процедурите за оценяване на съответствието, изисквани от настоящия регламент, доколкото това се отнася до съществените изисквания на настоящия регламент.

заличава се

Изменение 68

Предложение за регламент Член 9 – параграф 1

Текст, предложен от Комисията

Изменение

Машиностроителните изделия в обхвата на Регламент [Предложение за регламент за машините], които са продукти с цифрови елементи по

Машиностроителните изделия в обхвата на Регламент [Предложение за регламент за машините], които са продукти с цифрови елементи *или*

смисъла на настоящия регламент и за които е издадена ЕС декларация за съответствие въз основа на настоящия регламент, се считат за съответстващи на съществените изисквания за здраве и безопасност, определени в приложение [приложение III, раздели 1.1.9 и 1.2.1] към Регламент [Предложение за регламент за машините], по отношение на защитата срещу корупция и безопасността и надеждността на системите за управление, и доколкото постигането на нивото на защита, наложено от тези изисквания, е доказано в ЕС декларацията за съответствие, издадена съгласно настоящия регламент.

частично комплектовани продукти с цифрови елементи по смисъла на настоящия регламент и за които е издадена ЕС декларация за съответствие въз основа на настоящия регламент, се считат за съответстващи на съществените изисквания за здраве и безопасност, определени в приложение [приложение III, раздели 1.1.9 и 1.2.1] към Регламент [Предложение за регламент за машините], по отношение на защитата срещу корупция и безопасността и надеждността на системите за управление, и доколкото постигането на нивото на защита, наложено от тези изисквания, е доказано в ЕС декларацията за съответствие, издадена съгласно настоящия регламент.

Изменение 69

Предложение за регламент Член 10 – параграф -1 (нов)

Текст, предложен от Комисията

Изменение

-1. Производителите на софтуер, които се класифицират като микропредприятие съгласно определението в Препоръка 2003/361/ЕО на Комисията, полагат максимални усилия, за да изпълнят изискванията на настоящия регламент през 6-те месеца след пускането на софтуера на пазара. Тази разпоредба не се прилага за продуктите с цифрови елементи с висока степен на критичност.

Изменение 70

Предложение за регламент Член 10 – параграф 1

Текст, предложен от Комисията

1. Когато пускат на пазара даден продукт с цифрови елементи, производителите гарантират, че той е проектиран, разработен и **изработен** в съответствие със съществените изисквания, посочени в приложение I, раздел 1.

Изменение

1. Когато пускат на пазара даден продукт с цифрови елементи, производителите гарантират, че той е проектиран, разработен и **произведен** в съответствие със съществените изисквания, посочени в приложение I, раздел 1.

Изменение 71

Предложение за регламент Член 10 – параграф 4

Текст, предложен от Комисията

4. С оглед спазването на задължението, посочено в параграф 1, производителите полагат дължимата грижа, когато интегрират компоненти, доставени от трети страни, в продукти с цифрови елементи. **Те гарантират**, че тези компоненти не застрашават сигурността на продукта с цифрови елементи.

Изменение

4. С оглед спазването на задължението, посочено в параграф 1, производителите полагат дължимата грижа, когато интегрират компоненти, доставени от трети страни, в продукти с цифрови елементи. **Производителят е длъжен да гарантира**, че тези компоненти не застрашават сигурността на продукта с цифрови елементи.

Изменение 72

Предложение за регламент Член 10 – параграф 4 а (нов)

Текст, предложен от Комисията

Изменение

4 а. Производителите на компоненти предоставят информацията и документите, необходими за спазване на изискванията на настоящия регламент, когато доставят такива компоненти на производителя на крайните продукти. Тази информация се предоставя безплатно.

Изменение 73

Предложение за регламент Член 10 – параграф 6 – алинея 1

Текст, предложен от Комисията

При пускането на даден продукт с цифрови елементи на пазара и за очаквания експлоатационен срок на продукта или за период от пет години от пускането на продукта на пазара, в зависимост от това кой период е **по-кратък**, производителите гарантират, че уязвимостите на този продукт се отстраняват ефективно и в съответствие със съществените изисквания, посочени в приложение I, раздел 2.

Изменение

При пускането на даден продукт с цифрови елементи на пазара и за очаквания експлоатационен срок на продукта **към момента на пускането на продукта на пазара** или за период от пет години от пускането на продукта на пазара, в зависимост от това кой период е **по-дълъг**, производителите гарантират, че уязвимостите на този продукт се отстраняват ефективно и в съответствие със съществените изисквания, посочени в приложение I, раздел 2, **при условие че това се контролира от производителя.**

Изменение 74

Предложение за регламент Член 10 – параграф 10 – алинея 3 а (нова)

Текст, предложен от Комисията

Изменение

Когато се правят актуализации на софтуера, от производителя не се изисква да извършва друга оценка на съответствието на продукта с цифрови елементи, освен ако актуализацията на софтуера води до съществено изменение на продукта с цифрови елементи по смисъла на член 3, параграф 31 от настоящия регламент.

Изменение 75

Предложение за регламент Член 10 – параграф 9

Текст, предложен от Комисията

9. Производителите гарантират, че съществуват процедури, чрез които продуктите с цифрови елементи, които са обект на серийно производство, остават в съответствие. Производителят взема предвид по подходящ начин промените в процеса на разработване и производство или в проектирането или характеристиките на продукта с цифрови елементи, както и промените в хармонизираните стандарти, европейските схеми за сертифициране на киберсигурността или общите спецификации, посочени в член 19, чрез позоваване на които се декларира съответствието на продукта с цифрови елементи или чрез прилагане на които се проверява неговото съответствие.

Изменение

9. Производителите гарантират, че съществуват процедури, чрез които продуктите с цифрови елементи, които са обект на серийно производство, остават в съответствие. Производителят взема предвид по подходящ начин промените в процеса на разработване и производство или в проектирането или характеристиките на продукта с цифрови елементи, както и промените в хармонизираните стандарти, европейските схеми за сертифициране на киберсигурността или общите спецификации, посочени в член 19, чрез позоваване на които се декларира съответствието на продукта с цифрови елементи или чрез прилагане на които се проверява неговото съответствие.

Когато се появят нови знания, техники или стандарти, които не са били налични по време на проектирането на сериен продукт, производителят може да предвиди периодичното въвеждане на такива подобрения за бъдещите поколения продукти.

Изменение 76

Предложение за регламент Член 10 – параграф 9 а (нов)

Текст, предложен от Комисията

Изменение

9 а. Производителите съобщават публично какъв е очакваният експлоатационен срок на техните продукти по ясен и разбираем начин.

Изменение 77

Предложение за регламент Член 10 – параграф 12

Текст, предложен от Комисията

12. От пускането на пазара и за очаквания експлоатационен срок на даден продукт или за период от пет години от пускането на продукта на пазара, в зависимост от това кой период е **по-кратък**, производителите, които знаят или имат основание да смятат, че продуктът с цифрови елементи или въведените от производителя процеси не са в съответствие със съществените изисквания, определени в приложение I, незабавно предприемат необходимите корективни мерки, за да приведат продукта с цифрови елементи или процесите на производителя в съответствие с изискванията, да изтеглят или да изземат продукта, според случая.

Изменение 78

Предложение за регламент Член 11 – параграф 1

Текст, предложен от Комисията

1. Производителят уведомява ENISA за всяка активно използвана уязвимост, съдържаща се в продукта с цифрови елементи, без неоправдано забавяне и във всички случаи в рамките на **24** часа от узнаването ѝ.
Уведомлението включва подробности относно тази уязвимост и, когато е приложимо, всички предприети корективни или смекчаващи мерки. Без неоправдано забавяне, освен ако не са налице основателни причини, свързани с киберриска, ENISA препраща уведомлението до ЕРИКС, определен за целите на координираното оповестяване на уязвимости в съответствие с член [член X] от Директива [Директива XXX/XXXX (МИС 2)], на

PE742.490v02-00

Изменение

12. От пускането на пазара и за очаквания експлоатационен срок на даден продукт или за период от пет години от пускането на продукта на пазара, в зависимост от това кой период е **по-дълъг**, производителите, които знаят или имат основание да смятат, че продуктът с цифрови елементи или въведените от производителя процеси не са в съответствие със съществените изисквания, определени в приложение I, незабавно предприемат необходимите корективни мерки, за да приведат продукта с цифрови елементи или процесите на производителя в съответствие с изискванията, да изтеглят или да изземат продукта, според случая.

Изменение

1. Производителят уведомява ENISA **чрез ранно предупреждение** за всяка активно използвана уязвимост, съдържаща се в продукта с цифрови елементи, без неоправдано забавяне и във всички случаи в рамките на **48** часа от узнаването ѝ.

56/115

AD\1280305BG.docx

съответните държави членки след получаването му и информира органа за надзор на пазара за съобщената уязвимост.

Изменение 79

Предложение за регламент Член 11 – параграф 1 а (нов)

Текст, предложен от Комисията

Изменение

1 а. След узнаването за активно използвана уязвимост, оказваща значително въздействие върху сигурността на продукта с цифрови елементи, производителят съобщава без неоправдано забавяне на ENISA допълнителни подробности относно използваната уязвимост.

Изменение 80

Предложение за регламент Член 11 – параграф 1 б (нов)

Текст, предложен от Комисията

Изменение

1 б. След като бъде решен проблемът с уязвимостта, ENISA трябва да бъде уведомена за всички други уязвимости, които не оказват значително въздействие върху сигурността на продукта с цифрови елементи.

Изменение 81

Предложение за регламент Член 11 – параграф 1 в (нов)

Текст, предложен от Комисията

Изменение

1 в. Уведомлението включва подробности относно тази уязвимост

и когато е приложимо, всички предприети корективни или смекчаващи мерки, както и препоръчаните мерки за намаляване на риска. Без неоправдано забавяне, освен ако са налице основателни причини, свързани с киберриска, ENISA препраща уведомлението до ЕРИКС, определен за целите на координираното оповестяване на уязвимости в съответствие с член [член X] от Директива [Директива XXX/XXXX (МИС 2)], на съответните държави членки след получаването му и незабавно информира органа за надзор на пазара за наличието на уязвимост и когато е приложимо, за потенциалните мерки за намаляване на риска. Когато за съобщената уязвимост няма налични корективни или смекчаващи мерки, ENISA гарантира, че информацията за тази съобщена уязвимост се споделя в съответствие със строги протоколи за сигурност и въз основа на принципа „необходимост да се знае“.

Изменение 82

Предложение за регламент Член 11 – параграф 2

Текст, предложен от Комисията

2. Производителят уведомява ENISA за всеки инцидент, който оказва въздействие върху сигурността на продукта с цифрови елементи, без неоправдано забавяне и във всички случаи в рамките на 24 часа от узнаването му. Без неоправдано забавяне, освен ако **не** са налице основателни причини, свързани с киберриска, ENISA препраща уведомлението до единното звено за контакт, определено **за целите на координираното оповестяване на**

Изменение

2. Производителят уведомява **чрез ранно предупреждение** ENISA за всеки инцидент, който оказва **значително** въздействие върху сигурността на продукта с цифрови елементи, без неоправдано забавяне и във всички случаи в рамките на 24 часа от узнаването му. **Освен това производителят предоставя на ENISA повече подробности относно значителния инцидент, свързан с продукта с цифрови елементи, без неоправдано забавяне и във всички**

уязвимости в съответствие с член [член X] от Директива [Директива XXX/XXXX (МИС 2)], на съответните държави членки **след получаването му** и информира органа за надзор на пазара за съобщените инциденти. Уведомлението за инцидент включва информация за сериозността и въздействието на инцидента и, когато е приложимо, посочва дали производителят подозира, че инцидентът е причинен от незаконни или злонамерени действия, или смята, че той има трансгранично въздействие.

