Съвет на
Европейския съюз

Брюксел, 16 септември 2022 г.
(OR. en)

12429/22

Междуинституционално досие:
2022/0272(COD)

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

ПРЕДЛОЖЕНИЕ

От:	Генералния секретар на Европейската комисия, подписано от г-жа MARTINE DEPREZ, директор
Дата на получаване:	15 септември 2022 г.
До:	Генералния секретариат на Съвета
№ док. Ком.:	COM(2022) 454 final
Относно:	Предложение 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

Приложено се изпраща на делегациите документ COM(2022) 454 final.

Приложение: COM(2022) 454 final

ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 15.9.2022 г.
COM(2022) 454 final

2022/0272 (COD)

Предложение 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

(текст от значение за ЕИП)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

ОБЯСНИТЕЛЕН МЕМОРАНДУМ

1. КОНТЕКСТ НА ПРЕДЛОЖЕНИЕТО

• Основания и цели на предложението

Хардуерните и софтуерните продукти все по-често стават обект на успешни кибератаки, което води до годишни разходи, дължащи се на киберпрестъпност, в световен мащаб, които се оценяват на 5,5 трилиона евро до 2021 г. Тези продукти имат два основни проблема, които увеличават разходите за ползвателите и обществото: 1) ниско ниво на киберсигурност, което се изразява в широко разпространени уязвимости и недостатъчно и непоследователно предоставяне на актуализации на защитата за справяне с тях, и 2) 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. В свързана среда киберинцидент в един продукт може да засегне цяла организация или цяла верига на доставки, като често се разпространява през границите на вътрешния пазар в рамките на няколко минути. Това може да доведе до сериозно нарушаване на икономическите и социалните дейности или дори да има животозастрашаващи последици.

Киберсигурността на продуктите с цифрови елементи има силно трансгранично измерение, тъй като продуктите, произведени в една държава, често се използват в целия вътрешен пазар. Освен това инцидентите, които първоначално засягат един субект или една държава членка, често се разпространяват в рамките на минути на целия вътрешен пазар.

Въпреки че действащото законодателство в областта на вътрешния пазар се прилага към някои продукти с цифрови елементи, повечето хардуерни и софтуерни продукти понастоящем не са обхванати от никакво законодателство на ЕС, занимаващо се с тяхната киберсигурност. По-специално в настоящата правна рамка на ЕС не се разглежда киберсигурността на невградения софтуер, въпреки че атаките срещу киберсигурността все по-често са насочени към уязвимости в тези продукти, което води до значителни обществени и икономически разходи. Има многобройни примери за забележителни кибератаки в резултат на неоптимална защита на продуктите, като например криптовирусът червей WannaCry, който използва уязвимост на Windows, засегна 200 000 компютъра в 150 държави през 2017 г. и нанесе щети за милиарди щатски долари; атаката на веригата за доставки Kaseya VSA, при която чрез софтуера за мрежово администриране на Kaseya бяха атакувани над 1000 дружества и верига супермаркети беше принудена да затвори всичките си 500 магазина в Швеция; или многобройните инциденти, при които банкови приложения стават обект на хакерска атака с цел да бъдат откраднати пари от нищо неподозиращи потребители.

Поставени бяха две основни цели, които да осигурят правилното функциониране на вътрешния пазар: 1) създаване на условия за разработване на защитени продукти с цифрови елементи, като се гарантира, че на пазара се пускат хардуерни и софтуерни продукти с по-малко уязвимости, както и че производителите се отнасят сериозно към защитата през целия жизнен цикъл на продукта; и 2) създаване на условия, които позволяват на ползвателите да вземат предвид киберсигурността при избора и използването на продукти с цифрови елементи. Определени бяха четири специфични цели: i) да се гарантира, че производителите подобряват защитата на продуктите с цифрови елементи още от етапа на проектиране и разработване и през целия жизнен цикъл; ii) да се осигури съгласувана рамка за киберсигурност, която улеснява

спазването на изискванията от производителите на хардуер и софтуер; iii) да се повиши прозрачността на характеристиките за защитата на продуктите с цифрови елементи и iv) да се даде възможност на предприятията и потребителите да използват продуктите с цифрови елементи по безопасен начин.

Силно изразеният трансграничен характер на киберсигурността и нарастващият брой инциденти, които се разпространяват в други държави, сектори и продукти, означават, че целите не могат да бъдат постигнати ефективно само от държавите членки. Предвид глобалния характер на пазарите на продукти с цифрови елементи, държавите членки са изправени пред едни и същи рискове за един и същ продукт с цифрови елементи на тяхна територия. Възникващата фрагментирана рамка от потенциално различаващи се национални правила рискува да попречи на отворения и конкурентен единен пазар за продукти с цифрови елементи. Следователно са необходими съвместни действия на равнището на ЕС, за да се повиши доверието на ползвателите и привлекателността на продуктите с цифрови елементи в ЕС. Това би било от полза и за вътрешния пазар, като се осигури правна сигурност и се постигнат равнопоставени условия на конкуренция за доставчиците на продукти с цифрови елементи, както се подчертава и в окончателния доклад на Конференцията за бъдещето на Европа, в който гражданите призовават за по-силна роля на ЕС в борбата със заплахите за киберсигурността.

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

Рамката на ЕС се състои от няколко хоризонтални законодателни акта, които обхващат определени аспекти, свързани с киберсигурността, от различни гледни точки (продукти, услуги, управление на кризи и престъпления). През 2013 г. влезе в сила Директивата относно атаките срещу информационните системи[1], с която се хармонизират криминализирането и наказанията за редица престъпления, насочени срещу информационните системи. През август 2016 г. влезе в сила Директива (ЕС) 2016/1148 за мрежова и информационна сигурност (Директивата за МИС)[2], която е първият законодателен акт в целия ЕС в областта на киберсигурността. Нейното преразглеждане, в резултат на което беше приета [Директива XXX/XXXX (МИС 2)], повишава общото равнище на амбиция на ЕС. През 2019 г. влезе в сила Актът за киберсигурността на ЕС[3], чиято цел е да се повиши защитата на ИКТ продуктите, ИКТ услугите и ИКТ процесите чрез въвеждане на доброволна Европейска рамка за сертифициране на киберсигурността[4].

---

1 Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета (ОВ L 218, 14.8.2013 г., стр. 8—14).

2 Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194/1, 19.7.2016 г., стр. 1).

3 Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019 г., стр. 15).

4 Актът за киберсигурността позволява разработването на специални схеми за сертифициране. Всяка схема включва препратки към съответните стандарти, технически спецификации или други изисквания за киберсигурност, определени в схемата. Решението за разработване на сертифициране за киберсигурност се основава на риска.

Киберсигурността на цялата верига на доставките е гарантирана единствено ако всички нейни компоненти са защитени по отношение на киберзаплахите. Горепосоченото законодателство на ЕС обаче има съществени пропуски в това отношение, тъй като не включва задължителни изисквания за защитата на продукти с цифрови елементи.

Въпреки че предложеният Законодателен акт за киберустойчивост обхваща продукти с цифрови елементи, пуснати на пазара, [Директива XXX/XXXX (МИС 2)] има за цел да осигури високо равнище на киберсигурност на услугите, предоставяни от съществени и важни субекти. Съгласно [Директива XXX/XXXX (МИС 2)] от държавите членки се изисква да гарантират, че основни и важни субекти, които са обхванати от нея, като например доставчици на здравно обслужване или доставчици на компютърни услуги „в облак“ и субекти на държавната администрация, предприемат подходящи и пропорционални технически, оперативни и организационни мерки за киберсигурност. Това включва, наред с другото, изискване за гарантиране на защитата при придобиването, разработването и поддръжката на мрежи и информационни системи, включително отстраняването и оповестяването на уязвимости. Съгласно [Директива XXX/XXXX (МИС 2)] от Комисията се изисква да приеме актове за изпълнение за определяне на техническите и методологическите изисквания на тези мерки в срок от 21 месеца след датата на влизане в сила на тази директива за някои видове субекти, като например доставчиците на облачни услуги. За всички останали субекти Комисията може да приеме акт за изпълнение за определяне на техническите и методологическите изисквания, както и секторните изисквания. Тази рамка ще гарантира, че техническите спецификации и мерки, подобни на основните изисквания за киберсигурност от Законодателния акт за киберустойчивост, се прилагат и при проектирането, разработването и отстраняването на уязвимостите на софтуера, предоставян като услуга (софтуер като услуга). Например това би могло да бъде средство за гарантиране на високо равнище на киберсигурност в случаи като системите за електронни здравни досиета (ЕЗД), включително когато се предоставят като софтуер като услуга (SaaS) или се разработват в рамките на здравните институции (вътрешно), в съответствие с предложения [Регламент относно европейското пространство на здравни данни].

- **Взаимодействие с други политики на Съюза**

Както бе посочено в съобщението „Изграждане на цифровото бъдеще на Европа“[5], за ЕС е от решаващо значение да се възползва от всички предимства на цифровата ера и да укрепи своята промишленост и иновационен капацитет в рамките на безопасни и етични граници. В Европейската стратегия за данните се определят четири стълба — защита на данните, основни права, безопасност и киберсигурност — като основни необходими условия за общество, което разполага с възможността за използване на данни.

Настоящата рамка на ЕС[6], приложима за продукти, които също може да имат цифрови елементи, включва няколко законодателни акта, включително законодателство на ЕС относно конкретни продукти, обхващащо аспекти, свързани с безопасността, и общо законодателство относно отговорността за продуктите. Предложението е в съответствие с действащата регулаторна рамка на ЕС, свързана с продуктите, както и с

[5] Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите „Изграждане на цифровото бъдеще на Европа“ от 19 февруари 2020 г., COM(2020) 67 final.

[6] Предимно законодателство на новата законодателна рамка (НЗР).

неотдавнашни законодателни предложения, като например предложението на Комисията за [Регламент относно изкуствения интелект (ИИ)][7].

Предложеният регламент ще се прилага за всички радиосъоръжения, попадащи в обхвата на Делегиран регламент (ЕС) 2022/30 на Комисията. Освен това изискванията, определени в този регламент, включват всички елементи на съществените изисквания, посочени в член 3, параграф 3, букви г), д) и е) от Директива 2014/53/ЕС, включително основните елементи, посочени в [Решение за изпълнение XXX/2022 на Комисията относно искане за стандартизация, отправено до европейските организации за стандартизация], издадено въз основа на посочения делегиран регламент. За да се избегне регулаторно припокриване, се предвижда Комисията да отмени или измени делегирания регламент по отношение на радиосъоръженията, обхванати от предложения регламент, така че последният да се прилага към тях след влизането му в сила.

Освен това, за да се избегне дублиране на работата, се предвижда при изготвянето и разработването на хармонизирани стандарти за улесняване на прилагането на регламента, Комисията и европейските организации за стандартизация да вземат предвид работата по стандартизация, извършена в контекста на Решение за изпълнение C(2022)5637 на Комисията относно искане за стандартизация за Делегиран регламент 2022/30 относно радиосъоръженията.

2. ПРАВНО ОСНОВАНИЕ, СУБСИДИАРНОСТ И ПРОПОРЦИОНАЛНОСТ

• Правно основание

Правното основание за настоящото предложение е член 114 от Договора за функционирането на Европейския съюз (ДФЕС), в който е предвидено приемането на мерки за осигуряване на създаването и функционирането на вътрешния пазар. Целта на предложението е да се хармонизират изискванията за киберсигурността на продуктите с цифрови елементи във всички държави членки и да се премахнат пречките пред свободното движение на стоки.

Член 114 от ДФЕС може да се използва като правно основание за предотвратяване на появата на тези пречки, произтичащи от различията в националните законодателства и подходи относно начините за преодоляване на правната несигурност и пропуските в съществуващите правни рамки[8]. Освен това Съдът на ЕС призна, че прилагането на разнородни технически изисквания може да бъде валидно основание за задействане на член 114 от ДФЕС[9].

Настоящата законодателна рамка на ЕС, приложима за продукти с цифрови елементи, се основава на член 114 от ДФЕС и включва няколко законодателни акта, включително за конкретни продукти и аспекти, свързани с безопасността, или общо законодателство

---

[7] Предложение за Регламент на Европейския парламент и на Съвета за определяне на хармонизирани правила относно изкуствения интелект (Законодателен акт за изкуствения интелект) и за изменение на някои законодателни актове на Съюза от 21 април 2021 г., COM(2021) 206 final.

[8] Решение на Съда на Европейския съюз (голям състав) от 3 декември 2019 г., Чешка република срещу Европейски парламент и Съвет на Европейския съюз, Дело C-482/17, точка 35.

[9] Решение на Съда на Европейския съюз (голям състав) от 2 май 2006 г., Обединено кралство Великобритания и Северна Ирландия срещу Европейски парламент и Съвет на Европейския съюз, Дело C-217/04, точки 62—63.