случаи в рамките на 72 часа след узнаването за този значителен инцидент. Без неоправдано забавяне, освен ако са налице основателни причини, свързани с киберриска, ENISA препраща уведомлението до единното звено за контакт, определено в съответствие с член [член X] от Директива [Директива XXX/XXXX (МИС 2)], на съответните държави членки и **незабавно** информира органа за надзор на пазара за съобщените **значителни** инциденти. Уведомлението за инцидент включва информация, **която е строго необходима, за да се осведоми компетентният орган за инцидента и ако е целесъобразно и пропорционално на риска,** за сериозността и въздействието на инцидента, и когато е приложимо, посочва дали производителят подозира, че инцидентът е причинен от незаконни или злонамерени действия, или смята, че той има трансгранично въздействие. **Актът на уведомяване сам по себе си не води до повишена отговорност за уведомяващия субект.**

Изменение 83

Предложение за регламент Член 11 – параграф 2 а (нов)

Текст, предложен от Комисията

Изменение

2 а. Икономическите оператори, които са определени също така като съществени или важни субекти съгласно МИС 2 и които подават своето уведомление за инцидент съгласно МИС 2, следва да се считат за отговарящи на изискванията по точка 2 от настоящия член.

Изменение 84

Предложение за регламент
Член 11 – параграф 3

Текст, предложен от Комисията

3. ENISA предоставя на европейската мрежа за връзка на организациите при кибернетични кризи (EU-CyCLONe), създадена по силата на член [член X] от Директива [Директива XXX/XXXX (МИС 2)], информацията, съобщена по параграфи 1 и 2, ако тази информация е от значение за координираното управление на мащабни киберинциденти и кризи на оперативно равнище.

Изменение

3. ENISA предоставя на европейската мрежа за връзка на организациите при кибернетични кризи (EU-CyCLONe), създадена по силата на член [член X] от Директива [Директива XXX/XXXX (МИС 2)], информацията, съобщена по параграфи 1 и 2, ако тази информация е от значение за координираното управление на мащабни **и значителни** киберинциденти и кризи на оперативно равнище.

Изменение 85

Предложение за регламент
Член 11 – параграф 4

Текст, предложен от Комисията

4. Без неоправдано забавяне и след като е узнал за него, производителят информира ползвателите на продукта с цифрови елементи за **инцидента** и, когато е необходимо, за **корективните** мерки, които ползвателят може да приложи, за да намали въздействието на **инцидента**.

Изменение

4. Без неоправдано забавяне и след като е узнал за него, производителят информира ползвателите на продукта с цифрови елементи за **значителния инцидент, ако е целесъобразно и има вероятност те да бъдат неблагоприятно засегнати от този инцидент, и** когато е необходимо, за **намаляването на риска и за всички корективни** мерки, които ползвателят може да приложи, за да намали въздействието на **значителния инцидент по отношение на данните, които може да са засегнати, и потенциалните вреди**.

Изменение 86

Предложение за регламент
Член 11 – параграф 4 а (нов)

Текст, предложен от Комисията

Изменение

4 а. *Задълженията, определени в параграфи 1, 2 и 4, се прилагат по време на експлоатационния срок на продукта. По време на очаквания експлоатационен срок на продукта производителят предоставя безплатно актуализации на защитата, които се прилагат само за продукти с цифрови елементи, за които производителят е изготвил ЕС декларация за съответствие съгласно член 20 от настоящия регламент.*

Изменение 87

Предложение за регламент Член 11 – параграф 5

Текст, предложен от Комисията

Изменение

5. Чрез приемане на актове за изпълнение Комисията може да определи допълнително вида на информацията, формата и процедурата на уведомяването, подавани съгласно параграфи 1 и 2. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 51, параграф 2.

5. Чрез приемане на актове за изпълнение Комисията може да определи допълнително вида на информацията, формата и процедурата на уведомяването, подавани съгласно параграфи 1 и 2, **след като се консултира със заинтересованите страни и ЕРИКС**. Тези актове за изпълнение **вземат под внимание европейските и международните стандарти** и се приемат в съответствие с процедурата по разглеждане, посочена в член 51, параграф 2.

Изменение 88

Предложение за регламент Член 11 – параграф 6

Текст, предложен от Комисията

Изменение

6. Въз основа на уведомяването, получени по параграфи 1 и 2, ENISA

6. Въз основа на уведомяването, получени по параграфи 1 и 2, ENISA

изготвя двугодишен технически доклад за нововъзникващите тенденции по отношение на киберрисковете в продуктите с цифрови елементи и го представя на групата за сътрудничество за МИС, посочена в член *[член X]* от Директива *[Директива XXX/XXXX (МИС 2)]*. Първият такъв доклад се представя в срок от 24 месеца след началото на прилагане на задълженията, посочени в параграфи 1 и 2.

изготвя двугодишен технически доклад за нововъзникващите тенденции по отношение на киберрисковете в продуктите с цифрови елементи и го представя на групата за сътрудничество за МИС, посочена в член *14* от Директива *(ЕС) 2022/2555*. Първият такъв доклад се представя в срок от 24 месеца след началото на прилагане на задълженията, посочени в параграфи 1 и 2.

Изменение 89

Предложение за регламент Член 11 – параграф 7

Текст, предложен от Комисията

7. При установяване на уязвимост в компонент, включително в компонент с отворен код, който е интегриран в продукта с цифрови елементи, производителите докладват за уязвимостта на лицето или субекта, който поддържа компонента.

Изменение

7. При установяване на уязвимост в компонент, включително в компонент с отворен код, който е интегриран в продукта с цифрови елементи, производителите докладват за уязвимостта **и за предприетите корективни или смекчаващи мерки** на лицето или субекта, който поддържа компонента. **Това не освобождава производителя от задължението да поддържа продукта в съответствие с изискванията на настоящия регламент, нито създава задължения за разработчиците на свободни компоненти с отворен код, които нямат договорни отношения с въпросния производител.**

Изменение 90

Предложение за регламент Член 12 – параграф 3 – уводна част

Текст, предложен от Комисията

3. Упълномощеният представител

Изменение

3. Упълномощеният представител

изпълнява задачите, определени в пълномощието от страна на производителя. Пълномощието позволява на упълномощения представител да извършва най-малко следното:

изпълнява задачите, определени в пълномощието от страна на производителя. **Той предоставя на органите за надзор на пазара копие от пълномощието при поискване.** Пълномощието позволява на упълномощения представител да извършва най-малко следното:

Изменение 91

Предложение за регламент Член 12 – параграф 3 – буква а а (нова)

Текст, предложен от Комисията

Изменение

(а а) когато упълномощеният представител има основание да счита, че даден продукт с цифрови елементи представлява киберриск, той информира производителя;

Изменение 92

Предложение за регламент Член 12 – параграф 3 – буква б

Текст, предложен от Комисията

Изменение

б) при мотивирано искане от страна на орган за надзор на пазара да предоставя на този орган цялата информация и документация, необходима за доказване на съответствието на даден продукт с цифрови елементи;

б) при мотивирано искане от страна на орган за надзор на пазара да предоставя на този орган цялата информация и документация, необходима за доказване на **безопасността и** съответствието на даден продукт с цифрови елементи, **на език, който е лесно разбираем за този орган;**

Изменение 93

Предложение за регламент Член 12 – параграф 3 – буква в

Текст, предложен от Комисията

в) да сътрудничи на органите за надзор на пазара, по тяхно искане, при всяко действие, предприето за отстраняване на рисковете, свързани с продукти с цифрови елементи, обхванати от пълномощието на упълномощения представител.

Изменение

в) да сътрудничи на органите за надзор на пазара, по тяхно искане, при всяко действие, предприето за **ефективно** отстраняване на рисковете, свързани с продукти с цифрови елементи, обхванати от пълномощието на упълномощения представител.

Изменение 94

Предложение за регламент

Член 13 – параграф 2 – буква в а (нова)

Текст, предложен от Комисията

Изменение

(в а) всички документи, доказващи изпълнението на изискванията, посочени в настоящия член, са получени от производителя и са на разположение за проверка за период от 10 години.

Изменение 95

Предложение за регламент

Член 13 – параграф 3

Текст, предложен от Комисията

Изменение

3. Когато вносител счита или има основание да счита, че продукт с цифрови елементи или процесите, въведени от производителя, не са в съответствие със съществените изисквания, посочени в приложение I, вносителят не пуска продукта на пазара, докато този продукт или процесите, въведени от производителя, не бъдат приведени в съответствие със съществените изисквания, посочени в приложение I. Освен това, когато продуктът с цифрови елементи

3. Когато вносител счита или има основание да счита, **въз основа на информацията, с която разполага**, че продукт с цифрови елементи или процесите, въведени от производителя, не са в съответствие със съществените изисквания, посочени в приложение I, вносителят не пуска продукта на пазара, докато този продукт или процесите, въведени от производителя, не бъдат приведени в съответствие със съществените изисквания, посочени в приложение I. Освен това, когато

представлява значителен киберриск, вносителят информира за това производителя и органите за надзор на пазара.

продуктът с цифрови елементи представлява значителен киберриск, вносителят информира за това производителя и органите за надзор на пазара.

Изменение 96

Предложение за регламент Член 13 – параграф 4

Текст, предложен от Комисията

4. Вносителите посочват своето име, **регистрирано** търговско наименование или **регистрирана** търговска марка, пощенския адрес и адреса на електронна поща, на който може да се осъществи връзка с тях, върху продукта с цифрови елементи, или, когато това не е възможно, върху неговата опаковка, или в документ, който придружава продукта с цифрови елементи. Данните за връзка са на език, лесноразбираем за ползвателите и органите за надзор на пазара.

Изменение

4. Вносителите посочват своето име, **регистрираното си** търговско наименование или **регистрираната си** търговска марка, пощенския **си** адрес и адреса на електронна поща, на който може да се осъществи връзка с тях, върху продукта с цифрови елементи, или, когато това не е възможно, върху неговата опаковка, или в документ, който придружава продукта с цифрови елементи. Данните за връзка са на език, лесноразбираем за ползвателите и органите за надзор на пазара.

Изменение 97

Предложение за регламент Член 13 – параграф 6 – алинея 1

Текст, предложен от Комисията

Вносителите, които знаят или имат основание да смятат, че продукт с цифрови елементи, който са пуснали на пазара, или процесите, въведени от неговия производител, не са в съответствие със съществените изисквания, посочени в приложение I, незабавно предприемат необходимите корективни мерки за привеждане на продукта с цифрови елементи или на процесите, въведени от неговия производител, в съответствие със

Изменение

Вносителите, които знаят или имат основание да смятат, че продукт с цифрови елементи, който са пуснали на пазара, или процесите, въведени от неговия производител, не са в съответствие със съществените изисквания, посочени в приложение I, незабавно предприемат необходимите корективни мерки за привеждане на продукта с цифрови елементи или на процесите, въведени от неговия производител, в съответствие със

съществените изисквания, посочени в приложение I, или за изтегляне или изземване на продукта, ако е целесъобразно.

съществените изисквания, посочени в приложение I, или за изтегляне или изземване на продукта, ако е целесъобразно. **Въз основа на оценката на риска дистрибуторите и крайните ползватели трябва да бъдат своевременно информирани за липсата на съответствие и за мерките за намаляване на риска, които могат да предприемат.**

Изменение 98

Предложение за регламент Член 14 – параграф 2 – буква б а (нова)

Текст, предложен от Комисията

Изменение

б а) са получили от производителя или вносителя цялата информация и документация, изисквана съгласно настоящия регламент.

Изменение 99

Предложение за регламент Член 16 – параграф 1

Текст, предложен от Комисията

Изменение

Физическо или юридическо лице, различно от производителя, вносителя или дистрибутора, което извършва съществено изменение на продукта с цифрови елементи, се счита за производител за целите на настоящия регламент.

Физическо или юридическо лице, различно от производителя, вносителя или дистрибутора, което извършва **в рамките на професионалната си дейност** съществено изменение на продукта с цифрови елементи **и предоставя продукта на пазара**, се счита за производител за целите на настоящия регламент.

Изменение 100

Предложение за регламент Член 18 – параграф 1 а (нов)

Текст, предложен от Комисията

Изменение

1 а. Съгласно предвиденото в член 10, параграф 1 от Регламент (ЕС) 1025/2012 Комисията изисква от една или повече европейски организации за стандартизация да изготвят хармонизирани стандарти за изискванията, определени в приложение I.

Изменение 101

**Предложение за регламент
Член 18 – параграф 4 а (нов)**

Текст, предложен от Комисията

Изменение

4 а. В съответствие с член 10, параграф 1 от Регламент 1025/2012 при изготвянето на искането за стандартизация за продукти, попадащи в обхвата на настоящия регламент, Комисията се стреми към максимална хармонизация с международните стандарти за киберсигурност, които са действащи или предстои да бъдат приети. През първите три години след датата на прилагане на настоящия регламент Комисията разполага с правомощието да обявява действащи международни стандарти за отговарящи на изискванията на настоящия регламент без никакви европейски изменения, при условие че спазването на тези стандарти повишава в достатъчна степен сигурността на продуктите с цифрови елементи и че те са публикувани като отделна версия от една от европейските организации за стандартизация.

Изменение 102

Предложение за регламент
Член 19 – параграф 1

Текст, предложен от Комисията

Когато не съществуват хармонизирани стандарти като посочените в член 18, или когато Комисията прецени, че съответните хармонизирани стандарти са недостатъчни, за да изпълнят изискванията на настоящия регламент или да отговорят на искането на Комисията за стандартизация, или когато има неоправдани забавяния в процедурата по стандартизация, или когато искането на Комисията за хармонизирани стандарти не е било прието от европейските организации за стандартизация, Комисията има правомощието чрез актове за изпълнение да приема общи спецификации по отношение на съществените изисквания, посочени в приложение I. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 51, параграф 2.

Изменение

1. Комисията може да приема актове за изпълнение за установяване на общи спецификации, обхващащи технически изисквания, които осигуряват средства за постигане на съответствие със съществените изисквания по отношение на здравето и безопасността, установени в приложение I за продуктите, попадащи в обхвата на настоящия регламент. Тези актове за изпълнение се приемат само когато са изпълнени следните условия:

а) съгласно предвиденото в член 10, параграф 1 от Регламент (ЕС) № 1025/2012 Комисията е изискала от една или повече европейски организации за стандартизация да изготвят хармонизиран стандарт за съществените изисквания, посочени в приложение I, както и:

i) искането не е било прието; или

ii) хармонизираните стандарти, отговарящи на това искане, не са представени в срока, определен в съответствие с член 10, параграф 1 от Регламент (ЕС) 1025/2012; или

iii) хармонизираните стандарти не са в съответствие с искането;

както и

б) в Официален вестник на Европейския съюз не са публикувани данни за хармонизирани стандарти, обхващащи посочените в приложение I изисквания, в съответствие с Регламент (ЕС) 1025/2012 и не се очаква да бъдат публикувани такива данни в разумен срок.

Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 48, параграф 3.

Изменение 103

Предложение за регламент Член 19 – параграф 1 а (нов)

Текст, предложен от Комисията

Изменение

1 а. Преди да изготви проекта на акт за изпълнение, посочен в параграф 3, Комисията информира комитета, посочен в член 22 от Регламент (ЕС) 1025/2012, че счита, че условията по параграф 3 са изпълнени.

Изменение 104

Предложение за регламент Член 19 – параграф 1 б (нов)

Текст, предложен от Комисията

Изменение

1 б. При изготвянето на проекта на акт за изпълнение, посочен в параграф 1, Комисията взема предвид становищата на съответните органи или на експертната група и надлежно се консултира с всички съответни заинтересовани страни.

Изменение 105

**Предложение за регламент
Член 19 – параграф 1 в (нов)**

Текст, предложен от Комисията

Изменение

1 в. Когато хармонизиран стандарт е приет от европейска организация за стандартизация и е предложен на Комисията с цел публикуване на данните за него в Официален вестник на Европейския съюз, Комисията оценява хармонизирания стандарт в съответствие с Регламент (ЕС) 1025/2012. Когато в Официален вестник на Европейския съюз се публикуват данните за хармонизиран стандарт, Комисията отменя актовете за изпълнение, посочени в параграф 1, или части от тях, които обхващат същите изисквания като тези, обхванати от този хармонизиран стандарт.

Изменение 106

**Предложение за регламент
Член 19 – параграф 1 г (нов)**

Текст, предложен от Комисията

Изменение

1 г. Когато държава членка счита, че дадена обща спецификация не отговаря напълно на изискванията, посочени в приложение I, тя информира Комисията за това, като представя подробно обяснение. Комисията прави оценка на това подробно обяснение и може, ако е целесъобразно, да измени акта за изпълнение, с който се установява въпросната обща спецификация.

Изменение 107

Предложение за регламент
Член 20 – параграф 2

Текст, предложен от Комисията

2. ЕС декларацията за съответствие се съставя по образца, установен в приложение IV, и съдържа елементите, определени в съответните процедури за оценяване на съответствието, установени в приложение VI. Тази декларация се актуализира **непрекъснато**. Тя се предоставя на **езика или езиците, изисквани от** държавата членка, в която продуктът с цифрови елементи се пуска или се предоставя на пазара.

Изменение

2. ЕС декларацията за съответствие се съставя по образца, установен в приложение IV, и съдържа елементите, определени в съответните процедури за оценяване на съответствието, установени в приложение VI. Тази декларация се актуализира **по целесъобразност**. Тя се предоставя на **език, който е лесно разбираем за органите на** държавата членка, в която продуктът с цифрови елементи се пуска или се предоставя на пазара.

Изменение 108

Предложение за регламент
Член 20 а (нов)

Текст, предложен от Комисията

Изменение

Член 20 а

ЕС декларацията за вграждане на частично комплектовани продукти с цифрови елементи

1. **ЕС декларацията за вграждане се изготвя от производителите в съответствие с член 10, параграф 7 и в нея се посочва, че изпълнението на съответните съществени изисквания, определени в приложение I, е доказано.**

2. **ЕС декларацията за вграждане се съставя по образца, установен в приложение IVa (ново). Тази декларация се актуализира по целесъобразност. Тя се предоставя на езика или езиците, изисквани от държавата членка, в която частично комплектованият продукт с цифрови елементи се пуска или се предоставя на пазара.**

3. *Когато приложимите към частично комплектования продукт с цифрови елементи актове на Съюза, които изискват ЕС декларация за вграждане, са повече от един, се изготвя само една ЕС декларация за вграждане във връзка с всички такива актове на Съюза. В тази декларация се посочват съответните актове на Съюза, включително данните за публикуването им.*

4. *Комисията има правомощието да приема делегирани актове в съответствие с член 50 за допълване на настоящия регламент чрез добавяне на елементи към минималното съдържание на ЕС декларацията за вграждане, както е посочено в приложение IVa (ново), за да бъде отчетено технологичното развитие.*

Изменение 109

Предложение за регламент Член 22 – параграф 1

Текст, предложен от Комисията

1. Маркировката „СЕ“ се нанася върху самия продукт с цифрови елементи така, че да бъде видима, четлива и незаличима. Когато това не е възможно или не е гарантирано поради естеството на продукта с цифрови елементи, тя се поставя върху опаковката и върху ЕС декларацията за съответствие, посочена в член 20, придружаваща продукта с цифрови елементи. За продукти с цифрови елементи, които са под формата на софтуер, маркировката „СЕ“ се нанася или в ЕС декларацията за съответствие, посочена в член 20, или в уебсайта, придружаващ софтуерния продукт.

Изменение

1. Маркировката „СЕ“ се нанася върху самия продукт с цифрови елементи така, че да бъде видима, четлива и незаличима. Когато това не е възможно или не е гарантирано поради естеството на продукта с цифрови елементи, тя се поставя върху опаковката и върху ЕС декларацията за съответствие, посочена в член 20, придружаваща продукта с цифрови елементи. За продукти с цифрови елементи, които са под формата на софтуер, маркировката „СЕ“ се нанася или в ЕС декларацията за съответствие, посочена в член 20, или в уебсайта, придружаващ софтуерния продукт. **В последния случай съответният раздел на уебсайта трябва да бъде лесно и**

пряко достъпен за потребителите.

Изменение 110

Предложение за регламент

Член 22 – параграф 3

Текст, предложен от Комисията

3. Маркировката „СЕ“ се нанася, преди продуктът с цифрови елементи да бъде пуснат на пазара. Тя може да бъде следвана от пиктограма или друг знак, указващи специален риск или употреба, определени в актове за изпълнение, посочени в параграф 6.

Изменение

3. Маркировката „СЕ“ се нанася, преди продуктът с цифрови елементи да бъде пуснат на пазара. Тя може да бъде следвана от пиктограма или друг знак, указващи **на потребителите** специален риск или употреба, определени в актове за изпълнение, посочени в параграф 6.

Изменение 111

Предложение за регламент

Член 22 – параграф 5

Текст, предложен от Комисията

5. Държавите членки се основават на съществуващите механизми за гарантиране на правилното прилагане на режима за маркировката „СЕ“ и предприемат подходящите действия в случай на неправомерно използване на тази маркировка. Когато продуктът с цифрови елементи е предмет на друго законодателство на Съюза, което също предвижда нанасянето на маркировката „СЕ“, маркировката „СЕ“ указва, че продуктът отговаря и на изискванията на това друго законодателство.

Изменение

5. Държавите членки се основават на съществуващите механизми за гарантиране на правилното **и хармонизирано** прилагане на режима за маркировката „СЕ“ и предприемат подходящите **и координирани** действия в случай на неправомерно използване на тази маркировка. Когато продуктът с цифрови елементи е предмет на друго законодателство на Съюза, което също предвижда нанасянето на маркировката „СЕ“, маркировката „СЕ“ указва, че продуктът отговаря и на изискванията на това друго законодателство.

Изменение 112

Предложение за регламент

Член 22 – параграф 6

Текст, предложен от Комисията

6. Комисията може чрез **актове за изпълнение** да определя технически спецификации за пиктограми или други знаци, свързани със сигурността на продуктите с цифрови елементи, както и механизми за насърчаване на тяхното използване. Тези **актове за изпълнение** се приемат в съответствие с процедурата **по разглеждане**, посочена в член 51, параграф 2.