относно отговорността за продуктите. Тя обаче обхваща само някои аспекти, свързани с киберсигурността на материалните цифрови продукти и, когато е приложимо, на софтуера, вграден в тези продукти. На национално равнище държавите членки започват да предприемат национални мерки, които изискват от доставчиците на цифрови продукти да повишат тяхната киберсигурност[10]. Същевременно киберсигурността на цифровите продукти има особено силно трансгранично измерение, тъй като продуктите, произведени в една държава, често се използват от организации и потребители в целия вътрешен пазар. Инциденти, които първоначално засягат един субект или държава членка, често се разпространяват в рамките на няколко минути в организации, сектори и няколко държави членки.

Различните актове и инициативи, предприети досега на равнището на ЕС и на национално равнище, решават само частично установените проблеми и пораждат риск от създаване на разнородно законодателство в рамките на вътрешния пазар, като увеличават правната несигурност както за доставчиците, така и за ползвателите на тези продукти и създават ненужна тежест за дружествата да спазват редица изисквания за подобни видове продукти.

Предложеният регламент ще хармонизира и рационализира нормативната уредба на ЕС, като въведе изисквания за киберсигурност за продукти с цифрови елементи и ще избегне припокриването на изисквания, произтичащи от различни законодателни актове. Това ще доведе до по-голяма правна сигурност за операторите и ползвателите в целия Съюз, както и по-добра хармонизация на европейския единен пазар, като се създадат по-благоприятни условия за операторите, които се стремят да навлязат на пазара на ЕС.

- **Субсидиарност (при неизключителна компетентност)**

Силно изразеният трансграничен характер на киберсигурността като цяло и нарастващият брой на рисковете и инцидентите, които се разпространяват в други държави, сектори и продукти, означават, че целите на настоящата намеса не могат да бъдат постигнати ефективно само от държавите членки. Националните подходи при решаването на проблемите, и по-специално подходите, въвеждащи задължителни изисквания, ще създадат допълнителна правна несигурност и правни пречки. Безпроблемното разширяване на дейността на дружествата в други държави членки може да бъде възпрепятствано и по този начин ползвателите да бъдат лишени от ползите на техните продукти.

Следователно е необходимо съвместно действие на равнището на ЕС, за да се установи високо ниво на доверие сред ползвателите, което да увеличи привлекателността на продуктите на ЕС с цифрови елементи. Това ще бъде от полза и за цифровия единен пазар и вътрешния пазар като цяло, като се осигури правна сигурност и се постигнат равнопоставени условия на конкуренция за производителите на продукти с цифрови елементи.

В крайна сметка в заключенията на Съвета от 23 май 2022 г. относно развитието на киберсигурността на Европейския съюз Комисията се призовава да предложи общи изисквания за киберсигурност за свързаните устройства до края на 2022 г.

[10] Например през 2019 г. Финландия създаде схема за етикетиране на устройствата от областта на интернет на нещата, като например интелигентни телевизори, смартфони и играчки, въз основа на стандартите на ETSI. Германия наскоро въведе етикет за потребителска сигурност за широколентови маршрутизатори, интелигентни телевизори, камери, говорители, играчки, както и за роботи за почистване и градинарство.

- **Пропорционалност**

По отношение на пропорционалността на предложения регламент мерките в разгледаните варианти на политиката няма да надхвърлят необходимото за постигане на общите и специфичните цели и няма да наложат непропорционални разходи. По-конкретно разглежданата намеса ще гарантира, че продуктите с цифрови елементи ще бъдат защитени през целия им жизнен цикъл и пропорционално на рисковете, пред които са изправени, чрез обективно ориентирани и технологично неутрални изисквания, които остават разумни и като цяло отговарят на интересите на засегнатите субекти.

Съществените изисквания за киберсигурност в предложението се основават на широко използвани стандарти, а в процеса на стандартизация, който ще последва, ще бъдат взети предвид техническите особености на продуктите. Това означава, че контролът по сигурността ще бъде адаптиран, когато е необходимо за дадено ниво на риск. Освен това предвидените хоризонтални правила ще предвиждат оценка от трета страна само за критични продукти. Това ще включва само малък дял от пазара на продукти с цифрови елементи. Въздействието върху МСП ще зависи от тяхното присъствие на пазара на тези специфични категории продукти.

По отношение на пропорционалността на разходите за оценяване на съответствието, нотифицираните органи, които извършват оценките от трети страни, ще вземат предвид размера на предприятието при определяне на своите такси. Ще бъде предвиден и разумен преходен период от 24 месеца за подготовка на изпълнението, през който съответните пазари ще имат време да се подготвят, като същевременно бъде осигурена ясна насока за инвестициите в НИРД. Евентуалните разходи на предприятията за привеждане в съответствие ще бъдат компенсирани от ползите, които ще донесе по-високото ниво на сигурност на продуктите с цифрови елементи и в крайна сметка повишаването на доверието на ползвателите в тези продукти.

- **Избор на инструмент**

Регулаторната намеса би означавала приемането на регламент, а не на директива. Причината за това е, че за този конкретен вид продуктово законодателство регламентът би бил по-ефективен за решаване на установените проблеми и за постигане на формулираните цели, тъй като става въпрос за намеса, която обуславя пускането на вътрешния пазар на много широка категория продукти. Процесът на транспониране в случай на директива за подобна намеса би могъл да остави твърде голяма свобода на преценка на национално равнище, което потенциално би довело до липса на единство на някои съществени изисквания за киберсигурност, правна несигурност, допълнителна разпокъсаност или дори дискриминационни ситуации в трансграничен план, още повече като се има предвид фактът, че обхванатите продукти могат да бъдат с различно предназначение или употреба и че производителите могат да произвеждат множество категории такива продукти.

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

- **Консултации със заинтересованите страни**

Комисията се консултира с широк кръг от заинтересовани страни. Държавите членки и заинтересованите страни бяха поканени да участват в откритата обществена консултация, както и в проучванията и работните срещи, организирани в контекста на проучване, проведено от обединение, което подпомага подготвителната работа на

Комисията за оценката на въздействието: Wavestone, Център за европейски политически изследвания (CEPS) и ICF. Заинтересованите страни, с които бяха проведени консултации, включваха национални органи за надзор на пазара, органи на Съюза, занимаващи се с киберсигурност, производители на хардуер и софтуер, вносители и дистрибутори на хардуер и софтуер, търговски органи, потребителски организации и ползватели на продукти с цифрови елементи и граждани, изследователи и представители на академичните среди, нотифицирани органи и органи по акредитация, както и професионалисти от сектора на киберсигурността.

Консултациите включваха:

- Първото проучване, проведено от обединение, съставено от ICF, Wavestone, Carsa и CEPS, което е публикувано през декември 2021 г.[11] В проучването бяха установени няколко пазарни дефекта и бяха оценени възможните регулаторни намеси.
- Открита обществена консултация, която беше насочена към граждани, заинтересовани страни и експерти по киберсигурност. Бяха представени 176 отговора. Те допринесоха за събирането на разнообразни мнения и опит от всички групи заинтересовани страни.
- В работните срещи, организирани в рамките на проучването в подкрепа на подготвителната работа на Комисията за Законодателен акт за киберустойчивост, участваха около 100 представители от всички 27 държави членки, представляващи различни заинтересовани страни.
- Проведени бяха интервюта с експерти, за да се постигне по-задълбочено разбиране на настоящите предизвикателства в областта на киберсигурността, свързани с продуктите с цифрови елементи, и да се обсъдят варианти на политиката за потенциална регулаторна намеса.
- Проведени бяха двустранни обсъждания с национални органи по киберсигурност, частния сектор и потребителски организации.
- Проведени бяха целенасочени информационни кампании с ключови заинтересовани страни от МСП.

- **Събиране и използване на експертни становища**

Консултациите имаха за цел да се получи информация за петте основни критерия за оценка, основани на насоките на ЕС за по-добро регулиране (ефективност, ефикасност, адекватност, съгласуваност, добавена стойност за ЕС), както и за потенциалните въздействия на възможните варианти за бъдещето. Изпълнителят се обърна не само към заинтересованите страни, които биха били пряко засегнати от предложения регламент, но се консултира и с широк кръг експерти в областта на киберсигурността.

- **Оценка на въздействието**

Комисията извърши оценка на въздействието на настоящото предложение, разгледана от Комитета за регулаторен контрол (КРК) на Комисията. На 6 юли 2022 г. беше проведе среща с КРК, която беше последвана от положително становище. Оценката на

[11] Проучване на необходимостта от изисквания за киберсигурност за ИКТ продукти — № 2020—0715, окончателен доклад от проучването, достъпен на https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products.

въздействието беше коригирана, за да се вземат предвид препоръките и коментарите на КРК.

Комисията разгледа различни варианти на политиката за постигане на общата цел на предложението:

- Акт с незадължителен характер и доброволни мерки (вариант 1): При този вариант няма да има задължителна регулаторна намеса. Вместо това Комисията ще публикува съобщения, насоки, препоръки и евентуално кодекси за поведение, за да насърчи доброволните мерки. Националните схеми, доброволни или задължителни, ще продължат да се разработват, за да компенсират липсата на хоризонтални правила на ЕС.
- Допълнителна регулаторна намеса за киберсигурността на материални продукти с цифрови елементи и съответния вграден софтуер (вариант 2): Този вариант би довел до допълнителна регулаторна намеса за конкретен продукт, която би се ограничила до добавяне и/или изменение на изискванията за киберсигурност във вече съществуващото законодателство или до въвеждане на ново законодателство при поява на нови рискове, включително потенциално за невграден софтуер.

Варианти 3 и 4 предполагат хоризонтална регулаторна намеса с различен обхват, която до голяма степен следва новата законодателна рамка (НЗР). Тази рамка определя съществените изисквания като условие за пускането на определени продукти на вътрешния пазар. В НЗР обикновено се предвижда и оценяване на съответствието — процес, който се извършва от производителя, за да докаже дали са изпълнени определените изисквания, свързани с даден продукт.

- Смесен подход, включващ хоризонтални задължителни правила за киберсигурност на материални продукти с цифрови елементи и съответния вграден софтуер и поетапен подход за невградения софтуер (вариант 3): този вариант ще включва регламент, с който се въвеждат хоризонтални изисквания за киберсигурност за всички материални продукти с цифрови елементи и вградения в тях софтуер като условие за пускане на пазара, както и два подварианта — със и без задължителна оценка от трета страна (3i и 3ii). Софтуерът, който не е вграден, няма да бъде регулиран.
- Хоризонтална регулаторна намеса, с която се въвеждат изисквания за киберсигурност за широк набор от материални и нематериални продукти с цифрови елементи, включително невграден софтуер (вариант 4): този вариант е сходен с вариант 3, с изключение на обхвата. Вариант 4 включва невграден софтуер (с два подварианта, включващи съответно само критичен (4а) или целия софтуер (4б)) в обхвата на потенциалния регламент. За всеки подвариант ще бъдат разгледани същите подварианти, свързани с оценката на съответствието, както при вариант 3.

Вариант 4 (с подварианти, обхващащи целия софтуер и включващи задължителна оценка от трета страна за критични продукти) се очертава като предпочитан вариант въз основа на оценката на ефективността спрямо специфичните цели и ефикасността на разходите спрямо ползите. Този вариант би гарантирал определянето на специфични хоризонтални изисквания за киберсигурност за всички продукти с цифрови елементи, които се пускат или предоставят на вътрешния пазар, и би бил единственият вариант,

обхващащ цялата цифрова верига на доставки. Невграденият софтуер, който често е изложен на уязвимости, също ще бъде обхванат от такава регулаторна намеса, като по този начин ще се осигури съгласуван подход към всички продукти с цифрови елементи, с ясно разпределение на отговорностите за различните икономически оператори.

Този вариант на политиката носи и добавена стойност, тъй като обхваща задължението за полагане на дължима грижа и аспектите на целия жизнен цикъл след пускането на продуктите с цифрови елементи на пазара, за да се гарантира, наред с другото, подходяща информация за поддръжка на защитата и предоставяне на актуализации на защитата. Този вариант на политиката би допълнил по най-ефективен начин неотдавнашния преглед на рамката за МИС, като осигури предпоставките за засилена сигурност на веригата на доставките.