Изменение

6. Комисията може чрез **делегирани актове** да определя технически спецификации за **схеми за етикетирание, включително хармонизирани етикети**, пиктограми или други знаци, свързани със сигурността на продуктите с цифрови елементи, както и механизми за насърчаване на тяхното използване **от предприятията и потребителите и за повишаване на обществената осведоменост относно сигурността на продуктите с цифрови елементи**. Тези **делегирани актове** се приемат в съответствие с процедурата, посочена в член 50.

Изменение 113

Предложение за регламент
Член 22 – параграф 6 а (нов)

Текст, предложен от Комисията

Изменение

6 а. Частично комплектован продукт с цифрови елементи не се маркира с маркировката „СЕ“ съгласно настоящия регламент, без да се засягат разпоредбите за маркиране, произтичащи от друго приложимо законодателство на Съюза.

Изменение 114

Предложение за регламент
Член 22 – параграф 6 б (нов)

Текст, предложен от Комисията

Изменение

6 б. Комисията приема насоки и предоставя съвети на икономическите оператори, и по-специално тези, които са определени

като МСП, включително микропредприятия, относно прилагането на настоящия регламент. Целта на насоките и съветите е, по-специално, да се опрости и ограничи административната и финансовата тежест, като същевременно се гарантира ефективното и последователно прилагане на настоящия регламент в съответствие с общата цел за гарантиране на безопасността на продуктите и защитата на потребителите. Комисията следва да се консултира със съответните заинтересовани страни с експертен опит в областта на киберсигурността.

Изменение 115

Предложение за регламент

Член 23 – параграф 2

Текст, предложен от Комисията

2. Техническата документация се изготвя преди пускането на продукта с цифрови елементи на пазара и се актуализира непрекъснато, когато е целесъобразно, по време на очаквания експлоатационен срок на продукта или в продължение на пет години след пускането на пазара на продукта с цифрови елементи, в зависимост от това кой период е **по-кратък**.

Изменение

2. Техническата документация се изготвя преди пускането на продукта с цифрови елементи на пазара и се актуализира непрекъснато, когато е целесъобразно, по време на очаквания експлоатационен срок на продукта или в продължение на пет години след пускането на пазара на продукта с цифрови елементи, в зависимост от това кой период е **по-дълъг**.

Изменение 116

Предложение за регламент

Член 23 – параграф 3

Текст, предложен от Комисията

3. По отношение на продуктите с

Изменение

3. По отношение на продуктите с

цифрови елементи, *посочени в член 8 и член 24, параграф 4*, които са предмет и на други актове на Съюза, се изготвя едно-единствено досие с техническа документация, което съдържа информацията, посочена в приложение V към настоящия регламент, и информацията, изисквана от тези съответни актове на Съюза.

цифрови елементи, които са предмет и на други актове на Съюза, се изготвя едно-единствено досие с техническа документация, което съдържа информацията, посочена в приложение V към настоящия регламент, и информацията, изисквана от тези съответни актове на Съюза.

Изменение 117

Предложение за регламент Член 23 – параграф 5

Текст, предложен от Комисията

5. Комисията има правомощието да приема делегирани актове в съответствие с член 50 за допълване на настоящия регламент с елементите, които трябва да бъдат включени в техническата документация, посочена в приложение V, за да бъде отчетено технологичното развитие, както и промените, настъпили в процеса на прилагане на настоящия регламент.

Изменение

5. Комисията има правомощието да приема делегирани актове в съответствие с член 50 за допълване на настоящия регламент с елементите, които трябва да бъдат включени в техническата документация, посочена в приложение V, за да бъде отчетено технологичното развитие, както и промените, настъпили в процеса на прилагане на настоящия регламент. ***Комисията се стреми да сведе до минимум административната тежест, и по-специално за микро-, малките и средните предприятия.***

Изменение 118

Предложение за регламент Член 24 – параграф 1 – буква в а (нова)

Текст, предложен от Комисията

Изменение

(в а) европейска схема за сертифициране на киберсигурността, приета в съответствие с член 18, параграф 4 от Регламент (ЕС) 2019/881.

Изменение 119

Предложение за регламент Член 24 – параграф 3 – буква б

Текст, предложен от Комисията

б) „оценка на съответствието въз основа на пълно осигуряване на качеството“ (въз основа на модул Н), определена в приложение VI.

Изменение

б) „оценка на съответствието въз основа на пълно осигуряване на качеството“ (въз основа на модул Н), определена в приложение VI; **или**

Изменение 120

Предложение за регламент Член 24 – параграф 3 – буква б а (нова)

Текст, предложен от Комисията

Изменение

б а) когато е приложимо, европейска схема за сертифициране на киберсигурността с ниво на увереност „съществено“ или „високо“ съгласно Регламент (ЕС) 2019/881.

Изменение 121

Предложение за регламент Член 24 – параграф 4 а (нов)

Текст, предложен от Комисията

Изменение

4 а. За продуктите, за които се прилага законодателството на Съюза за хармонизация, основано на новата законодателна рамка, производителят следва съответното оценяване на съответствието, както се изисква съгласно тези правни актове. Изискванията, посочени в глава III, се прилагат за тези продукти.

Изменение 122

Предложение за регламент
Член 24 – параграф 5

Текст, предложен от Комисията

5. Нотифицираните органи вземат предвид специфичните интереси и потребности на малките и средните предприятия (**МСП**) при определянето на таксите за процедурите за оценяване на съответствието и ги намаляват пропорционално на техните специфични интереси и нужди.

Изменение

5. Нотифицираните органи вземат предвид специфичните интереси и потребности на **микро-**, малките и средните предприятия при определянето на таксите за процедурите за оценяване на съответствието и ги намаляват пропорционално на техните специфични интереси и нужди. **Комисията предприема действия за осигуряване на по-достъпни процедури на разумни цени и подходяща финансова подкрепа в рамките на съществуващите програми на Съюза, по-специално с цел облекчаване на тежестта за микро-, малките и средните предприятия.**

Изменение 123

Предложение за регламент
Член 24 – параграф 5 а (нов)

Текст, предложен от Комисията

Изменение

5 а. За продуктите с цифрови елементи, които попадат в обхвата на настоящия регламент и са пуснати на пазара или въведени в експлоатация от кредитни институции, регулирани от Директива 2013/36/ЕС, оценяването на съответствието се извършва като част от процедурата, посочена в членове 97 – 101 от тази директива.

Изменение 124

Предложение за регламент
Член 24 а (нов)

Текст, предложен от Комисията

Изменение

Член 24 а (нов)

Когато продуктите с цифрови елементи имат еквивалентен хардуер или софтуер, образец от продукта може да бъде представителен за група продукти за целите на следните процедури за оценяване на съответствието:

а) процедурата за вътрешен контрол (въз основа на модул А), посочена в приложение VI; или

б) процедурата „ЕС изследване на типа“ (въз основа на модул В), определена в приложение VI, последвана от процедура „ЕС съответствие с типа въз основа на вътрешен производствен контрол“ (въз основа на модул С), определена в приложение VI;

Изменение 125

**Предложение за регламент
Член 27 – параграф 5**

Текст, предложен от Комисията

Изменение

5. Нотифициращият орган запазва поверителността на получената от него информация.

5. Нотифициращият орган запазва поверителността на получената от него информация, ***включително правата върху интелектуалната собственост, поверителната търговска информация и търговските тайни.***

Изменение 126

**Предложение за регламент
Член 27 – параграф 6 а (нов)**

Текст, предложен от Комисията

Изменение

6 а. Нотифициращият орган

свежда до минимум бюрократичните процедури и таксите, особено за МСП.

Изменение 127

Предложение за регламент Член 29 – параграф 7 а (нов)

Текст, предложен от Комисията

Изменение

7 а. Държавите членки и Комисията въвеждат подходящи мерки, за да гарантират достатъчна наличност на квалифицирани специалисти, така че да се сведат до минимум затрудненията в дейностите на органите за оценяване на съответствието.

Изменение 128

Предложение за регламент Член 29 – параграф 10

Текст, предложен от Комисията

Изменение

10. Персоналът на органа за оценяване на съответствието спазва задължение за служебна тайна по отношение на информацията, получена при изпълнение на неговите задачи, съгласно приложение VI или съгласно разпоредба от националното право по прилагането му, освен по отношение на органите за надзор на пазара на държавата членка, в която осъществява дейността си. Правата **на** собственост се защитават. Органът за оценяване на съответствието разполага с документиращи процедури, гарантиращи спазването на настоящия параграф.

10. Персоналът на органа за оценяване на съответствието спазва задължение за служебна тайна по отношение на информацията, получена при изпълнение на неговите задачи, съгласно приложение VI или съгласно разпоредба от националното право по прилагането му, освен по отношение на органите за надзор на пазара на държавата членка, в която осъществява дейността си. Правата **върху интелектуалната собственост, поверителната търговска информация и търговските тайни** се защитават. Органът за оценяване на съответствието разполага с документиращи процедури, гарантиращи спазването на настоящия параграф.

Изменение 129

Предложение за регламент Член 29 – параграф 12

Текст, предложен от Комисията

12. Органите за оценяване на съответствието извършват дейностите си съгласно набор от последователни, справедливи и разумни условия, по-специално като вземат предвид интересите на **МСП** във връзка с таксите.

Изменение

12. Органите за оценяване на съответствието извършват дейностите си съгласно набор от последователни, справедливи и разумни условия **в съответствие с член 37, параграф 2**, по-специално като вземат предвид интересите на **микро-, малките и средните предприятия** във връзка с таксите.

Изменение 130

Предложение за регламент Член 36 – параграф 3

Текст, предложен от Комисията

3. Комисията гарантира, че всяка **чувствителна** информация, получена в хода на разследването, се третира като поверителна.

Изменение

3. Комисията гарантира, че всяка информация, получена в хода на разследването, се третира като поверителна, **включително правата върху интелектуалната собственост, поверителната търговска информация и търговските тайни.**

Изменение 131

Предложение за регламент Член 37 – параграф 2

Текст, предложен от Комисията

2. Оценяването на съответствието се осъществява по пропорционален начин, като се избягва ненужната тежест за икономическите оператори. Органите за оценяване на съответствието осъществяват своите дейности, като надлежно отчитат

Изменение

2. Оценяването на съответствието се осъществява по пропорционален начин, като се избягва ненужната тежест за икономическите оператори **и се обръща специално внимание на МСП**. Органите за оценяване на съответствието осъществяват своите

размера на дадено предприятие, сектора, в който осъществява дейност, неговата структура, степента на сложност на **съответната** технология на продукта и масовия или серийния характер на производството.

дейности, като надлежно отчитат размера на дадено предприятие, сектора, в който осъществява дейност, неговата структура, степента на сложност **и излагане на риск на съответния тип и** технология на продукта и масовия или серийния характер на производството.

Изменение 132

Предложение за регламент Член 37 – параграф 5

Текст, предложен от Комисията

5. Когато в процеса на наблюдение на съответствието след издаването на сертификата нотифицираният орган установи, че даден продукт вече не отговаря на посочените в настоящия регламент изисквания, той изисква от производителя да предприеме подходящи корективни мерки и спира временно действието или отнема сертификата, ако това се налага.

Изменение

5. Когато в процеса на наблюдение на съответствието след издаването на сертификата нотифицираният орган установи, че даден продукт вече не отговаря на посочените в настоящия регламент изисквания, той изисква от производителя да предприеме подходящи корективни мерки и **ограничава**, спира временно действието или отнема сертификата, ако това се налага.