Предпочитаният вариант би донесъл значителни ползи за различните заинтересовани страни. За предприятията той би предотвратил различаващите се правила за сигурността за продукти с цифрови елементи и би намалил разходите за привеждане в съответствие със свързаното законодателство в областта на киберсигурността. Той би намалил броя на киберинцидентите, разходите за действията при инцидент и накърняването на репутацията. За целия ЕС се смята, че инициативата би могла да доведе до намаляване на разходите от инциденти, засягащи дружествата, с около 180—290 млрд. евро годишно. В резултат на това би се увеличил оборотът поради повишеното търсене на продукти с цифрови елементи. Съответно би се подобрила репутацията на дружествата в световен мащаб, което води до увеличаване на търсенето и извън ЕС. За ползвателите предпочитаният вариант би повишил прозрачността на характеристиките на сигурността и би улеснил използването на продуктите с цифрови елементи. Потребителите и гражданите ще се възползват и от по-добрата защита на основните си права, като неприкосновеност на личния живот и защита на личните данни.

Когато бе поискано да оценят ефективността на политическите намеси, участниците в обществената консултация се съгласиха, че вариант 4 би бил най-ефективната мярка (4,08 по скалата от 1 до 5). В това число влизат потребителските организации (5,00), респондентите, определящи себе си като ползватели (4,22), нотифицираните органи (4,17), органите за надзор на пазара (5,00) и производителите на продукти с цифрови елементи (3,85), включително малките и средните предприятия (4,05).

- **Пригодност и опростяване на законодателството**

В настоящото предложение се определят изискванията, които ще се прилагат към производителите на софтуер и хардуер. Необходимо е да се осигури правна сигурност и да се избегне допълнителна разпокъсаност на пазара на свързаните с продуктите изисквания за киберсигурност на вътрешния пазар, което се доказва от широката подкрепа на различните заинтересовани страни за хоризонтална намеса. Предложението ще сведе до минимум регулаторната тежест, наложена на производителите от няколко акта за безопасност на продуктите. Привеждането в съответствие с НЗР означава по-добро функциониране на намесата и нейното прилагане. Предложението рационализира процеса на предпазните процедури, като включва производителите и държавите членки преди уведомяването на Комисията. Голяма част от производителите, попадащи в обхвата на предложението, вече са запознати с функционирането на НЗР, което ще допринесе за нейното разбиране и прилагане. По отношение на потребителите и дружествата предложението ще насърчи доверието в продуктите с цифрови елементи.

- **Основни права**

Очаква се всички варианти на политиката да засилят до известна степен защитата на основните права и свободи, като неприкосновеност на личния живот, защита на личните данни, свобода на стопанската инициатива и защита на собствеността или личното достойнство и почтеност. По-специално предпочитаният вариант на политиката 4, състоящ се от хоризонтални регулаторни намеси и широк обхват на политиката, би бил най-ефективен в това отношение, тъй като е по-вероятно да спомогне за намаляване на броя и сериозността на инцидентите, включително нарушенията на сигурността на личните данни. Той също така би увеличил правната сигурност и би довел до равнопоставени условия на конкуренция за икономическите оператори, би повишил доверието на ползвателите и привлекателността на продуктите на ЕС с цифрови елементи като цяло, като по този начин ще бъде защитена собствеността и ще се подобрят условията за осъществяване на стопанска дейност от икономическите оператори.

Хоризонталните изисквания за киберсигурност ще допринесат за сигурността на личните данни чрез защита на поверителността, целостта и наличността на информацията в продуктите с цифрови елементи. Спазването на тези изисквания ще улесни спазването на изискването за сигурност на обработването на лични данни съгласно Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните — ОРЗД)[12]. Предложението ще повиши прозрачността и информираността на ползвателите, включително и на тези, които може да са с по-слаби умения в областта на киберсигурността. Ползвателите ще бъдат също така по-добре информирани за рисковете, възможностите и ограниченията на продуктите с цифрови елементи, което ще ги постави в по-добра позиция да предприемат необходимите превантивни и смекчаващи мерки за намаляване на остатъчните рискове.

4. ОТРАЖЕНИЕ ВЪРХУ БЮДЖЕТА

За да изпълни възложените ѝ задачи съгласно настоящия регламент, Агенцията на Европейския съюз за киберсигурност (ENISA) ще трябва да преразпредели ресурси в размер на приблизително 4,5 ЕПРВ. Комисията ще трябва да разпредели 7 ЕПРВ, за да изпълни задълженията си, свързани с прилагането на настоящия регламент.

Подробен преглед на свързаните разходи е представен във „финансовата обосновка“ към настоящото предложение.

5. ДРУГИ ЕЛЕМЕНТИ

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

Комисията ще наблюдава изпълнението, прилагането и спазването на тези нови разпоредби, за да оцени тяхната ефективност. В това отношение регламентът ще изисква оценка и преглед от страна на Комисията и представяне на публичен доклад на Европейския парламент и на Съвета до 36 месеца след датата на прилагане и на всеки четири години след това.

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

- **Подробно разяснение на конкретните разпоредби на предложението**

Общи разпоредби (глава I)

С настоящото предложение за регламент се установяват: а) правила за пускането на пазара на продукти с цифрови елементи, за да се гарантира киберсигурността на тези продукти; б) съществени изисквания за проектирането, разработването и производството на продукти с цифрови елементи, както и задължения за икономическите оператори във връзка с тези продукти по отношение на киберсигурността; в) съществени изисквания за процесите на отстраняване на уязвимостите, въведени от производителите, за да се гарантира киберсигурността на продуктите с цифрови елементи през целия им жизнен цикъл, и задължения за икономическите оператори във връзка с тези процеси; г) правила за надзор на пазара и правоприлагане на горепосочените правила и изисквания.

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

Предложеният регламент няма да се прилага за продукти с цифрови елементи в обхвата на Регламент (ЕС) 2017/745 [медицински изделия за хуманна употреба и принадлежности за такива изделия] и Регламент (ЕС) 2017/746 [медицински изделия за инвитро диагностика за хуманна употреба и принадлежности за такива изделия], тъй като и двата регламента съдържат изисквания по отношение на изделията, включително по отношение на софтуера, и общи задължения за производителите, обхващащи целия жизнен цикъл на изделията, както и процедури за оценяване на съответствието. Настоящият регламент няма да се прилага за продукти с цифрови елементи, които са сертифицирани в съответствие с Регламент 2018/1139 [високо и еднакво равнище на безопасност на гражданското въздухоплаване], нито за продукти, за които се прилага Регламент (ЕС) 2019/2144 [относно изискванията за одобряване на типа на моторни превозни средства и техните ремаркета, както и на системи, компоненти и отделни технически възли, предназначени за такива превозни средства].

Критичните продукти с цифрови елементи подлежат на специфични процедури за оценяване на съответствието и се разделят на клас I и клас II, както е посочено в приложение III, което отразява нивото на киберриска, като клас II представлява по-голям риск. Даден продукт с цифрови елементи се приема за критичен и поради това се включва в приложение III, като се отчита въздействието на потенциалните уязвимости на киберсигурността, включени в продукта с цифрови елементи. При определянето на киберриска се вземат предвид, наред с другото, свързаните с киберсигурността функционални възможности на продукта с цифрови елементи и предвидената му употреба в чувствителна среда, като например в промишлена среда.

Комисията има също така правомощието да приема делегирани актове 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, 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, приети за включването на продукти с цифрови елементи с висока степен на критичност в списъка на приложение III, както и с оглед на оценката дали тази категория продукти се използва

или на нея се разчита от основните субекти от вида, посочен в [приложение I] към [Директива XXX/XXXX (МИС 2)], или ще има потенциално бъдещо значение за дейността на тези субекти; или е от значение за устойчивостта на цялата верига на доставките на продукти с цифрови елементи срещу смущаващи събития.

Задължения на икономическите оператори (глава II)

С предложението се въвеждат задължения за производителите, вносителите и дистрибуторите въз основа на Решение 768/2008/ЕО. Съществените изисквания и задълженията в областта на киберсигурността предвиждат, че всички продукти с цифрови елементи се предлагат на пазара само ако при надлежна доставка, правилно монтиране, извършване на техническа поддръжка и използване по предназначение, което може да бъде разумно предвидено, отговарят на съществените изисквания за киберсигурност, посочени в настоящия регламент.

Съществените изисквания и задължения ще задължат производителите да отчитат киберсигурността при проектирането, разработването и производството на продукти с цифрови елементи, да полагат дължимата грижа за аспектите на сигурността при проектирането и разработването на своите продукти, да бъдат прозрачни по отношение на аспектите на киберсигурността, които трябва да бъдат съобщени на клиентите, да осигуряват поддръжка на сигурността (актуализации) по пропорционален начин и да спазват изискванията за отстраняване на уязвимости.

За икономическите оператори — от производителите до дистрибуторите и вносителите, ще бъдат установени задължения във връзка с пускането на пазара на продукти с цифрови елементи, които да са адекватни на тяхната роля и отговорности във веригата на доставките.

Съответствие на продукта с цифрови елементи (глава III)

За продуктъа с цифрови елементи, който съответства на хармонизираните стандарти или части от тях, данните за които са били публикувани в *Официален вестник на Европейския съюз*, се приема, че съответства на установените в приложение I съществени изисквания от предложения регламент. Когато не съществуват хармонизирани стандарти или те са недостатъчни, или когато има неоправдано забавяне в процедурата по стандартизация, или когато искането на Комисията не е било прието от европейските организации по стандартизация, Комисията може, посредством актове за изпълнение, да приеме общи спецификации.

Освен това за продуктите с цифрови елементи, които са сертифицирани или за които е издадена ЕС декларация за съответствие или сертификат по европейска схема за сертифициране на киберсигурността съгласно Регламент (ЕС) 2019/881 и за които Комисията е посочила чрез акт за изпълнение, че може да предостави презумпция за съответствие с настоящия регламент, се приема, че съответстват на съществените изисквания на настоящия регламент или на части от него, доколкото ЕС декларацията за съответствие или сертификатът за киберсигурност, или части от тях, покриват тези изисквания.

Освен това, за да се избегне ненужна административна тежест за производителите, когато е приложимо, Комисията следва да уточни дали сертификат за киберсигурност, издаден по такава европейска схема за сертифициране на киберсигурността, премахва задължението на производителите да извършват оценка на съответствието от трета страна, както е предвидено в настоящия регламент за съответните изисквания.

Производителят извършва оценяване на съответствието на продукта с цифрови елементи и на въведените от него процеси за отстраняване на уязвимостите, за да

докаже съответствието със съществените изисквания, посочени в приложение I, като следва една от процедурите, посочени в приложение VI. Производителите на критични продукти от клас I и II използват съответните модули, необходими за съответствието. Производителите на критични продукти от клас II трябва да включат трета страна в оценяването на съответствието им.

Нотифициране на органите за оценка на съответствието (глава VI)

Правилното функциониране на нотифицираните органи е от ключово значение за осигуряването на високо равнище на киберсигурност, както и на доверие на всички заинтересовани страни към системата на Новия подход. Поради това, в съответствие с Решение 768/2008/ЕО предложението определя изисквания за националните органи, които отговарят за органите за оценка на съответствието (нотифицирани органи). То оставя крайната отговорност за назначаване и наблюдение на нотифицираните органи на държавите членки. Държавите членки трябва да определят нотифициращ орган, отговорен за установяването и провеждането на необходимите процедури за оценка и нотифициране на органите за оценяване на съответствието, както и за наблюдението на тези нотифицирани органи, включително на тяхното съответствие с посоченото в член 24.

Надзор на пазара и правоприлагане (глава V)

В съответствие с Регламент (ЕС) 2019/1020 националните органи за надзор на пазара осъществяват надзор на пазара на територията на съответната държава членка. 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, създадени съгласно [член X] от [Директива XXX/XXXX (МИС 2)], или определените национални органи за сертифициране на киберсигурността по член 58 от Регламент (ЕС) 2019/881. От икономическите оператори се изисква да си сътрудничат изцяло с органите за надзор на пазара и с други компетентни органи.

Делегирани правомощия и процедури на комитет (глава VI)

С цел да се гарантира, че регулаторната рамка може да бъде адаптирана, когато е необходимо, на Комисията се предоставя правомощието да приема актове в съответствие с член 290 от ДФЕС за актуализиране на списъка с критични продукти от клас I и II и за уточняване на определенията на тези продукти; уточняване дали е необходимо ограничение или изключване за продукти с цифрови елементи, обхванати от други правила на Съюза, с които се определят изисквания, постигащи същото ниво на защита като настоящия регламент; налагане на задължение за сертифициране на някои продукти с цифрови елементи с висока степен на критичност въз основа на критериите, определени в настоящия регламент; уточняване на минималното съдържание на ЕС декларацията за съответствие и допълване на елементите, които трябва да бъдат включени в техническата документация.

Комисията има също така правомощието да приема актове за изпълнение, с които: да определя формата или елементите на задълженията за докладване и на описа на софтуерните компоненти; да определя европейските схеми за сертифициране на киберсигурността, които могат да се използват за доказване на съответствие със съществените изисквания или части от тях, както е посочено в настоящия регламент; да приема общи спецификации; да определя техническите спецификации за нанасяне на маркировката „CE“; да приема корективни или ограничителни мерки на равнището на

Съюза при извънредни обстоятелства, които оправдават незабавна намеса за запазване на доброто функциониране на вътрешния пазар.

Поверителност и санкции (глава VII)

Всички страни, които прилагат настоящия регламент, зачитат поверителността на информацията и данните, получени при изпълнението на техните задачи и дейности.

За да се гарантира ефективното прилагане на предвидените съгласно настоящия регламент задължения, всеки компетентен орган за надзор на пазара следва да разполага с правомощието да налага или изисква налагането на административни глоби. Също така настоящият регламент установява максимални размери на административните глоби, които следва да бъдат предвидени в националните законодателства при неспазване на задълженията, определени в настоящия регламент.

Преходни и заключителни разпоредби (глава VIII)

За да се даде време на производителите, нотифицираните органи и държавите членки да се адаптират към новите изисквания, предложеният регламент ще започне да се прилага [24 месеца] след влизането му в сила, с изключение на задължението за докладване на производителите, което ще се прилага [12 месеца] след датата на влизане в сила.

2022/0272 (COD)

Предложение 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

(текст от значение за ЕИП)

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

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

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

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

като взеха предвид становището на Комитета на регионите[2],

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

(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.

(2) Настоящият регламент има за цел да определи граничните условия за разработването на защитени продукти с цифрови елементи, като се гарантира, че на пазара се пускат хардуерни и софтуерни продукти с по-малко уязвимости, както и че производителите се отнасят сериозно към сигурността през целия жизнен цикъл на продукта. Той също така има за цел да създаде условия, които позволяват на ползвателите да вземат предвид киберсигурността при избора и използването на продукти с цифрови елементи.

(3) Съответното законодателство на Съюза, което понастоящем е в сила, включва няколко набора от хоризонтални правила, които разглеждат определени аспекти, свързани с киберсигурността, от различни гледни точки, включително мерки за

[1] ОВ С , , стр. .
[2] ОВ С , , стр. .

подобряване на сигурността на цифровата верига на доставките. Съществуващото законодателство на Съюза, свързано с киберсигурността, включително [Директива XXX/XXXX (МИС 2)] и Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета[3], обаче не обхваща пряко задължителните изисквания за сигурността на продуктите с цифрови елементи.

(4) Въпреки че съществуващото законодателство на Съюза се прилага за някои продукти с цифрови елементи, не съществува хоризонтална регулаторна рамка на Съюза, която да установява всеобхватни изисквания за киберсигурност за всички продукти с цифрови елементи. Различните актове и инициативи, предприети до момента на равнището на Съюза и на национално равнище, решават само частично установените проблеми и рискове, свързани с киберсигурността, и пораждат разнородно законодателство в рамките на вътрешния пазар, като увеличават правната несигурност както за производителите, така и за ползвателите на тези продукти и добавят ненужна тежест за дружествата да спазват редица изисквания за подобни видове продукти. Киберсигурността на тези продукти има особено силно трансгранично измерение, тъй като продуктите, произведени в една държава, често се използват от организации и потребители в целия вътрешен пазар. Именно това налага тази област да бъде регулирана на равнището на Съюза. Нормативната уредба на Съюза следва да бъде хармонизирана чрез въвеждане на изисквания за киберсигурност за продуктите с цифрови елементи. Също така следва да се гарантира правна сигурност за операторите и ползвателите в целия Съюз, както и по-добра хармонизация на единния пазар, като се създадат по-жизнеспособни условия за операторите, които се стремят да навлязат на пазара на Съюза.

(5) На равнището на Съюза в различни програмни и политически документи, като Стратегията на ЕС за киберсигурност за цифровото десетилетие[4], заключенията на Съвета от 2 декември 2020 г. и от 23 май 2022 г. или резолюцията на Европейския парламент от 10 юни 2021 г.[5], се призовава за специфични изисквания на Съюза за киберсигурност за цифрови или свързани с интернет продукти, като няколко държави по света въвеждат мерки за решаване на този въпрос по своя собствена инициатива. В заключителния доклад на Конференцията за бъдещето на Европа[6] гражданите призоваха за „по-силна роля на ЕС в противодействието на киберзаплахите“.

(6) За да се повиши общото ниво на киберсигурност на всички продукти с цифрови елементи, пуснати на вътрешния пазар, е необходимо да се въведат обективно ориентирани и технологично неутрални съществени изисквания за киберсигурност за тези продукти, които да се прилагат хоризонтално.

---

[3] Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019 г., стр. 15).

[4] JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/BG/ALL/?uri=JOIN:2020:18:FIN.

[5] 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_BG.html.

[6] *Конференция за бъдещето на Европа — Доклад за крайните резултати*, май 2022 г., предложение 28(2). Конференцията се проведе между април 2021 г. и май 2022 г. Тя беше единствена по рода си, водена от гражданите проява на съвещателна демокрация на равнището целия Европейски съюз, която включи хиляди европейски граждани, както и политически дейци, социални партньори, представители на гражданското общество и основни заинтересовани страни.

(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.

(8) С определянето на изисквания за киберсигурност при пускането на пазара на продукти с цифрови елементи ще се повиши киберсигурността на тези продукти както за потребителите, така и за предприятията. Това включва и изисквания за пускане на пазара на потребителски продукти с цифрови елементи, предназначени за уязвими потребители, като например играчки и бебешки монитори.

(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 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.

(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 причини, различни от такива,

свързани изключително с подобряване на сигурността, съвместимостта или оперативната съвместимост на софтуера.

(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.

(12) В Регламент (ЕС) 2017/745 на Европейския парламент и на Съвета[7] са определени правилата за медицинските изделия, а в Регламент (ЕС) 2017/746 на Европейския парламент и на Съвета[8] са определени правилата за медицинските изделия за *инвитро* диагностика. И в двата регламента киберрисковете са разгледани и са придружени от конкретни подходи, които са разгледани и в настоящия регламент. По-конкретно, в регламенти (ЕС) 2017/745 и (ЕС) 2017/746 се определят съществени изисквания за медицинските изделия, които функционират чрез електронна система или които сами по себе си са софтуер. Някои невградени софтуери и подходът на целия жизнен цикъл също са обхванати от тези регламенти. Тези изисквания задължават производителите да разработват и създават своите продукти, като прилагат принципите за управление на риска и като определят изисквания относно мерките за ИТ сигурност, както и съответните процедури за оценяване на съответствието. Освен това от декември 2019 г. са в сила специфични насоки относно киберсигурността за медицинските изделия, които предоставят на производителите на медицински изделия, включително изделията за *инвитро* диагностика, насоки за това как да изпълнят всички съответни съществени изисквания от приложение I към тези регламенти по отношение на киберсигурността[9]. Поради това продуктите с цифрови елементи, за които се прилага някой от тези регламенти, не следва да бъдат предмет на настоящия регламент.

---

7 Регламент (ЕС) 2017/745 на Европейския парламент и на Съвета от 5 април 2017 г. за медицинските изделия, за изменение на Директива 2001/83/ЕО, Регламент (ЕО) № 178/2002 и Регламент (ЕО) № 1223/2009 и за отмяна на директиви 90/385/ЕИО и 93/42/ЕИО на Съвета (ОВ L 117, 5.5.2017 г., стр. 1).

8 Регламент (ЕС) 2017/746 на Европейския парламент и на Съвета от 5 април 2017 г. за медицинските изделия за инвитро диагностика и за отмяна на Директива 98/79/ЕО и Решение 2010/227/ЕС на Комисията (ОВ L 117, 5.5.2017 г., стр. 176).

9 MDCG 2019-16, одобрен от Координационната група по медицинските изделия (MDCG), създадена с член 103 от Регламент (ЕС) 2017/745.

(13) С Регламент (ЕС) 2019/2144 на Европейския парламент и на Съвета[10] се установяват изисквания за одобряването на типа на превозните средства, както и на техните системи и компоненти, като се въвеждат определени изисквания за киберсигурност, включително относно функционирането на сертифицирана система за управление на киберсигурността, относно актуализациите на софтуера, обхващащи политиките и процесите на организациите за киберрисковете, свързани с целия жизнен цикъл на превозните средства, оборудването и услугите, в съответствие с приложимите правила на Организацията на обединените нации относно техническите спецификации и киберсигурността[11], и се предвиждат специфични процедури за оценяване на съответствието. В областта на въздухоплаването основната цел на Регламент (ЕС) 2018/1139 на Европейския парламент и на Съвета[12] е да се установи и поддържа високо и еднакво равнище на безопасност на гражданското въздухоплаване в Съюза. С него се създава рамка за съществени изисквания за летателна годност на въздухоплавателни продукти, части, оборудване, включително софтуер, които отчитат задълженията за защита срещу заплахи за информационната сигурност. Поради това продуктите с цифрови елементи, за които се прилага Регламент (ЕС) 2019/2144, и продуктите, сертифицирани в съответствие с Регламент (ЕС) 2018/1139, не са предмет на съществените изисквания и процедурите за оценяване на съответствието, определени в настоящия регламент. Процесът на сертифициране съгласно Регламент (ЕС) 2018/1139 осигурява нивото на увереност, към което е насочен настоящият регламент.

(14) С настоящия регламент се установяват хоризонтални правила за киберсигурност, които не са специфични за сектори или определени продукти с цифрови елементи. Независимо от това могат да бъдат въведени специфични по сектори или продукти правила на Съюза, в които да се определят изисквания, насочени към всички или някои от рисковете, обхванати от съществените изисквания, установени в настоящия регламент. В такива случаи прилагането на настоящия регламент по отношение на продукти с цифрови елементи, обхванати от други правила на Съюза, с които се установяват изисквания за справяне с всички или

---

10 Регламент (ЕС) 2019/2144 на Европейския парламент и на Съвета от 27 ноември 2019 г. относно изискванията за одобряване на типа на моторни превозни средства и техните ремаркета, както и на системи, компоненти и отделни технически възли, предназначени за такива превозни средства, по отношение на общата безопасност на моторните превозни средства и защитата на пътниците и уязвимите участници в движението по пътищата, за изменение на Регламент (ЕС) 2018/858 на Европейския парламент и на Съвета и за отмяна на регламенти (ЕО) № 78/2009, (ЕО) № 79/2009 и (ЕО) № 661/2009 на Европейския парламент и на Съвета и на регламенти (ЕО) № 631/2009, (ЕС) № 406/2010, (ЕС) № 672/2010, (ЕС) № 1003/2010, (ЕС) № 1005/2010, (ЕС) № 1008/2010, (ЕС) № 1009/2010, (ЕС) № 19/2011, (ЕС) № 109/2011, (ЕС) № 458/2011, (ЕС) № 65/2012, (ЕС) № 130/2012, (ЕС) № 347/2012, (ЕС) № 351/2012, (ЕС) № 1230/2012 и (ЕС) 2015/166 на Комисията (ОВ L 325, 16.12.2019 г., стр. 1).

11 Правило № 155 на ООН — Единни предписания за одобрение на превозни средства по отношение на киберсигурността и системата за управление на киберсигурността [2021/387].

12 Регламент (ЕС) 2018/1139 на Европейския парламент и на Съвета от 4 юли 2018 г. относно общи правила в областта на гражданското въздухоплаване и за създаването на Агенция за авиационна безопасност на Европейския съюз и за изменение на регламенти (ЕО) № 2111/2005, (ЕО) № 1008/2008, (ЕС) № 996/2010, (ЕС) № 376/2014 и на директиви 2014/30/ЕС и 2014/53/ЕС на Европейския парламент и на Съвета и за отмяна на регламенти (ЕО) № 552/2004 и (ЕО) № 216/2008 на Европейския парламент и на Съвета и Регламент (ЕИО) № 3922/91 на Съвета (ОВ L 212, 22.8.2018 г., стр. 1).

някои от рисковете, обхванати от съществените изисквания, посочени в приложение I към настоящия регламент, може да бъде ограничено или изключено, когато такова ограничение или изключване е в съответствие с общата регулаторна рамка, приложима към тези продукти, и когато секторните правила постигат същото ниво на защита като предвиденото в настоящия регламент. Комисията има правомощието да приема делегирани актове за изменение на настоящия регламент чрез определяне на такива продукти и правила. По отношение на съществуващото законодателство на Съюза, за което следва да се прилагат такива ограничения или изключения, настоящият регламент съдържа специални разпоредби, за да се изясни връзката му с това законодателство на Съюза.

(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 Делегиран регламент 2022/30 относно радиосъоръженията.