Изменение 133

Предложение за регламент Член 40 – параграф 1

Текст, предложен от Комисията

1. Комисията гарантира създаването и правилното функциониране на подходяща координация и сътрудничество между нотифицираните органи под формата на междусекторна група от нотифицирани органи.

Изменение

1. Комисията гарантира създаването и правилното функциониране на подходяща координация и сътрудничество между нотифицираните органи, **вземайки предвид необходимостта от намаляване на бюрократичните процедури и таксите**, под формата на междусекторна група от нотифицирани органи.

Изменение 134

Предложение за регламент

Член 40 – параграф 2

Текст, предложен от Комисията

2. Държавите членки осигуряват участието на нотифицираните от тях органи в работата на такава група пряко или чрез определени представители.

Изменение

2. Държавите членки осигуряват участието на нотифицираните от тях органи в работата на такава група пряко или чрез определени представители, **вземайки предвид необходимостта от намаляване на бюрократичните процедури и таксите.**

Изменение 135

Предложение за регламент

Член 41 – параграф 3

Текст, предложен от Комисията

3. Когато е приложимо, органите за надзор на пазара си сътрудничат с националните органи за сертифициране в областта на киберсигурността, определени съгласно член 58 от Регламент (ЕС) 2019/881, и редовно обменят информация. По отношение на надзора на изпълнението на задълженията за докладване по член 11 от настоящия регламент определените органи за надзор на пазара си сътрудничат с ENISA.

Изменение

3. Когато е приложимо, органите за надзор на пазара си сътрудничат с националните органи за сертифициране в областта на киберсигурността, определени съгласно член 58 от Регламент (ЕС) 2019/881, и редовно обменят информация. По отношение на надзора на изпълнението на задълженията за докладване по член 11 от настоящия регламент определените органи за надзор на пазара си сътрудничат **ефективно** с ENISA. **Органите за надзор на пазара могат да поискат от ENISA да предостави технически консултации по въпроси, свързани с изпълнението и прилагането на настоящия регламент, включително по време на разследвания в съответствие с член 43, когато органите за надзор на пазара могат да поискат от ENISA да предостави необвързващи оценки на съответствието на продуктите с цифрови елементи.**

Изменение 136

Предложение за регламент

Член 41 – параграф 7

Текст, предложен от Комисията

7. Комисията улеснява **обмена** на опит между определените органи за надзор на пазара.

Изменение

7. Комисията улеснява **редовния и структуриран обмен** на опит между определените органи за надзор на пазара, **включително чрез специализирана група за административно сътрудничество (ADCO), създадена съгласно параграф 11 от настоящия член.**

Изменение 137

Предложение за регламент

Член 41 – параграф 8

Текст, предложен от Комисията

8. **Органите за надзор на пазара могат да предоставят** насоки и съвети на икономическите оператори относно прилагането на настоящия регламент **с подкрепата на Комисията.**

Изменение

8. **Комисията приема** насоки и **предоставя** съвети на икономическите оператори, **и по-специално на тези, които са определени като МСП, включително микропредприятия,** относно прилагането на настоящия регламент. **Целта на насоките и съветите е, по-специално, да се опрости и ограничи административната и финансовата тежест, като същевременно се гарантира ефективното и последователно прилагане в съответствие с общата цел за гарантиране на безопасността на продуктите и защитата на потребителите.**

Изменение 138

Предложение за регламент

Член 41 – параграф 8 а (нова)

8 а. *На органите за надзор на пазара се осигуряват необходимите средства, за да получават жалби от потребителите в съответствие с член 11 от Регламент (ЕО) № 2019/1020, също и чрез създаване на ясни и достъпни механизми за улесняване на докладването на уязвимости, инциденти и киберзаплахи.*

Изменение 139

Предложение за регламент Член 41 – параграф 11

Текст, предложен от Комисията

Изменение

11. Създава се специализирана група за административно сътрудничество (ADCO) за еднакво прилагане на настоящия регламент в съответствие с член 30, параграф 2 от Регламент (ЕС) 2019/1020. Тази ADCO група е съставена от представители на определените органи за надзор на пазара и, ако е целесъобразно, от представители на единните служби за връзка.

11. Създава се специализирана група за административно сътрудничество (ADCO) за еднакво прилагане на настоящия регламент, **за да се улеснява структурното сътрудничество във връзка с прилагането на настоящия регламент и да се рационализират практиките на органите за надзор на пазара в рамките на Съюза**, в съответствие с член 30, параграф 2 от Регламент (ЕС) 2019/1020. Тази ADCO група **има по-специално задачите, посочени в член 32, параграф 2 от Регламент (ЕС) 2019/1020**, и е съставена от представители на определените органи за надзор на пазара, **ENISA** и ако е целесъобразно, от представители на единните служби за връзка. **ADCO групата провежда редовни заседания и когато е необходимо, по надлежно обосновано искане на Комисията, ENISA или държава членка, координира действията си с други съществуващи дейности на Съюза, свързани с надзора на пазара и безопасността на потребителите, и по**

целесъобразност си сътрудничи и обменя информация с други мрежи, групи и органи на Съюза. ADCO групата може да кани експерти и други трети страни, включително организации на потребителите, да присъстват на нейните заседания.

Изменение 140

Предложение за регламент Член 41 – параграф 11 а (нов)

Текст, предложен от Комисията

Изменение

11 а. За продукти с цифрови елементи, попадащи в обхвата на настоящия регламент, които се разпространяват, въвеждат в експлоатация или използват от финансови институции, регулирани от съответното законодателство на Съюза в областта на финансовите услуги, органът за надзор на пазара за целите на настоящия регламент е съответният орган, отговарящ за финансовия надзор на тези институции съгласно посоченото законодателство.

Изменение 141

Предложение за регламент Член 42 – параграф 1

Текст, предложен от Комисията

Изменение

Когато това е необходимо за оценяване на съответствието на продуктите с цифрови елементи и на процесите, въведени от техните производители, със съществените изисквания, посочени в приложение I, и при мотивирано искане, на органите за надзор на пазара се предоставя достъп до данните, необходими за оценяване на

Когато това е необходимо за оценяване на съответствието на продуктите с цифрови елементи и на процесите, въведени от техните производители, със съществените изисквания, посочени в приложение I, и при мотивирано искане, на органите за надзор на пазара се предоставя достъп до данните, необходими за оценяване на

проектирането, разработването, производството и отстраняването на уязвимостите на такива продукти, включително до свързаната с тях вътрешна документация на съответния икономически оператор.

проектирането, разработването, производството и отстраняването на уязвимостите на такива продукти, включително до свързаната с тях вътрешна документация на съответния икономически оператор. ***Когато е целесъобразно и в съответствие с член 52, параграф 1, буква а), това става в защитена и контролирана среда, определена от производителя.***

Изменение 142

Предложение за регламент Член 43 – параграф 1 – алинея 2

Текст, предложен от Комисията

Когато в хода на тази оценка органът за надзор на пазара открие, че за продукта с цифрови елементи не са спазени изискванията, определени в настоящия регламент, той без забавяне изисква от съответния оператор да предприеме необходимите корективни действия, за да приведе продукта в съответствие с тези изисквания или да го изтегли от пазара, или да го иззме в определен от него разумен срок, съобразен с естеството на риска.

Изменение

Когато в хода на тази оценка органът за надзор на пазара открие, че за продукта с цифрови елементи не са спазени изискванията, определени в настоящия регламент, ***или че продуктът представлява друга заплаха за националната сигурност***, той без забавяне изисква от съответния ***икономически*** оператор да предприеме необходимите корективни действия, за да приведе продукта в съответствие с тези изисквания или да го изтегли от пазара, или да го иззме в определен от него разумен срок, съобразен с естеството на риска.

Преди да извърши горепосочената оценка, органът за надзор на пазара може, ако е необходимо и като отчита значимостта на киберриска, да изиска от съответния оператор да предприеме незабавни действия за временно прекратяване или ограничаване на наличността на продукта на пазара за периода на горепосочената оценка.

Изменение 143

Предложение за регламент
Член 43 – параграф 4 – алинея 1

Текст, предложен от Комисията

Когато производителят на даден продукт с цифрови елементи не предприеме подходящи корективни действия в посочения в параграф 1, втора алинея срок, органът за надзор на пазара предприема всички подходящи временни мерки, за да забрани или ограничи предоставянето на продукта на националния пазар, да изтегли продукта от този пазар или да го изземе.

Изменение

Когато производителят на даден продукт с цифрови елементи не предприеме подходящи корективни действия в посочения в параграф 1, втора алинея срок **или компетентният орган на държавата членка счита, че продуктът представлява заплаха за националната сигурност**, органът за надзор на пазара предприема всички подходящи временни мерки, за да забрани или ограничи предоставянето на продукта на националния пазар, да изтегли продукта от този пазар или да го изземе.

Изменение 144

Предложение за регламент
Член 45 – параграф 1

Текст, предложен от Комисията

1. Когато Комисията има достатъчно основания да счита, включително въз основа на информация, предоставена от ENISA, че продукт с цифрови елементи, който представлява значителен киберриск, не отговаря на изискванията, установени в настоящия регламент, тя **може да поиска** от съответните органи за надзор на пазара да извършат оценка на съответствието и да изпълнят процедурите, посочени в член 43.

Изменение

1. Когато Комисията има достатъчно основания да счита, включително въз основа на информация, предоставена от **компетентните органи на държавите членки, екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС), определени или създадени в съответствие с Директива (ЕС) 2022/2555, или ENISA**, че продукт с цифрови елементи, който представлява значителен киберриск, не отговаря на изискванията, установени в настоящия регламент, тя **изисква** от съответните органи за надзор на пазара да извършат оценка на съответствието и да изпълнят процедурите, посочени в член 43.

Изменение 145

Предложение за регламент Член 45 – параграф 2

Текст, предложен от Комисията

2. При **извънредни** обстоятелства, които оправдават незабавна намеса за запазване на доброто функциониране на вътрешния пазар, и когато Комисията има **достатъчно** основания да счита, че продуктът, посочен в параграф 1, продължава да не отговаря на изискванията, установени в настоящия регламент, и съответните органи за надзор на пазара не са предприели ефективни мерки, Комисията **може да поиска от** ENISA да извърши оценка на съответствието. Комисията надлежно информира съответните органи за надзор на пазара. Съответните икономически оператори си сътрудничат при необходимост с ENISA.

Изменение

2. При обстоятелства, които оправдават незабавна намеса за запазване на доброто функциониране на вътрешния пазар, и когато Комисията има основания да счита, че продуктът, посочен в параграф 1, продължава да не отговаря на изискванията, установени в настоящия регламент, и съответните органи за надзор на пазара не са предприели ефективни мерки, Комисията **изисква от** ENISA да извърши оценка на съответствието. Комисията надлежно информира съответните органи за надзор на пазара. Съответните икономически оператори си сътрудничат при необходимост с ENISA.