(16) Директива 85/374/ЕИО[13] допълва настоящия регламент. В тази директива се определят правилата за отговорност за дефектни продукти, така че увредените лица да могат да претендират за обезщетение, когато вредата е причинена от дефектни продукти. С нея се установява принципът, че производителят на даден продукт носи отговорност за вреди, причинени от липсата на безопасност в неговия продукт, независимо от вината („обективна отговорност“). Когато тази липса на безопасност се състои в липсата на актуализации на защитата след пускането на продукта на пазара и това причинява вреди, може да бъде потърсена отговорност от производителя. Задълженията на производителите, свързани с предоставянето на такива актуализации на защитата, следва да бъдат определени в настоящия регламент.

[13] Директива 85/374/ЕИО на Съвета от 25 юли 1985 г. за сближаване на законовите, подзаконовите и административните разпоредби на държавите членки относно отговорността за вреди, причинени от дефект на стока (ОВ L 210, 7.8.1985 г.).

(17) Настоящият регламент не следва да засяга Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета[14], включително разпоредбите за създаване на механизми за сертифициране на защитата на данните и на печати и маркировки за защита на данните, с цел да се докаже съответствието на операциите по обработване от страна на администраторите и обработващите лични данни с посочения регламент. Такива операции могат да бъдат вградени в продукт с цифрови елементи. Защитата на данните на етапа на проектирането и по подразбиране, както и киберсигурността като цяло, са ключови елементи на Регламент (ЕС) 2016/679. Като защитават потребителите и организациите от киберрискове, съществените изисквания за киберсигурността, установени в настоящия регламент, трябва също така да допринесат за подобряване на защитата на личните данни и неприкосновеността на личния живот на гражданите. Следва да се обмисли възможността за полезно взаимодействие както по отношение на стандартизацията, така и по отношение на сертифицирането на аспектите на киберсигурността чрез сътрудничеството между Комисията, европейските организации за стандартизация, Агенцията на Европейския съюз за киберсигурност (ENISA), Европейския комитет по защита на данните (ЕКЗД), създаден с Регламент (ЕС) 2016/679, и националните надзорни органи за защита на личните данни. Полезни взаимодействия между настоящия регламент и правото на Съюза в областта на защитата на личните данни следва да се създадат и в областта на надзора на пазара и правоприлагането. За тази цел националните органи за надзор на пазара, определени съгласно настоящия регламент, следва да си сътрудничат с органите за надзор на правото на Съюза в областта на защитата на данни. Последните следва също така да имат достъп до информация, която е от значение за изпълнението на техните задачи.

(18) Доколкото техните продукти попадат в обхвата на настоящия регламент, издателите на портфейли за европейска цифрова самоличност, както е посочено в [член 6а, параграф 2 от Регламент (ЕС) № 910/2014, изменен с Предложение за регламент за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на рамка за европейска цифрова самоличност], следва да отговарят както на хоризонталните съществени изисквания, установени с настоящия регламент, така и на специфичните изисквания за сигурност, установени с [член 6а от Регламент (ЕС) № 910/2014, изменен с Предложение за регламент за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на рамка за европейска цифрова самоличност]. За да се улесни спазването на изискванията, издателите на портфейли следва да могат да докажат съответствието на портфейлите за европейска цифрова самоличност с изискванията, определени съответно в двата акта, като сертифицират своите продукти по европейска схема за сертифициране на киберсигурността, създадена съгласно Регламент (ЕС) 2019/881 и за която Комисията е определила чрез акт за изпълнение презумпция за съответствие с настоящия регламент, доколкото сертификатът или части от него покриват тези изисквания.

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

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

(20) Продуктите с цифрови елементи следва да носят маркировката „CE“, 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 „CE“.

(21) За да се гарантира, че производителите могат да пускат софтуер за целите на тестването, преди да подложат продуктите си на оценяване на съответствието, държавите членки следва да не възпрепятстват предлагането на незавършен софтуер, като например алфа версии, бета версии или кандидати за пускане на пазара, при условие че версията се предоставя само за времето, необходимо за нейното изпитване и събиране на обратна информация. Производителите следва да гарантират, че софтуерът, който се предоставя при тези условия, се пуска само след оценка на риска и че той отговаря във възможно най-голяма степен на изискванията за сигурност, свързани с характеристиките на продуктите с цифрови елементи, наложени с настоящия регламент. Производителите следва също така да прилагат във възможно най-голяма степен изискванията за отстраняване на уязвимостите. Производителите следва да не принуждават ползвателите да надграждат до версии, пуснати само за целите на изпитването.

(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.

(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.

(24) Обновяването, поддръжката и ремонтът на продукт с цифрови елементи, както е определено в [Регламент за екопроектиране], не водят непременно до съществено изменение на продукта, например ако предвидената употреба и функционалните възможности не се променят и нивото на риска остава същото. Осъвременяването на продукта от страна на производителя обаче може да доведе до промени в проектирането и разработването на продукта и следователно може да повлияе на предвидената употреба и съответствието на продукта с определените в настоящия регламент изисквания.

(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.

(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.

(27) Категориите критични продукти с цифрови елементи, посочени в приложение III към настоящия регламент, следва да се разбират като продукти, които имат основни функционални възможности от типа, посочен в приложение III към настоящия регламент. Например в приложение III към настоящия регламент са изброени продукти, които по своите функционални възможности се определят като микропроцесори с общо предназначение от клас II. В резултат на това микропроцесорите с общо предназначение подлежат на задължително оценяване на съответствието от трета страна. Това не се отнася за други продукти, които не са изрично посочени в приложение III към настоящия регламент и които могат да включват микропроцесор с общо предназначение. Комисията следва да приеме делегирани актове [до 12 месеца от влизането в сила на настоящия регламент], за да уточни определенията на продуктовите категории, обхванати от клас I и клас II, както е посочено в приложение III.

(28) В настоящия регламент киберрисковете са целенасочено разгледани. Продуктите с цифрови елементи обаче могат да представляват други рискове, които не са свързани с киберсигурността. Тези рискове следва да продължат да се регулират от друго приложимо законодателство на Съюза относно продуктите. Ако не е приложимо друго законодателство на Съюза за хармонизация, те следва да бъдат предмет на Регламент [Регламент относно общата безопасност на продуктите]. Поради това, с оглед на целевия характер на настоящия регламент, като изключение от член 2, параграф 1, трета алинея, буква б) от Регламент [Регламент относно общата безопасност на продуктите], глава III, раздел 1, глави V и VII и глави IX—XI от Регламент [Регламент относно общата безопасност на продуктите] следва да се прилага за продукти с цифрови елементи по отношение на рисковете, които не са обхванати от настоящия регламент, ако тези продукти не са предмет на специфични изисквания, наложени от друго законодателство на Съюза за хармонизация по смисъла на [член 3, точка 25 от Регламента относно общата безопасност на продуктите].

(29) Продуктите с цифрови елементи, класифицирани като високорискови системи с ИИ съгласно член 6 от Регламент [Регламента относно ИИ][15], 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

[15] [Регламент относно ИИ].

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 [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].

(30) Машиностроителните изделия, попадащи в обхвата на Регламент [Предложение за регламент за машините], които са продукти с цифрови елементи по смисъла на настоящия регламент и за които е издадена декларация за съответствие въз основа на настоящия регламент, следва да се считат за съответстващи на съществените изисквания за здраве и безопасност, определени в [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, доколкото съответствието с тези изисквания се доказва от ЕС декларацията за съответствие, издадена съгласно настоящия регламент.

(31) Регламент [Предложение за регламент относно европейското пространство на здравни данни] допълва основните изисквания, определени в настоящия регламент. Поради това системите за електронни здравни досиета („системи за ЕЗД“), попадащи в обхвата на Регламент [Предложение за регламент за европейско пространство на здравни данни], които са продукти с цифрови елементи по смисъла на настоящия регламент, следва също да отговарят на съществените изисквания, определени в настоящия регламент. Техните производители следва да докажат съответствието, както се изисква от Регламент [Предложение за регламент за европейско пространство на здравни данни]. За да се улесни спазването на изискванията, производителите могат да изготвят единна техническа документация, съдържаща изискваните от двата правни акта елементи. Тъй като настоящият регламент не обхваща самия SaaS, системите за ЕЗД, предлагани чрез модела за лицензиране и доставяне на SaaS, не попадат в обхвата на настоящия регламент. По подобен начин системите за ЕЗД, които се разработват и използват вътрешно, не попадат в обхвата на настоящия регламент, тъй като не се предлагат на пазара.

(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.

(33) За да се подобри сигурността на продуктите с цифрови елементи, пуснати на вътрешния пазар, е необходимо да се определят съществени изисквания. Тези съществени изисквания следва да не засягат координираните от ЕС оценки на риска на критичните вериги на доставките, установени с [член X] от Директива [Директива XXX/XXXX (МИС 2)][16], които отчитат както технически, така и, когато е уместно, нетехнически рискови фактори, като например неправомерно влияние от страна на трета държава върху доставчиците. Освен това следва да не се засягат прерогативите на държавите членки да определят допълнителни изисквания, които отчитат нетехнически фактори с цел осигуряване на високо ниво на устойчивост, включително тези, определени в Препоръка (ЕС) 2019/534, в координираната оценка на риска за сигурността на 5G мрежите в целия Съюз и в набора от инструменти на ЕС за киберсигурност на 5G, договорени от групата за сътрудничество в областта за МИС, както е посочено в [Директива XXX/XXXX (МИС 2)].

(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.

(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 сигурността на техните продукти с цифрови елементи, производителите следва също така да

[16] Директива XXX на Европейския парламент и на Съвета от [дата] [относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148 (ОВ L xx, дата, стр. x)].

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.

(36) Производителите на продукти с цифрови елементи следва да въведат политики за координирано оповестяване на уязвимости, за да улеснят докладването на уязвимости от физически или юридически лица. В политиката за координирано оповестяване на уязвимости следва да се посочи структуриран процес, чрез който уязвимостите се съобщават на производителя по начин, който му позволява да диагностицира и отстрани такива уязвимости, преди подробната информация за уязвимостите да бъде разкрита на трети страни или на обществеността. Предвид факта, че информацията за уязвимости, които могат да бъдат използвани в широко разпространени продукти с цифрови елементи, може да бъде продадена на високи цени на черния пазар, производителите на такива продукти следва да могат да използват програми, като част от своите политики за координирано оповестяване на уязвимости, за стимулиране на докладването на уязвимости, като гарантират, че физическите или юридическите лица получават признание и компенсация за усилията си (т.нар. „програми за награда за откриване на уязвимости“).

(37) За да се улесни анализът на уязвимостта, производителите следва да установят и документират компонентите, които се съдържат в продуктите с цифрови елементи, включително чрез изготвяне на опис на софтуерните компоненти. Описът на софтуерните компоненти може да предостави на тези, които произвеждат, купуват и работят със софтуер, информация, която подобрява разбирането им за веригата на доставките, което има множество предимства, като най-вече помага на производителите и ползвателите да проследяват нововъзникващи уязвимости и рискове. Особено важно е производителите да гарантират, че техните продукти не съдържат уязвими компоненти, разработени от трети страни.

(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 Съвета[17]. Регламент (ЕС) № 1025/2012 предвижда процедура за възражения срещу хармонизирани стандарти, когато тези стандарти не отговарят напълно на изискванията на настоящия регламент.

(39) С Регламент (ЕС) 2019/881 се създава доброволна Европейска рамка за сертифициране на киберсигурността на продукти, процеси и услуги в областта

[17] 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).

на ИКТ. Европейските схеми за сертифициране на киберсигурността могат да обхващат продукти с цифрови елементи, обхванати от настоящия регламент. Следва да бъдат създадени полезни взаимодействия между настоящия регламент и Регламент (ЕС) 2019/881. С цел да се улесни оценяването на съответствието с изискванията, определени в настоящия регламент, за продуктите с цифрови елементи, които са сертифицирани или за които е издадена ЕС декларация за съответствие по схема за киберсигурност съгласно Регламент (ЕС) 2019/881 и които са били определени от Комисията в акт за изпълнение, се приема, че съответстват на съществените изисквания на настоящия регламент, доколкото сертификатът за киберсигурност или декларацията за съответствие, или части от тях покриват тези изисквания. Необходимостта от нови европейски схеми за сертифициране на киберсигурността за продукти с цифрови елементи следва да бъде оценена с оглед на настоящия регламент. Такива бъдещи европейски схеми за сертифициране на киберсигурността, които обхващат продукти с цифрови елементи, следва да отчитат съществените изисквания, както са определени в настоящия регламент, и да улесняват съответствието с него. На Комисията следва да бъде предоставено правомощието да определи чрез актове за изпълнение европейските схеми за сертифициране на киберсигурността, които могат да се използват за доказване на съответствие със съществените изисквания, определени в настоящия регламент. Освен това, за да се избегне ненужна административна тежест за производителите, когато е приложимо, Комисията следва да уточни дали сертификат за киберсигурност, издаден по такива европейски схеми за сертифициране на киберсигурността, премахва задължението на производителите да извършват оценка на съответствието от трета страна, както е предвидено в настоящия регламент за съответните изисквания.

(40) След влизането в сила на акта за изпълнение за определяне на [Регламент за изпълнение (ЕС) № .../... на Комисията от XXXX г. относно европейската схема за сертифициране на киберсигурността (ЕССК), основана на общи критерии], който се отнася до хардуерни продукти, обхванати от настоящия регламент, като например хардуерни модули за сигурност и микропроцесори, Комисията може да уточни чрез акт за изпълнение по какъв начин ЕССК предоставя презумпция за съответствие със съществените изисквания, посочени в приложение I към настоящия регламент, или с части от тях. Освен това в такъв акт за изпълнение може да се уточни по какъв начин сертификатът, издаден съгласно ЕССК, премахва задължението за производителите да извършват оценка от трета страна, както се изисква от настоящия регламент, за съответните изисквания.

(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 тези изисквания.

(42) Производителите следва да изготвят ЕС декларация за съответствие, за да предоставят изискваната съгласно настоящия регламент информация относно съответствието на продуктите с цифрови елементи със съществените изисквания на настоящия регламент и, когато е приложимо, на другото приложимо законодателство на Съюза за хармонизация, което обхваща продукта. От производителите може също така да се изисква да изготвят ЕС декларация за съответствие съгласно друго законодателство на Съюза. За да се гарантира ефективен достъп до информация за целите на надзора на пазара, следва да се изработи единна ЕС декларация за съответствие за всички съответни актове на Съюза. За да се намали административната тежест за икономическите оператори, следва да е възможно тази единна ЕС декларация за съответствие да представлява досие, включващо относимите отделни декларации за съответствие.

(43) Маркировката „CE“, указваща съответствието на продукта, е видимата последица от цял един процес, включващ оценяване на съответствието в широк смисъл. Основните принципи относно маркировката „CE“ са установени в Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета[18]. Правилата за нанасяне на маркировката „CE“ върху продукти с цифрови елементи следва да бъдат определени в настоящия регламент. Маркировката „CE“ следва да бъде единствената маркировка, гарантираща съответствието на продуктите с цифрови елементи с изискванията на настоящия регламент.

(44) За да се даде възможност на икономическите оператори да докажат съответствието си със съществените изисквания, определени в настоящия регламент, както и за да се даде възможност на органите за надзор на пазара да гарантират, че предлаганите на пазара продукти с цифрови елементи отговарят на тези изисквания, е необходимо да се предвидят процедури за оценяване на съответствието. В Решение № 768/2008/ЕО на Европейския парламент и на Съвета[19] са установени модули за процедури за оценяване на съответствието, пропорционални на нивото на риска и на изискваното ниво на сигурност. За да се осигури междусекторна съгласуваност и да се избегнат допълнителни варианти, процедурите за оценяване на съответствието, подходящи за проверка на съответствието на продуктите с цифрови елементи със съществените изисквания, определени в настоящия регламент, се основават на тези модули. Процедурите за оценяване на съответствието следва да разглеждат и проверяват както свързаните с продукта, така и с процеса изисквания, обхващащи целия жизнен цикъл на продуктите с цифрови елементи, включително планирането, проектирането, разработването или производството, изпитването и поддръжката на продукта.

(45) Като общо правило оценяването на съответствието на продукти с цифрови елементи следва да се извършва от производителя на негова отговорност, като се

---

[18] 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).

[19] Решение № 768/2008/ЕО на Европейския парламент и Съвета от 9 юли 2008 г. относно обща рамка за предлагането на пазара на продукти и за отмяна на Решение № 93/465/ЕИО (ОВ L 218, 13.8.2008 г., стр. 82).

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 B+C или модул H 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.

(46) Докато създаването на материални продукти с цифрови елементи обикновено изисква от производителите да положат значителни усилия през етапите на проектиране, разработване и производство, създаването на продукти с цифрови елементи под формата на софтуер се съсредоточава почти изключително върху проектирането и разработването, а етапът на производство играе второстепенна роля. Въпреки това в много случаи софтуерните продукти все още трябва да бъдат компилирани, създадени, пакетирани, предоставени за изтегляне или копирани на физически носител, преди да бъдат пуснати на пазара. Тези дейности следва да се разглеждат като дейности, равностойни на производство, когато се прилагат съответните модули за оценяване на съответствието, за да се провери съответствието на продукта със съществените изисквания на настоящия регламент в етапите на проектиране, разработване и производство.

(47) С цел извършване на оценяване на съответствието на продукти с цифрови елементи от трета страна, националните нотифициращи органи следва да уведомят Комисията и другите държави членки за органите за оценяване на съответствието, при условие че те отговарят на набор от изисквания, по-специално за независимост, компетентност и липса на конфликт на интереси.

(48) С цел осигуряване на сходно ниво на качеството при оценяването на съответствието на продукти с цифрови елементи, е необходимо също така да се определят изискванията за нотифициращите органи и другите органи, участващи в оценяването, нотифицирането и наблюдението на нотифицираните органи. Системата, установена в настоящия регламент, следва да се допълни със системата за акредитация, предвидена в Регламент (ЕО) № 765/2008. Тъй като акредитацията е важно средство за проверка на компетентността на органите за

оценяване на съответствието, тя също следва да бъде използвана за целите на нотифицирането.

(49) Прозрачната акредитация, предвидена в Регламент (ЕО) № 765/2008, осигуряваща необходимото ниво на доверие в сертификатите за съответствие, следва да се разглежда от националните органи на публичната власт в целия Съюз като предпочитано средство за доказване на техническата компетентност на органите за оценяване на съответствието. Въпреки това, националните органи могат да счетат, че притежават подходящите средства сами да извършват тази оценка. В такива случаи, с цел да се гарантира подходящото ниво на доверие в оценките, извършвани от други национални органи, те следва да предоставят на Комисията и на другите държави членки необходимите документи, доказващи съответствието на оценените органи за оценяване на съответствието с приложимите регулаторни изисквания.

(50) Органите за оценяване на съответствието често възлагат части от своите дейности, свързани с оценяването на съответствието, на подизпълнители, или използват свои поделения за тази цел. С цел запазване нивото на защита, изисквано за продуктите с цифрови елементи, които се пускат на пазара, е от съществено значение подизпълнителите и поделенията, извършващи оценяване на съответствието, да отговарят на същите изисквания като нотифицираните органи във връзка с изпълнението на задачи по оценяване на съответствието.

(51) Уведомлението за орган за оценяване на съответствието следва да бъде изпратено от нотифициращия орган до Комисията и другите държави членки чрез информационната система NANDO (информационна система за нотифицираните и определените организации по Новия подход). NANDO е средство за електронно нотифициране, разработено и управлявано от Комисията, в което може да се намери списък на всички нотифицирани органи.

(52) Тъй като нотифицираните органи могат да предлагат своите услуги в целия Съюз, е целесъобразно да се даде възможност на другите държави членки и на Комисията да повдигат възражения относно нотифициран орган. Следователно е важно да се определи срок, през който всякакви съмнения или съображения относно компетентността на органите за оценяване на съответствието да бъдат изяснени, преди те да започнат да функционират като нотифицирани органи.

(53) В интерес на конкурентоспособността е от съществено значение нотифицираните органи да прилагат процедурите за оценяване на съответствието, без да се създава ненужна тежест за икономическите оператори. По същата причина, както и за да се гарантира еднаквото третиране на икономическите оператори, трябва да се осигури съответствие в техническото прилагане на процедурите за оценяване на съответствието. Това следва да се постигне най-добре посредством съответната координация и сътрудничество между нотифицираните органи.

(54) Надзорът на пазара е основно средство при осигуряването на правилно и еднакво прилагане на законодателството на Съюза. Следователно е необходимо да се създаде правната рамка, в която този надзор ще може да бъде провеждан ефективно. Правилата на Съюза за надзор на пазара и контрол на продуктите, които се въвеждат на пазара на Съюза, предвидени в Регламент (ЕС) 2019/1020

на Европейския парламент и на Съвета[20], се прилагат за продуктите с цифрови елементи, обхванати от настоящия регламент.

(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.

(56) Следва да бъде създадена специализирана група за административно сътрудничество (ADCO група) за еднакво прилагане на настоящия регламент в съответствие с член 30, параграф 2 от Регламент (ЕС) 2019/1020. Тази ADCO група следва да бъде съставена от представители на определените органи за надзор на пазара и, ако е целесъобразно, от представители на единните служби за връзка. Комисията следва да подкрепя и насърчава сътрудничеството между органите за надзор на пазара чрез Мрежата на Съюза за съответствието на продуктите, създадена въз основа на член 29 от Регламент (ЕС) 2019/1020 и състояща се от представители на всяка държава членка, включително представител на всяка единна служба за връзка, посочени в член 10 от Регламент (ЕС) 2019/1020, и национален експерт по избор, председателите на ADCO групи и представители на Комисията. Комисията следва да участва в заседанията на мрежата, нейните подгрупи и съответната ADCO група. Тя следва също така да подпомага тази ADCO група чрез изпълнителен секретариат, който осигурява техническа и логистична подкрепа.

(57) С цел да се осигурят навременни, пропорционални и ефективни мерки по отношение на продуктите с цифрови елементи, представляващи значителен киберриск, следва да се предвиди предпазна процедура на Съюза, в рамките на която заинтересованите страни да бъдат информирани за мерките, които се планира да бъдат предприети по отношение на такива продукти. Вследствие на това също така органите за надзор на пазара ще могат, в сътрудничество със съответните икономически оператори, да предприемат действия на по-ранен

[20] Регламент (ЕС) 2019/1020 на Европейския парламент и на Съвета от 20 юни 2019 г. относно надзора на пазара и съответствието на продуктите и за изменение на Директива 2004/42/ЕО и регламенти (ЕО) № 765/2008 и (ЕС) № 305/2011 (ОВ L 169, 25.6.2019 г., стр. 1).

етап, когато това е необходимо. Когато между държавите членки и Комисията е постигнато съгласие по отношение на основателността на мярка, предприета от дадена държава членка, не следва да се изисква допълнителна намеса на Комисията, освен когато несъответствието се дължи на недостатъци на хармонизиран стандарт.

(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 изземе 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.

(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 разпореди 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 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.

(60) В случаите, когато има признаци за неспазване на настоящия регламент в няколко държави членки, органите за надзор на пазара следва да могат да извършват съвместни дейности с други органи с цел проверка на съответствието и установяване на киберрисковете на продуктите с цифрови елементи.

(61) Едновременните координирани действия за контрол („мащабни проверки“) са специфични правоприлагащи действия от органите за надзор на пазара, които могат допълнително да повишат сигурността на продуктите. Мащабните проверки следва да се провеждат по-специално в случаите, когато пазарни тенденции, жалби на потребителите или други признаци сочат, че определени категории продукти често представляват киберрискове. ENISA следва да представи на органите за надзор на пазара предложения за категории продукти, за които могат да бъдат организирани мащабни проверки, наред с другото, въз основа на получените уведомления за уязвимости и инциденти с продукти.

(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 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 законотворчество[21]. 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.

[21] ОВ L 123, 12.5.2016 г., стр. 1.

(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 уведомленията относно активно използвани уязвимости и инциденти, подавани до ENISA от производителите, да 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 Съвета[22].

(64) За да се гарантира надеждно и конструктивно сътрудничество между органите за надзор на пазара на равнището на Съюза и на национално равнище, всички страни, участващи в прилагането на настоящия регламент, следва да зачитат поверителността на информацията и данните, получавани при изпълнението на техните задачи.

(65) За да се гарантира ефективното прилагане на предвидените съгласно настоящия регламент задължения, всеки компетентен орган за надзор на пазара следва да разполага с правомощието да налага или изисква налагането на административни глоби. Поради това следва да бъдат определени максимални размери на административните глоби, които да бъдат предвидени в националните законодателства при неспазване на задълженията, предвидени в настоящия регламент. При вземането на решение относно размера на административната глоба във всеки отделен случай следва да се вземат предвид всички обстоятелства от значение за конкретната ситуация и като минимум тези, които са изрично установени в настоящия регламент, включително дали други органи за надзор на пазара вече са налагали административни глоби на същия оператор за подобни нарушения. Такива обстоятелства могат да бъдат утежняващи, когато нарушението на същия оператор продължава да се извършва на територията на други държави членки, различни от тази, в която вече е била наложена административна глоба, или смекчаващи, като се гарантира, че всяка друга административна глоба, разглеждана от друг орган за надзор на пазара за същия икономически оператор или за същия вид нарушение, следва вече да отчита, заедно с други съответни конкретни обстоятелства, санкцията и нейния размер, наложени в други държави членки. Във всички такива случаи кумулативната административна глоба, която може да бъде наложена от органите за надзор на пазара на няколко държави членки на един и същ

[22] 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).