Изменение 146

Предложение за регламент Член 46 – параграф 1

Текст, предложен от Комисията

1. Когато след извършване на оценката по член 43 органът за надзор на пазара на държава членка установи, че въпреки че даден продукт с цифрови елементи и въведените от производителя процеси са в съответствие с настоящия регламент, те представляват значителен киберриск и освен това представляват риск за здравето или безопасността на хората, за спазването на задълженията по правото на Съюза или националното право, предназначени за защита на основните права, за достъпността, автентичността, целостта или поверителността на

Изменение

1. Когато след извършване на оценката по член 43 органът за надзор на пазара на държава членка установи, че въпреки че даден продукт с цифрови елементи и въведените от производителя процеси са в съответствие с настоящия регламент, те представляват значителен киберриск и освен това представляват риск за здравето или безопасността на хората, за спазването на задълженията по правото на Съюза или националното право, предназначени за защита на основните права, за достъпността, автентичността, целостта или поверителността на

услугите, предлагани чрез електронна информационна система от основни субекти от вида, посочен в /приложение I към Директива XXX/XXXX (МИС 2)/, или за други аспекти на защитата на обществения интерес, той изисква от съответния оператор да предприеме всички подходящи мерки, за да гарантира, че продуктът с цифрови елементи и процесите, въведени от съответния производител, когато са пуснати на пазара, вече не представляват този риск, да изтегли продукта с цифрови елементи от пазара или да го иземе в разумен срок, съобразен с естеството на риска.

услугите, предлагани чрез електронна информационна система от основни субекти от вида, посочен в приложение I към Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2), или за други аспекти на защитата на обществения интерес, той изисква от съответния **икономически** оператор да предприеме всички подходящи мерки, за да гарантира, че продуктът с цифрови елементи и процесите, въведени от съответния производител, когато са пуснати на пазара, вече не представляват този риск, да изтегли продукта с цифрови елементи от пазара или да го иземе в разумен срок, съобразен с естеството на риска.

Изменение 147

Предложение за регламент Член 46 – параграф 2

Текст, предложен от Комисията

2. Производителят или други съответни оператори гарантират, че се предприемат корективни действия по отношение на въпросните продукти с цифрови елементи, които те са предоставили на пазара в целия Съюз, в рамките на срока, определен от органа за надзор на пазара на държавата членка, посочен в параграф 1.

Изменение

2. Производителят или други съответни **икономически** оператори гарантират, че се предприемат корективни действия по отношение на въпросните продукти с цифрови елементи, които те са предоставили на пазара в целия Съюз, в рамките на срока, определен от органа за надзор на пазара на държавата членка, посочен в параграф 1.

Изменение 148

Предложение за регламент Член 46 – параграф 6

Текст, предложен от Комисията

6. Когато Комисията има достатъчно основания да счита, включително въз основа на информация, предоставена от ENISA, че даден продукт с цифрови елементи, въпреки че е в съответствие с настоящия регламент, представлява рисковете, посочени в параграф 1, тя **може да поиска от** съответния орган или органи за надзор на пазара да извършат оценка на съответствието и да следват процедурите, посочени в член 43 и параграфи 1, 2 и 3 от настоящия член.

Изменение

6. Когато Комисията има достатъчно основания да счита, включително въз основа на информация, предоставена от ENISA, че даден продукт с цифрови елементи, въпреки че е в съответствие с настоящия регламент, представлява рисковете, посочени в параграф 1, тя **изисква от** съответния орган или органи за надзор на пазара да извършат оценка на съответствието и да следват процедурите, посочени в член 43 и параграфи 1, 2 и 3 от настоящия член.

Изменение 149

Предложение за регламент Член 46 – параграф 7

Текст, предложен от Комисията

7. При **извънредни** обстоятелства, които оправдават незабавна намеса за запазване на доброто функциониране на вътрешния пазар, и когато Комисията има достатъчно основания да счита, че продуктът, посочен в параграф 6, продължава да носи рисковете, посочени в параграф 1, и съответните национални органи за надзор на пазара не са предприели ефективни мерки, Комисията **може да поиска** от ENISA да извърши оценка на рисковете, свързани с този продукт, и информира съответните органи за надзор на пазара за това. Съответните икономически оператори си сътрудничат при необходимост с ENISA.

Изменение

7. При обстоятелства, които оправдават незабавна намеса за запазване на доброто функциониране на вътрешния пазар, и когато Комисията има достатъчно основания да счита, че продуктът, посочен в параграф 6, продължава да носи рисковете, посочени в параграф 1, и съответните национални органи за надзор на пазара не са предприели ефективни мерки, Комисията **изисква** от ENISA да извърши оценка на рисковете, свързани с този продукт, и информира съответните органи за надзор на пазара за това. Съответните икономически оператори си сътрудничат при необходимост с ENISA.

Изменение 150

Предложение за регламент
Член 48 – параграф 1

Текст, предложен от Комисията

1. Органите за надзор на пазара **могат да се договорят** с други съответни органи **да извършват съвместни дейности**, насочени към гарантиране на киберсигурността и защитата на потребителите по отношение на конкретни продукти с цифрови елементи, пуснати или предоставени на пазара, по-специално продукти, за които често се установява, че представляват киберрискове.

Изменение

1. Органите за надзор на пазара **редовно извършват съвместни действия** с други съответни органи, насочени към гарантиране на киберсигурността и защитата на потребителите по отношение на конкретни продукти с цифрови елементи, пуснати или предоставени на пазара, по-специално продукти, за които често се установява, че представляват киберрискове. **Тези действия включват проверки на продукти, придобити под прикрита самоличност.**

Изменение 151

Предложение за регламент
Член 48 – параграф 2

Текст, предложен от Комисията

2. Комисията или ENISA **могат да предложат** съвместни дейности за проверка на съответствието с настоящия регламент, които да се провеждат от органите за надзор на пазара въз основа на признаци или информация за потенциално несъответствие в няколко държави членки на продукти, попадащи в обхвата на настоящия регламент, с изискванията, определени от него.

Изменение

2. Комисията или ENISA **предлагат** съвместни дейности за проверка на съответствието с настоящия регламент, които да се провеждат от органите за надзор на пазара въз основа на признаци или информация за потенциално несъответствие в няколко държави членки на продукти, попадащи в обхвата на настоящия регламент, с изискванията, определени от него.

Изменение 152

Предложение за регламент
Член 49 – параграф 1

Текст, предложен от Комисията

1. Органите за надзор на пазара

Изменение

1. Органите за надзор на пазара

могат да решат да проведат едновременни координирани действия за контрол („мащабни проверки“) на конкретни продукти или категории продукти с цифрови елементи, за да проверят съответствието с настоящия регламент или да открият нарушения на настоящия регламент.

редовно провеждат едновременни координирани действия за контрол („мащабни проверки“) на конкретни продукти или категории продукти с цифрови елементи, за да проверят съответствието с настоящия регламент или да открият нарушения на настоящия регламент.

Изменение 153

Предложение за регламент Член 49 – параграф 2

Текст, предложен от Комисията

2. Освен когато участващите органи за надзор на пазара са се договорили за друго, мащабните проверки се координират от Комисията. Координаторът на мащабната проверка **може**, когато е целесъобразно, **да оповести публично** общите резултати.

Изменение

2. Освен когато участващите органи за надзор на пазара са се договорили за друго, мащабните проверки се координират от Комисията. Координаторът на мащабната проверка **оповестява публично**, когато е целесъобразно, общите резултати.

Изменение 154

Предложение за регламент Член 49 – параграф 3

Текст, предложен от Комисията

3. При изпълнение на своите задачи ENISA **може**, включително въз основа на уведомленията, получени съгласно член 11, параграфи 1 и 2, **да определи** категориите продукти, за които **могат да бъдат организирани** мащабни проверки. Предложението за мащабни проверки се представя на потенциалния координатор, посочен в параграф 2, за разглеждане от органите за надзор на пазара.

Изменение

3. При изпълнение на своите задачи ENISA, включително въз основа на уведомленията, получени съгласно член 11, параграфи 1 и 2, **определя** категориите продукти, за които **се организират** мащабни проверки. Предложението за мащабни проверки се представя на потенциалния координатор, посочен в параграф 2, за разглеждане от органите за надзор на пазара.

Изменение 155

Предложение за регламент
Член 49 – параграф 5

Текст, предложен от Комисията

5. Органите за надзор на пазара **могат да приканят** служителите на Комисията и други придружаващи ги лица, упълномощени от Комисията, да участват в мащабните проверки.

Изменение

5. Органите за надзор на пазара **приканват** служителите на Комисията и други придружаващи ги лица, упълномощени от Комисията, да участват в мащабните проверки.

Изменение 156

Предложение за регламент
Член 49 а (нов)

Текст, предложен от Комисията

Изменение

Член 49 а (нов)

Предоставяне на технически консултации

- 1. Комисията определя чрез акт за изпълнение експертна група, която да предоставя технически консултации на органите за надзор на пазара по въпроси, свързани с изпълнението и прилагането на настоящия регламент. В акта за изпълнение се посочват, *inter alia*, подробностите, свързани със състава на групата, нейното функциониране и възнаграждението на нейните членове. Експертната група по-специално предоставя необвързващи оценки на продукти с цифрови елементи по искане на орган за надзор на пазара, който провежда разследване съгласно член 43, както и необвързващи оценки на списъка на критичните продукти с цифрови елементи, посочен в приложение II, и на евентуалната необходимост от актуализиране на този списък.**
- 2. Експертната група се състои от независими експерти, назначени от Комисията за срок от три години,**

който може да бъде подновен, въз основа на техния научен или технически опит в областта.

3. Комисията назначава брой експерти, който се счита за достатъчен, за да се отговори на предвидените нужди

4. Комисията предприема необходимите мерки за управление и предотвратяване на евентуални конфликти на интереси.

Декларациите за интереси на членовете на експертната група се оповестяват публично.

5. Назначените експерти изпълняват задачите си с най-високо ниво на професионализъм, независимост, безпристрастност и обективност.

6. При приемането на позиции, становища и доклади експертната група се опитва да постигне консенсус. Ако не може да бъде постигнат консенсус, решенията се вземат с обикновено мнозинство от членовете на групата.

Изменение 157

Предложение за регламент Член 53 – параграф 1

Текст, предложен от Комисията

1. Държавите членки определят правилата относно санкциите, приложими при нарушения на настоящия регламент от икономически оператори, и вземат всички необходими мерки, за да осигурят тяхното изпълнение. Предвидените **наказания** трябва да бъдат ефективни, пропорционални и възпиращи.

Изменение

1. Държавите членки определят правилата относно санкциите, приложими при нарушения на настоящия регламент от икономически оператори, и вземат всички необходими мерки, за да осигурят тяхното изпълнение. Предвидените **санкции** трябва да бъдат ефективни, пропорционални и възпиращи **и да отчитат особеностите на микро-, малките и средните предприятия.**

Изменение 158

Предложение за регламент Член 53 – параграф 6 – буква а а (нова)

Текст, предложен от Комисията

Изменение

(а а) дали нарушението е извършено по непредпазливост;

Изменение 159

Предложение за регламент Член 53 – параграф 6 – буква б

Текст, предложен от Комисията

Изменение

б) дали други органи за надзор на пазара вече са наложили административни глоби на същия оператор за подобно нарушение;

б) дали **същите или** други органи за надзор на пазара вече са наложили административни глоби на същия оператор за подобно нарушение;

Изменение 160

Предложение за регламент Член 53 – параграф 6 – буква в

Текст, предложен от Комисията

Изменение

в) размера и пазарния дял на оператора, извършил нарушението.

в) размера и пазарния дял на оператора, извършил нарушението, **като се вземат предвид мащабът на рисковете и последиците и финансовите особености на микро-, малките и средните предприятия;**

Изменение 161

Предложение за регламент Член 53 – параграф 6 – буква в а (нова)

Текст, предложен от Комисията

Изменение

(в а) последващото поведение на оператора след получаване на информация или узнаване за съответното несъответствие, включително дали след като е узнал за несъответствието, операторът е предприел всички подходящи корективни мерки и обосновани необходими мерки за избягване или свеждане до минимум на потенциалните отрицателни последици.