икономически оператор за един и същ вид нарушение, следва да гарантира спазването на принципа на пропорционалност.

(66) При налагане на административни глоби на лица, които не са предприятие, компетентният орган следва да има предвид общото равнище на доход в съответната държава членка, както и икономическото състояние на лицето, когато определя подходящия размер на глобата. Държавите членки следва да определят дали и до каква степен публичните органи следва да подлежат на административни глоби.

(67) В отношенията си с трети държави ЕС се стреми да насърчава международната търговия с регулирани продукти. С оглед улесняване на търговията могат да се прилагат широк спектър от мерки, включително няколко правни инструмента, като например двустранни (междуправителствени) споразумения за взаимно признаване (СВП) за оценка на съответствието и маркиране на регулирани продукти. СВП се сключват между Съюза и трети държави, които се намират на сравнимо ниво на техническо развитие и имат съвместим подход по отношение на оценяването на съответствието. Тези споразумения се основават на взаимното приемане на сертификати, маркировки за съответствие и протоколи от изпитвания, издадени от органите за оценяване на съответствието на една от страните в съответствие със законодателството на другата страна. Понастоящем СВП са в сила за няколко държави. Споразуменията се сключват в редица специфични сектори, които могат да се различават в отделните държави. С цел допълнително улесняване на търговията и като се отчита, че веригите за доставка на продукти с цифрови елементи са глобални, СВП относно оценяването на съответствието могат да бъдат сключени от Съюза за продукти, регулирани от настоящия регламент, в съответствие с член 218 от ДФЕС. Сътрудничеството с партньорски държави също е важно, за да се засили киберустойчивостта в световен мащаб, тъй като в дългосрочен план това ще допринесе за укрепване на рамката за киберсигурност както в ЕС, така и извън него.

(68) Комисията следва периодично да извършва преглед на настоящия регламент, като се консултира със заинтересованите страни, по-специално с цел установяване на необходимостта от изменения предвид промените в обществените, политическите, технологичните или пазарните условия.

(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.

(70) Доколкото целта на настоящия регламент не може да бъде постигната в достатъчна степен от държавите членки, а поради последиците от действието може да бъде по-добре постигната на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от Договора за Европейския съюз. В съответствие с принципа на пропорционалност, уреден в същия член, настоящият регламент не надхвърля необходимото за постигането на тази цел.

(71) В съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета[23] беше проведена консултация с Европейския надзорен орган по защита на данните, който излезе със становище на […] г.,

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

ГЛАВА I

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет

С настоящия регламент се определят:

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

б) съществени изисквания за проектирането, разработването и производството на продукти с цифрови елементи, както и задължения за икономическите оператори във връзка с тези продукти по отношение на киберсигурността;

в) съществени изисквания за процесите на отстраняване на уязвимостите, въведени от производителите, за да се гарантира киберсигурността на продуктите с цифрови елементи през целия им жизнен цикъл, и задължения за икономическите оператори във връзка с тези процеси;

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

Член 2

Обхват

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.

2. Настоящият регламент не се прилага за продукти с цифрови елементи, за които се прилагат следните актове на Съюза:

   а) Регламент (ЕС) 2017/745;

   б) Регламент (ЕС) 2017/746;

   в) Регламент (ЕС) 2019/2144.

3. Настоящият регламент не се прилага за продукти с цифрови елементи, които са сертифицирани в съответствие с Регламент (ЕС) 2018/1139.

---

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

4. Прилагането на настоящия регламент за продукти с цифрови елементи, обхванати от други правила на Съюза, определящи изисквания, които се отнасят до всички или някои от рисковете, обхванати от съществените изисквания, посочени в приложение I, може да бъде ограничено или изключено, когато:

   а) това ограничаване или изключване е в съответствие с общата регулаторна рамка, приложима към тези продукти; и

   б) секторните правила постигат същото ниво на защита като предвиденото в настоящия регламент.

   Комисията има правомощието да приема делегирани актове в съответствие с член 50 за изменение на настоящия регламент, като посочва дали е необходимо такова ограничение или изключване, съответните продукти и правила, както и обхвата на ограничението, ако е приложимо.

5. Настоящият регламент не се прилага за продукти с цифрови елементи, разработени изключително за целите на националната сигурност или за военни цели, или за продукти, специално предназначени за обработка на класифицирана информация.

Член 3

Определения

За целите на настоящия регламент се прилагат следните определения:

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;

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;

3) „критичен продукт с цифрови елементи“ означава продукт с цифрови елементи, който представлява киберриск в съответствие с критериите, определени в член 6, параграф 2, и чиито основни функционални възможности са посочени в приложение III;

4) „продукт с цифрови елементи с висока степен на критичност“ означава продукт с цифрови елементи, който представлява киберриск в съответствие с критериите, определени в член 6, параграф 5;

5) „оперативна технология“ означава програмируеми цифрови системи или устройства, които взаимодействат с физическата среда, или управляват устройства, които взаимодействат с физическата среда;

6) „софтуер“ означава частта от електронна информационна система, която се състои от компютърен код;

7) „хардуер“ означава физическа електронна информационна система или части от нея, които могат да обработват, съхраняват или предават цифрови данни;

8) „компонент“ означава софтуер или хардуер, предназначен за интегриране в електронна информационна система;

9) „електронна информационна система“ означава всяка система, включително електрическо или електронно оборудване, способна да обработва, съхранява или предава цифрови данни;

10) „логическа връзка“ означава виртуална репрезентация на връзка за данни, осъществена чрез софтуерен интерфейс;

11) „физическа връзка“ означава всяка връзка между електронни информационни системи или компоненти, осъществена чрез физически средства, включително чрез електрически или механични интерфейси, проводници или радиовълни;

12) „непряка връзка“ означава връзка с устройство или мрежа, която не се осъществява пряко, а по-скоро като част от по-голяма система, която може да се свърже пряко с такова устройство или мрежа;

13) „привилегия“ означава право на достъп, предоставено на определени ползватели или програми за извършване на операции, свързани със сигурността, в рамките на електронна информационна система;

14) „разширена привилегия“ означава право на достъп, предоставено на определени ползватели или програми за извършване на разширен набор от операции, свързани със сигурността, в рамките на електронна информационна система, което, ако бъде неправилно използвано или компрометирано, може да позволи на злонамерен участник да получи по-широк достъп до ресурсите на системата или организацията;

15) „крайна точка“ означава всяко устройство, което е свързано с мрежа и служи като входна точка към тази мрежа;

16) „мрежови или компютърни ресурси“ означава данни или хардуерни или софтуерни функционални възможности, които са достъпни локално или чрез мрежа или друго свързано устройство;

17) „икономически оператор“ означава производителят, упълномощеният представител, вносителят, дистрибуторът или всяко друго физическо или юридическо лице, което подлежи на задълженията, определени в настоящия регламент;

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;

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;

20) „вносител“ означава всяко физическо или юридическо лице, установено в Съюза, което пуска на пазара продукт с цифрови елементи, който носи името или търговската марка на физическо или юридическо лице, установено извън Съюза;

21) „дистрибутор“ означава всяко физическо или юридическо лице във веригата на доставки, различно от производителя или вносителя, което предоставя

определен продукт с цифрови елементи на пазара на Съюза, без да засяга характеристиките му;

22) „пускане на пазара“ означава предоставянето за първи път на продукт с цифрови елементи на пазара на Съюза;

23) „предоставяне на пазара“ означава всяка доставка на продукт с цифрови елементи за разпространение или използване на пазара на Съюза в процеса на търговска дейност, срещу заплащане или безвъзмездно;

24) „предвидена употреба“ означава използването, за което е предназначен даден продукт с цифрови елементи от производителя, включително специфичният контекст и условия на употреба, посочени в информацията, предоставена от производителя в инструкциите за употреба, рекламните или търговските материали и твърдения, както и в техническата документация;

25) „разумно предвидима употреба“ означава употреба, която не е непременно предвидената употреба, предоставена от производителя в инструкциите за употреба, рекламните или търговските материали и твърдения, както и в техническата документация, но която е вероятно да възникне в резултат на разумно предвидимо човешко поведение или технически операции или взаимодействия;

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;

27) „нотифициращ орган“ означава националният орган, отговарящ за въвеждането и извършването на необходимите процедури за оценяването, определянето и нотифицирането на органи за оценяване на съответствието и за провеждането на мониторинг по отношение на тях;

28) „оценяване на съответствието“ означава процесът на проверка дали са изпълнени съществените изисквания, определени в приложение I;

29) „орган за оценяване на съответствието“ означава орган, определен в член 2, параграф 13 от Регламент (ЕС) № 765/2008;

30) „нотифициран орган“ е орган за оценяване на съответствието, определен съгласно член 33 от настоящия регламент и друго приложимо законодателство на Съюза за хармонизация;

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;

32) маркировка „CE“ означава маркировка, чрез която производителят указва, че даден продукт с цифрови елементи и процесите, въведени от производителя, са в съответствие със съществените изисквания, определени в приложение I, и с друго приложимо законодателство на Съюза, с което се хармонизират условията за предлагане на продукти на пазара („законодателство на Съюза за хармонизация“) и в което се предвижда нейното нанасяне;

33) „орган за надзор на пазара“ означава орган съгласно определението в член 3, точка 4 от Регламент (ЕС) 2019/1020;

34) „хармонизиран стандарт“ означава хармонизиран стандарт съгласно определението в член 2, точка 1, буква в) от Регламент (ЕС) № 1025/2012;

35) „киберриск“ означава риск, както е определен в [член X] от [Директива XXX/XXXX (МИС 2)];

36) „значителен киберриск“ означава киберриск, за който въз основа на техническите му характеристики може да се предположи, че има голяма вероятност от инцидент, който може да доведе до сериозни отрицателни въздействия, включително чрез причиняване на значителни материални или нематериални загуби или смущения;

37) „опис на софтуерните компоненти“ означава официален запис, съдържащ подробна информация и връзки по веригата на доставка на компонентите, включени в софтуерните елементи на даден продукт с цифрови елементи;

38) „уязвимост“ означава уязвимост, както е определена в член [член X] от Директива [Директива XXX/XXXX (МИС 2)];

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;

40) „лични данни“ означава данните, определени в член 4, параграф 1 от Регламент (ЕС) 2016/679.

Член 4

Свободно движение

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.

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.

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.

Член 5

Изисквания за продукти с цифрови елементи

Продукти с цифрови елементи се предоставят на пазара само ако:

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

2) въведените от производителя процеси отговарят на съществените изисквания, посочени в приложение I, раздел 2.

Член 6

Критични продукти с цифрови елементи

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.

2. Комисията има правомощието да приема делегирани актове в съответствие с член 50 за изменение на приложение III чрез включване на нова категория в списъка с категориите критични продукти с цифрови елементи или оттегляне на съществуваща категория от този списък. Когато оценява необходимостта от изменение на списъка в приложение III, Комисията взема предвид нивото на киберриска, свързан с категорията продукти с цифрови елементи. При определяне на нивото на киберриск се вземат предвид един или няколко от следните критерии:

   а) функционалните възможности на продукта с цифрови елементи, свързани с киберсигурността, и дали продуктът с цифрови елементи има поне един от следните атрибути:

      i) той е проектиран да работи с разширена привилегия или да управлява привилегии;

      ii) той има пряк или привилегирован достъп до мрежови или компютърни ресурси;

      iii) той е предназначен да контролира достъпа до данни или оперативни технологии;

      iv) той изпълнява функция, която е от критично значение за доверието, по-специално функции за сигурност, като например контрол на мрежата, сигурност на крайните точки и защита на мрежата.

   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)];

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

   г) потенциалната степен на неблагоприятно въздействие, по-специално по отношение на неговия интензитет и способността му да засегне множество лица;

   д) степента, в която използването на продукти с цифрови елементи вече е причинило материални или нематериални загуби или смущения или е породило значителни опасения във връзка с настъпването на неблагоприятно въздействие.

3. Комисията има правомощието да приеме делегиран акт в съответствие с член 50 за допълване на настоящия регламент чрез уточняване на определенията на продуктовите категории от клас I и клас II, както е посочено в приложение III. Делегираният акт се приема [до 12 месеца от влизането в сила на настоящия регламент].

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

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:

   а) се използва или на нея се разчита от основните субекти от вида, посочен в приложение [приложение I] към Директива [Директива XXX/XXXX (МИС 2)], или ще има потенциално бъдещо значение за дейността на тези субекти; или

   б) е от значение за устойчивостта на цялата верига на доставките на продукти с цифрови елементи срещу смущаващи събития.