Изменение 162

Предложение за регламент Раздел VII а (нов)

Текст, предложен от Комисията

Изменение

МЕРКИ В ПОДКРЕПА НА ИНОВАЦИИТЕ

Изменение 163

Предложение за регламент Член 53 а (нов)

Текст, предложен от Комисията

Изменение

Член 53 а

Регулаторни лаборатории

Комисията и ENISA могат да създадат Европейска регулаторна лаборатория с доброволно участие на производителите на продукти с цифрови елементи с цел:

а) осигуряване на контролирана среда, която улеснява разработването, изпитването и валидирането при проектирането, разработването и производството на продукти с

цифрови елементи, преди те да бъдат пуснати на пазара или въведени в експлоатация в съответствие с конкретен план;

б) предоставяне на практическа подкрепа на икономическите оператори, включително чрез насоки и най-добри практики за спазване на съществените изисквания, посочени в приложение I;

в) допринасяне за натрупването на регулаторен опит, основан на факти.

Изменение 164

Предложение за регламент Член 54 – заглавие

Текст, предложен от Комисията

Изменение на Регламент (ЕС) 2019/1020

Изменение

Изменение на Регламент (ЕС) 2019/1020
и на Директива 2020/1828/ЕО

Изменение 165

Предложение за регламент Член 54 – параграф 1 а (нов)

Текст, предложен от Комисията

Изменение на Регламент (ЕС) 2019/1020

Изменение

1а. В приложение I към Директива 2020/1828/ЕО се добавя следната точка:

„67. [Регламент XXX] [Законодателен акт за киберустойчивост]“.

Изменение 166

Предложение за регламент Член 54 а (нов)

Изменение на Регламент (ЕС) 2019/1020

Текст, предложен от Комисията

Изменение

Член 54 а (нов)

Делегиран регламент (ЕС) 2022/30

Настоящият регламент е изготвен така, че всички продукти, обхванати от съществените изисквания, определени в член 3, параграф 3, букви г), д) и е) от Директива 2014/53/ЕС, във вида, в който са описани в делегиран регламент (ЕС) 2022/30, да отговарят на изискванията на настоящия регламент. За да се създаде правна сигурност, Делегиран регламент (ЕС) 2022/30 ще бъде отменен, когато настоящият регламент влезе в сила.

Изменение 167

**Предложение за регламент
Член 57 – параграф 2**

Текст, предложен от Комисията

Изменение

Той се прилага от [24 месеца след датата на влизането в сила на настоящия регламент]. **Член 11 обаче се прилага от [12 месеца след датата на влизането в сила на настоящия регламент].**

Той се прилага от [36 месеца след датата на влизането в сила на настоящия регламент]. **Що се отнася до продуктите с критични елементи, глави II, III, V и VII се прилагат не по-рано от [20 месеца след датата на публикуване на хармонизираните стандарти, разработени в рамките на стандартизацията, изисквана за целите на настоящия регламент].**

Не по-късно от 6 месеца след датата на влизане в сила на настоящия регламент Комисията издава насоки за това как да се прилагат изискванията на настоящия регламент по отношение на нематериални продукти.

Изменение 168

Предложение за регламент
Приложение I – част 1 – точка 3 – уводна част

Текст, предложен от Комисията

(3) Въз основа на оценката на **риска**, посочена в член 10, параграф 2, и когато е приложимо, продуктите с цифрови елементи:

Изменение

(3) Въз основа на оценката на **киберриска**, посочена в член 10, параграф 2, и когато е приложимо, продуктите с цифрови елементи:

Изменение 169

Предложение за регламент
Приложение I – част 1 – точка 3 – буква - а (нова)

Текст, предложен от Комисията

Изменение

-а) се пускат на пазара без известни уязвимости, които могат да бъдат използвани по отношение на външно устройство или мрежа;

Изменение 170

Предложение за регламент
Приложение I – част 1 – точка 3 – буква а

Текст, предложен от Комисията

Изменение

а) се доставят с конфигурация с настройки за сигурност по подразбиране, **включително възможност за възстановяване на продукта до първоначалното му състояние,**

а) се доставят с конфигурация с настройки за сигурност по подразбиране,

Изменение 171

Предложение за регламент
Приложение I – част 1 – точка 3 – буква в

Текст, предложен от Комисията

Изменение

в) защитават поверителността на

в) защитават поверителността на

съхранени, предадени или обработени по друг начин данни, лични или други, като например чрез криптиране на съответните данни в покой или при пренос чрез най-съвременните механизми,

съхранени, предадени или обработени по друг начин данни, лични или други, като например чрез криптиране, **токенизация, проверки за отстраняване на слабостите или друга адекватна защита** на съответните данни в покой или при пренос чрез най-съвременните механизми,

Изменение 172

Предложение за регламент Приложение I – част 1 – точка 3 – буква г

Текст, предложен от Комисията

г) защитават целостта на съхранени, предадени или обработени по друг начин данни, лични или други, команди, програми и конфигурация срещу манипулиране или промяна, които не са разрешени от ползвателя, както и докладват за повреди,

Изменение

г) защитават целостта на съхранени, предадени или обработени по друг начин данни, лични или други, команди, програми и конфигурация срещу манипулиране или промяна, които не са разрешени от ползвателя, както и докладват за повреди **или възможен неразрешен достъп**,

Изменение 173

Предложение за регламент Приложение I – част 1 – точка 3 – буква е

Текст, предложен от Комисията

е) защитават наличието на основни функции, включително устойчивост срещу и овладяване на атаки за отказ на услуга,

Изменение

е) защитават наличието на **съществени и** основни функции, включително устойчивост срещу и овладяване на атаки за отказ на услуга,

Изменение 174

Предложение за регламент Приложение I – част 1 – точка 3 – буква и

Текст, предложен от Комисията

и) са проектирани, разработени и произведени по такъв начин, че да бъде намалено въздействието на даден инцидент чрез подходящи механизми и техники за овладяване на зловреден код,

Изменение

и) са проектирани, разработени и произведени по такъв начин, че да бъде намалено въздействието на даден **значителен** инцидент чрез подходящи механизми и техники за овладяване на зловреден код,

Изменение 175

Предложение за регламент Приложение I – част 1 – точка 3 – буква й

Текст, предложен от Комисията

й) осигуряват информация, свързана със сигурността, **посредством** записване и/или наблюдение на съответната вътрешна дейност, включително достъпа до данни, услуги или функции или тяхната промяна,

Изменение

й) осигуряват информация, свързана със сигурността, **като при поискване от ползвателя предоставят възможности за** записване и/или наблюдение, **локално и на ниво устройство, за** съответната вътрешна дейност, включително достъпа до данни, услуги или функции или тяхната промяна,

Изменение 176

Предложение за регламент Приложение I – част 1 – точка 3 – буква к

Текст, предложен от Комисията

к) гарантират, че по отношение на уязвимостите се предприемат мерки посредством актуализации на защитата, включително, когато е приложимо, чрез автоматични актуализации и уведомяване на ползвателите за налични актуализации.

Изменение

к) гарантират, че по отношение на уязвимостите се предприемат мерки посредством актуализации на защитата, включително, когато е приложимо, **отделно от актуализациите на функционалните възможности, както и** чрез автоматични актуализации и уведомяване на ползвателите за налични актуализации;

Изменение 177

Предложение за регламент
Приложение I – част 1 – точка 3 – буква к а (нова)

Текст, предложен от Комисията

Изменение

(ка) са проектирани, разработени и произведени така, че при достигане на края на жизнения цикъл да могат по безопасен начин да бъдат спрени и евентуално рециклирани, включително като се позволява на потребителите да изтеглят и премахват за постоянно всички данни по безопасен начин.

Изменение 178

Предложение за регламент
Приложение I – част 2 – параграф 1 – точка 2

Текст, предложен от Комисията

Изменение

(2) във връзка с рисковете за продуктите с цифрови елементи, незабавно предприемат действия и отстраняват уязвимостите, включително чрез осигуряване на актуализации на защитата,

(2) във връзка с рисковете за продуктите с цифрови елементи, незабавно предприемат действия и отстраняват **критичните и сериозните уязвимости**, включително чрез осигуряване на актуализации на защитата, **или документират причините за неотстраняването на уязвимостта**,

Изменение 179

Предложение за регламент
Приложение I – част 2 – параграф 1 – точка 4

Текст, предложен от Комисията

Изменение

(4) след като бъде предоставена актуализация на защитата, публично разкриват информация за коригираните уязвимости, включително описание на уязвимостите, информация, която дава възможност на ползвателите да

(4) след като бъде предоставена актуализация на защитата, публично **или в съответствие с най-добрите практики в сектора** разкриват информация за коригираните **известни** уязвимости, включително описание на

идентифицират засегнатия продукт с цифрови елементи, въздействието на уязвимостите, тяхната сериозност и информация, помагаща на ползвателите да коригират уязвимостите,

уязвимостите, информация, която дава възможност на ползвателите да идентифицират засегнатия продукт с цифрови елементи, въздействието на уязвимостите, тяхната сериозност и **ясна и достъпна** информация, помагаща на ползвателите да коригират уязвимостите,

Изменение 180

Предложение за регламент

Приложение I – част 2 – параграф 1 – точка 4 а (нова)

Текст, предложен от Комисията

Изменение

(4 а) информацията относно корекциите и уязвимостите се споделя и разкрива по контролиран начин, като се спазват принципите за „намаляване на вредите“ и търговските тайни чрез отговорно разкриване на уязвимостите на участниците, които могат да предприемат действия за намаляване на уязвимостта, и тя не се прави публично достояние, за да се избегне рискът от неволно информиране на потенциални извършители на атаки;

Изменение 181

Предложение за регламент

Приложение I – част 2 – параграф 1 – точка 7

Текст, предложен от Комисията

Изменение

(7) предоставят механизми за сигурно разпространение на актуализации за продукти с цифрови елементи, за да се гарантира, че уязвимостите, които могат да бъдат използвани, са коригирани или овладени своевременно,

(7) предоставят механизми за сигурно разпространение на актуализации **на защитата** за продукти с цифрови елементи, за да се гарантира, че уязвимостите, които могат да бъдат използвани, са коригирани или овладени своевременно,

Изменение 182

Предложение за регламент Приложение I – част 2 – параграф 1 – точка 8

Текст, предложен от Комисията

(8) гарантират, че когато **са налични** софтуерни поправки или актуализации за сигурност с цел преодоляване на установени проблеми със сигурността, **те се разпространяват** незабавно и безплатно, придружени от информационни съобщения, предоставящи на ползвателите необходимата информация, включително относно потенциалните действия, които трябва да бъдат предприети.

Изменение

(8) гарантират, че когато **могат разумно да бъдат предоставени** софтуерни поправки или актуализации за сигурност с цел преодоляване на установени проблеми със сигурността, **има средства, чрез които ползвателите могат да ги получат** незабавно и безплатно **или на прозрачна и недискриминационна цена**, придружени от информационни съобщения, предоставящи на ползвателите необходимата информация, включително относно потенциалните действия, които трябва да бъдат предприети.

Изменение 183

Предложение за регламент Приложение II – параграф 1 – точка 2

Текст, предложен от Комисията

2. **центъра** за контакт, където може да бъде докладвана и получена информация за уязвимости в киберсигурността на продукта,

Изменение

2. **единното звено** за контакт, където може да бъде докладвана и получена информация за уязвимости в киберсигурността на продукта,

Изменение 184

Предложение за регламент Приложение II – параграф 1 – точка 5

Текст, предложен от Комисията

5. **известните или предвидимите обстоятелства, свързани с използването на продукта с цифрови елементи в съответствие с неговото**

Изменение

заличава се

предназначение или в условия на разумно предвидима неправилна експлоатация, които могат да доведат до значими рискове за киберсигурността,

Изменение 185

Предложение за регламент Приложение II – параграф 1 – точка 6

Текст, предложен от Комисията

6. ако и когато е приложимо, къде *може да бъде намерен описът* на софтуерните компоненти,

Изменение

6. ако и когато е приложимо, къде *компетентните органи могат да намерят описа* на софтуерните компоненти,

Изменение 186

Предложение за регламент Приложение II – параграф 1 – точка 8

Текст, предложен от Комисията

8. вида на техническата поддръжка за сигурност, предлагана от производителя, и до кога ще бъде предоставяна, *най-малко до кога ползвателите могат да очакват да получават актуализации на защитата,*

Изменение

8. вида на техническата поддръжка за сигурност, предлагана от производителя, и до кога ще бъде предоставяна,

Изменение 187

Предложение за регламент Приложение II – параграф 1 – точка 8 а (нова)

Текст, предложен от Комисията

Изменение

8 а. крайната дата на очаквания експлоатационен срок на продукта, ясно посочена, когато е приложимо, върху опаковката на продукта, до която производителят гарантира

ефективното отстраняване на уязвимостите и предоставянето на актуализации на защитата,

Изменение 188

**Предложение за регламент
Приложение II – параграф 1 – точка 9 – буква а**

Текст, предложен от Комисията

Изменение

а) необходимите мерки при първоначалното пускане в експлоатация и през целия жизнен цикъл на продукта, за да се гарантира неговото безопасно използване, *заличава се*

Изменение 189

**Предложение за регламент
Приложение II – параграф 1 – точка 9 – буква б**

Текст, предложен от Комисията

Изменение

б) по какъв начин промените в продукта ще засягат сигурността на данните, *заличава се*

Изменение 190

**Предложение за регламент
Приложение II – параграф 1 – точка 9 – буква в а (нова)**

Текст, предложен от Комисията

Изменение

(в а) очаквания експлоатационен срок на продукта и докога производителят гарантира ефективното отстраняване на уязвимостите и предоставянето на актуализации на защитата;

Изменение 191

**Предложение за регламент
Приложение II – параграф 1 – точка 9 – буква г**

Текст, предложен от Комисията

Изменение

г) сигурното извеждане от експлоатация на продукта, включително информация за това как данните на ползвателите могат да бъдат премахнати по сигурен начин.

заличава се

Изменение 192

**Предложение за регламент
Приложение III – параграф 1 – точка 3 а (нова)**

Текст, предложен от Комисията

Изменение

3 а. Платформи за удостоверяване на автентичността, разрешаване и проследяване;

Изменение 193

**Предложение за регламент
Приложение III – част I – точка 15**

Текст, предложен от Комисията

Изменение

15. Физически мрежови интерфейси;

15. Физически *и виртуални* мрежови интерфейси;

Изменение 194

**Предложение за регламент
Приложение III – част I – точка 18**

Текст, предложен от Комисията

Изменение

18. Маршрутизатори, модеми, предназначени за връзка с интернет, и комутатори, които са извън обхвата на клас II;

заличава се

Изменение 195

Предложение за регламент Приложение III – част I – точка 23

Текст, предложен от Комисията

23. **Индустриален** интернет на предметите, който е извън обхвата на клас II.

Изменение

23. **Индустриални продукти с цифрови елементи, които могат да бъдат посочени като част от** интернет на предметите, който е извън обхвата на клас II.

Изменение 196

Предложение за регламент Приложение III – част II – точка 4

Текст, предложен от Комисията

4. Защитни стени, системи за установяване и/или предотвратяване на проникване, предназначени за промишлена употреба;

Изменение

4. Защитни стени, **защитни илюзове**, системи за установяване и/или предотвратяване на проникване, предназначени за промишлена употреба;

Изменение 197

Предложение за регламент Приложение III – част II – точка 7

Текст, предложен от Комисията

7. Маршрутизатори, модеми, предназначени за връзка с интернет, и комутатори, **предназначени за промишлена употреба**;

Изменение

7. Маршрутизатори, модеми, предназначени за връзка с интернет, комутатори **и други мрежови възли, които са необходими за предоставянето на услугата за свързаност**;

Изменение 198

Предложение за регламент Приложение IV а (ново)

ПРИЛОЖЕНИЕ IVa

**ЕС ДЕКЛАРАЦИЯ ЗА ВГРАЖДАНЕ
НА ЧАСТИЧНО КОМПЛЕКТОВАНИ
ПРОДУКТИ С ЦИФРОВИ
ЕЛЕМЕНТИ**

*ЕС декларацията за вграждане за
частично комплектовани продукти,
посочена в член 20а, съдържа цялата
изброена по-долу информация:*

- 1. наименование, тип и всякаква
допълнителна информация за
уникалната идентификация на
частично комплектования продукт с
цифрови елементи,*
- 2. предмет на декларацията
(идентификация на частично
окомплектования продукт,
позволяваща проследяването му. При
необходимост може да се добави
снимка),*
- 3. изявление, че описаният по-
горе частично комплектован продукт
е в съответствие с приложимото
законодателство на Съюза за
хармонизация,*
- 4. позоваване на съответните
актове на Съюза, включително
данните за публикуването им,*
- 5. Допълнителна информация:*

Подписано за и от името на:

.....

(място и дата на издаване):

(име, длъжност) (подпис):

Изменение 199

Предложение за регламент
Приложение V – параграф 1 – част 1 – буква а

Текст, предложен от Комисията

Изменение

- a) неговото предназначение,** **заличава се**

Изменение 200

Предложение за регламент Приложение V – параграф 1 – точка 2

Текст, предложен от Комисията

Изменение

- 2. описание на проектирането, разработването и производството на продукта и на процесите на отстраняване на уязвимостите, включително:** **заличава се**

a) пълна информация за проекта и разработването на продукта с цифрови елементи, включително, когато е приложимо, чертежи и схеми и/или описание на архитектурата на системата, в което се обяснява как компонентите на софтуера се надграждат или се свързват помежду си и се интегрират в цялостното обработване,

б) пълна информация и спецификации на процесите за отстраняване на уязвимости, въведени от производителя, включително опис на софтуерните компоненти, политика относно координираното оповестяване на уязвимости, доказателство за предоставяне на адрес за контакт за докладване на уязвимостите и описание на техническите решения за безопасно разпространение на актуализации;

в) пълна информация и спецификации на процесите на производство и наблюдение на продукта с цифрови елементи и валидирането на тези процеси;

Изменение 201

Предложение за регламент Приложение V – параграф 1 – точка 3

Текст, предложен от Комисията

3. оценка на рисковете за киберсигурността, срещу които продуктът с цифрови елементи е проектиран, разработен, произведен, доставен и поддържан, както е посочено в член 10 от настоящия Регламент;

Изменение

3. **деклариране или обобщение на киберрисковете, с оглед на които продуктът с цифрови елементи е проектиран, разработен, произведен, доставен и поддържан, в съответствие с член 10 от настоящия регламент, и след обосновано искане от орган за надзор на пазара, при условие че е необходимо, за да може този орган да провери съответствието със съществените изисквания, посочени в приложение I, подробна** оценка на рисковете за киберсигурността, срещу които продуктът с цифрови елементи е проектиран, разработен, произведен, доставен и поддържан, както е посочено в член 10 от настоящия Регламент;

**ПРИЛОЖЕНИЕ: СПИСЪК НА ОБРАЗОВАНИЯТА ИЛИ ЛИЦАТА,
ПРЕДОСТАВИЛИ ИНФОРМАЦИЯ НА ДОКЛАДЧИКА**

Следният списък е изготвен на доброволни начала в рамките на изключителната отговорност на докладчика. В хода на изготвянето на проекта на становище следните образования или лица са предоставили информация на докладчика:

Образование и/или лице
Apple
BDI Federation of German Industries
BEUC
BSA The Software Alliance
Confederation of Danish Industries
Digital Europe
ETNO
Kaspersky
Microsoft
Samsung
TIC Council
Xiaomi

ПРОЦЕДУРА НА ПОДПОМАГАЩАТА КОМИСИЯ

Пълни заглавия	Хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и изменение на Регламент (ЕС) 2019/1020		
Позовавания	COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)		
Водеща комисия Дата на обявяване в заседание	ITRE 9.11.2022		
Становище на Дата на обявяване в заседание	IMCO 9.11.2022		
Асоциирани комисии - Дата на обявяване в заседание	20.4.2023		
Докладчик по становище Дата на назначаване	Morten Løkkegaard 16.12.2022		
Разглеждане в комисия	2.3.2023	25.4.2023	23.5.2023
Дата на приемане	29.6.2023		
Резултат от окончателното гласуване	+: -: 0:	41 1 0	
Членове, присъствали на окончателното гласуване	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Biljana Borzan, Vlad-Marius Botoș, Anna Cavazzini, Dita Charanzová, Deirdre Clune, David Cormand, Alexandra Geese, Maria Grapini, Svenja Hahn, Krzysztof Hetman, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Kateřina Konečná, Andrey Kovatchev, Maria-Manuel Leitão-Marques, Antonius Manders, Beata Mazurek, Leszek Miller, Anne-Sophie Pelletier, Miroslav Radačovský, René Repasi, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Kim Van Sparrentak, Marion Walsmann		
Заместници, присъствали на окончателното гласуване	Marco Campomenosi, Maria da Graça Carvalho, Geoffroy Didier, Francisco Guerreiro, Tsvetelina Penkova, Catharina Rinzema, Kosma Złotowski		
Заместници (чл. 209, пар. 7), присъствали на окончателното гласуване	Asger Christensen, Nicolás González Casares, Grzegorz Tobiszowski		

ПОИМЕННО ОКОНЧАТЕЛНО ГЛАСУВАНЕ В ПОДПОМАГАЩАТА КОМИСИЯ

41	+
ECR	Beata Mazurek, Grzegorz Tobiszowski, Kosma Złotowski
ID	Alessandra Basso, Marco Campomenosi, Virginie Joron
NI	Miroslav Radačovský
PPE	Pablo Arias Echeverría, Maria da Graça Carvalho, Deirdre Clune, Geoffroy Didier, Krzysztof Hetman, Arba Kokalari, Andrey Kovatchev, Antonius Manders, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Marion Walsmann
Renew	Andrus Ansip, Vlad-Marius Botoș, Dita Charanzová, Asger Christensen, Svenja Hahn, Catharina Rinzema
S&D	Alex Agius Saliba, Biljana Borzan, Nicolás González Casares, Maria Grapini, Maria-Manuel Leitão-Marques, Leszek Miller, Tsvetelina Penkova, René Repasi, Christel Schaldemose
The Left	Kateřina Konečná, Anne-Sophie Pelletier
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Francisco Guerreiro, Kim Van Sparrentak

1	-
ECR	Eugen Jurzyca

0	0

Легенда на използваните знаци:

+ : „за“

- : „против“

0 : „въздържал се“