Член 7

Обща безопасност на продуктите

Като изключение от член 2, параграф 1, трета алинея, буква б) от Регламент [Регламент относно общата безопасност на продуктите], когато продуктите с цифрови елементи не са предмет на специфични изисквания, наложени от друго законодателство на Съюза за хармонизация по смисъла на [член 3, точка 25 от Регламента относно общата безопасност на продуктите], към тези продукти по отношение на рисковете, които не са обхванати от настоящия регламент, се прилагат глава III, раздел 1, глави V и VII и глави IX—XI от Регламент [Регламент относно общата безопасност на продуктите].

Член 8

Високорискови системи с ИИ

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 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.

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 за нотифициране съгласно Регламент [Регламент относно ИИ].

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.

Член 9

Машиностроителни изделия

Машиностроителните изделия в обхвата на Регламент [Предложение за регламент за машините], които са 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.

ГЛАВА II

ЗАДЪЛЖЕНИЯ НА ИКОНОМИЧЕСКИТЕ ОПЕРАТОРИ

Член 10

Задължения на производителите

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.

2. С оглед на изпълнението на задължението по параграф 1 производителите извършват оценка на киберрисковете, свързани с продукта с цифрови елементи, и вземат предвид резултата от тази оценка по време на етапите на планиране, проектиране, разработване, производство, доставка и поддръжка на продукта с цифрови елементи с цел свеждане до минимум на киберрисковете, предотвратяване на инциденти с компютърната сигурност, както и свеждане до минимум на последиците от такива инциденти, включително по отношение на здравето и безопасността на ползвателите.

3. При пускането на пазара на продукт с цифрови елементи производителят включва оценка на киберриска в техническата документация, както е посочено в член 23 и приложение V. 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, оценката на киберриска може да бъде част от оценката на риска, изисквана от тези съответни актове на Съюза. Когато някои съществени изисквания не са приложими към предлагания на пазара продукт с цифрови елементи, производителят включва ясна обосновка в тази документация.

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.

5. Производителят систематично документира — по начин, който е пропорционален на естеството и киберрисковете, съответните аспекти на киберсигурността, отнасящи се до продукта с цифрови елементи, включително уязвимостите, за които е узнал, и всяка информация от значение, предоставена от трети страни, и когато е приложимо, актуализира оценката на риска на продукта.

6. 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.

   Производителите разполагат с подходящи политики и процедури, включително политики за координирано оповестяване на уязвимости, посочени в приложение I, раздел 2, точка 5 за обработване и отстраняване на потенциални уязвимости в продукта с цифрови елементи, за които е съобщено от вътрешни или външни източници.

7. Преди да пуснат даден продукт с цифрови елементи на пазара, производителите изготвят техническата документация, посочена в член 23.

   Те извършват или възлагат извършването на избраните процедури за оценяване на съответствието, посочени в член 24.

   Когато чрез тази процедура за оценяване на съответствието е доказано съответствието на продукта с цифрови елементи със съществените изисквания, определени в приложение I, раздел 1, и на въведените от производителя

процеси със съществените изисквания, определени в приложение I, раздел 2, производителите изготвят ЕС декларацията за съответствие съгласно член 20 и нанасят маркировката „CE“ съгласно член 22.

8. Производителите съхраняват техническата документация и ЕС декларацията за съответствие, когато е приложимо, на разположение на органите за надзор на пазара в продължение на десет години след пускането на пазара на продукта с цифрови елементи.

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.

10. Производителите гарантират, че продуктите с цифрови елементи се придружават от информацията и инструкциите, посочени в приложение II, в електронна или физическа форма. Тази информация и инструкции са на език, който е лесноразбираем за ползвателите. Те трябва да са ясни, разбираеми, смислени и четливи. Те позволяват сигурно инсталиране, експлоатация и използване на продуктите с цифрови елементи.

11. Производителите предоставят ЕС декларацията за съответствие заедно с продукта с цифрови елементи или включват в инструкциите и информацията, посочени в приложение II, интернет адреса, на който може да се намери ЕС декларацията за съответствие.

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 коригиращи мерки, за да приведат продукта с цифрови елементи или процесите на производителя в съответствие с изискванията, да изтеглят или да изземат продукта, според случая.

13. При мотивирано искане от страна на орган за надзор на пазара производителите предоставят на този орган, на лесноразбираем за него език, цялата информация и документация на хартиен или електронен носител, необходима за доказване на съответствието на продукта с цифрови елементи и на въведените от производителя процеси със съществените изисквания, посочени в приложение I. Те си сътрудничат с този орган, по негово искане, във връзка с всички мерки, предприети за отстраняване на киберрисковете, породени от пуснатия от тях на пазара продукт с цифрови елементи.

14. Производител, който прекратява дейността си и в резултат на това не е в състояние да изпълни задълженията, предвидени в настоящия регламент, информира, преди прекратяването на дейността да влезе в сила, съответните органи за надзор на пазара за това положение, както и, с всички налични

средства и доколкото е възможно, ползвателите на съответните продукти с цифрови елементи, пуснати на пазара.

15. Чрез актове за изпълнение Комисията може да определи формата и елементите на описа на софтуерните компоненти, посочен в приложение I, раздел 2, точка 1. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 51, параграф 2.

Член 11

Задължения на производителите за представяне на отчети

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

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 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.

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.

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.

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

6. Въз основа на уведомленията, 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.

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.

Член 12

Упълномощени представители

1. Производителят може да назначи упълномощен представител чрез писмено пълномощно.

2. Задълженията, определени в член 10, параграфи 1—6, член 10, параграф 7, първо тире и член 10, параграф 9 не са част от пълномощието на упълномощения представител.

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

   а) да съхранява на разположение на органите за надзор на пазара ЕС декларацията за съответствие, посочена в член 20, и техническата документация, посочена в член 23, в продължение на десет години след пускането на пазара на продукта 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 съответствието на даден продукт с цифрови елементи;

   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.

Член 13

Задължения на вносителите

1. Вносителите пускат на пазара само продукти с цифрови елементи, които отговарят на съществените изисквания, определени в приложение I, раздел 1, и при които въведените от производителя процеси са в съответствие със съществените изисквания, определени в приложение I, раздел 2.

2. Преди да пуснат един продукт с цифрови елементи на пазара на Съюза, вносителите гарантират, че:

   а) съответната процедура за оценяване на съответствието, посочена в член 24, е била проведена от производителя;

б) производителят е изготвил техническата документация;

в) върху продукта с цифрови елементи е нанесена маркировката „CE“, посочена в член 22, и той е придружен от информацията и инструкциите за употреба, посочени в приложение II.

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

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.

5. Вносителите гарантират, че продуктът с цифрови елементи се придружава от инструкциите и информацията, посочени в приложение II, предоставени на лесноразбираем за ползвателите език.

6. 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 коригиращи 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.

При установяване на уязвимост в продукта с цифрови елементи вносителите информират производителя без неоправдано забавяне за тази уязвимост. Освен това, когато продуктът с цифрови елементи представлява значителен киберриск, вносителите информират незабавно за това органите за надзор на пазара на държавите членки, в които са предоставили продукта с цифрови елементи на пазара, като предоставят подробни данни, по-специално за несъответствието с изискванията и за всякакви предприети коригиращи мерки.

7. В продължение на десет години след пускането на пазара на продукта с цифрови елементи, вносителите съхраняват копие от ЕС декларацията за съответствие на разположение на органите за надзор на пазара и гарантират, че при поискване техническата документация може да бъде предоставена на тези органи.

8. При мотивирано искане от страна на орган за надзор на пазара вносителите му предоставят цялата информация и документация на хартиен или електронен носител, необходима за доказване на съответствието на продукта с цифрови елементи със съществените изисквания, посочени в приложение I, раздел 1, както и на въведените от производителя процеси със съществените изисквания, посочени в приложение I, раздел 2, на лесноразбираем за този орган език. Те

сътрудничат на този орган, по негово искане, за всякакви коригиращи мерки, предприети за отстраняване на киберрисковете, свързани с продуктите с цифрови елементи, които те са пуснали на пазара.

9. Когато вносителят на продукт с цифрови елементи узнае, че производителят на този продукт е преустановил дейността си и в резултат на това не е в състояние да изпълни задълженията, предвидени в настоящия регламент, вносителят информира съответните органи за надзор на пазара за това положение, както и, с всички налични средства и доколкото е възможно, ползвателите на пуснатите на пазара продукти с цифрови елементи.

Член 14

Задължения на дистрибуторите

1. Когато предоставят продукт с цифрови елементи на пазара, дистрибуторите действат с дължимата грижа по отношение на изискванията на настоящия регламент.

2. Преди да предоставят на пазара продукт с цифрови елементи, дистрибуторите проверяват дали:

   а) продуктът с цифрови елементи има нанесена маркировката „CE“;

   б) производителят и вносителят са изпълнили задълженията, посочени съответно в член 10, параграфи 10 и 11 и член 13, параграф 4.

3. Когато дистрибутор 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, дистрибуторът не предоставя продукта с цифрови елементи на пазара, докато този продукт или процесите, въведени от производителя, не бъдат приведени в съответствие. Освен това, когато продуктът с цифрови елементи представлява значителен киберриск, дистрибуторът информира за това производителя и органите за надзор на пазара.

4. Дистрибуторите, които знаят или имат основание да смятат, че продукт с цифрови елементи, който са предоставили на пазара, или процесите, въведени от неговия производител, не са в съответствие със съществените изисквания, посочени в приложение I, гарантират, че са предприети необходимите коригиращи мерки за привеждане на продукта с цифрови елементи или на процесите, въведени от неговия производител, в съответствие, или за изтегляне или изземване на продукта, ако е целесъобразно.

   При установяване на уязвимост в продукта с цифрови елементи дистрибуторите информират производителя за тази уязвимост без неоправдано забавяне. Освен това, когато продуктът с цифрови елементи представлява значителен киберриск, дистрибуторите информират незабавно за това органите за надзор на пазара на държавите членки, в които са предоставили продукта с цифрови елементи на пазара, като предоставят подробни данни, по-специално за несъответствието с изискванията и за всякакви предприети коригиращи мерки.

5. При мотивирано искане от страна на орган за надзор на пазара дистрибуторите му предоставят цялата информация и документация на хартиен или електронен носител, необходима за доказване на съответствието на продукта с цифрови

елементи и на въведените от производителя процеси със съществените изисквания, посочени в приложение I на лесноразбираем за този орган език. Те сътрудничат на този орган, по негово искане, за всякакви корективни мерки, предприети за отстраняване на киберрисковете, свързани с продуктите с цифрови елементи, които те са предоставили на пазара.

6. Когато дистрибуторът на продукт с цифрови елементи узнае, че производителят на този продукт е преустановил дейността си и в резултат на това не е в състояние да изпълни задълженията, предвидени в настоящия регламент, дистрибуторът информира съответните органи за надзор на пазара за това положение, както и, с всички налични средства и доколкото е възможно, ползвателите на пуснатите на пазара продукти с цифрови елементи.

Член 15

Случаи, в които задълженията на производителите се прилагат и към вносителите и дистрибуторите

Вносител или дистрибутор се счита за производител за целите на настоящия регламент и подлежи на задълженията на производителя, посочени в член 10 и член 11, параграфи 1, 2, 4 и 7, когато този вносител или дистрибутор пуска на пазара продукт с цифрови елементи под своето име или търговска марка или извършва съществено изменение на вече пуснатия на пазара продукт с цифрови елементи.

Член 16

Други случаи, в които се прилагат задълженията на производителите

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.

Това лице подлежи на задълженията на производителя, посочени в член 10 и член 11, параграфи 1, 2, 4 и 7, за частта от продукта, която е засегната от съществената изменение, или, ако съществената изменение оказва въздействие върху киберсигурността на продукта с цифрови елементи като цяло, за целия продукт.

Член 17

Идентификация на икономическите оператори

1. По искане на органите за надзор на пазара и когато информацията е налична, икономическите оператори посочват следната информация:

   а) име и адрес на всеки икономически оператор, който им е доставил продукт с цифрови елементи;

   б) име и адрес на всеки икономически оператор, на когото са доставили продукт с цифрови елементи;

2. Икономическите оператори могат да представят информацията, посочена в параграф 1, в продължение на десет години, след като продуктът с цифрови елементи им е бил доставен, и в продължение на десет години, след като те са доставили продукта с цифрови елементи.

ГЛАВА III

СЪОТВЕТСТВИЕ НА ПРОДУКТА С ЦИФРОВИ ЕЛЕМЕНТИ

Член 18

Презумпция за съответствие

1. За продуктите с цифрови елементи и процесите, въведени от производителя, които съответстват на хармонизираните стандарти или на части от тях, данните за които са били публикувани в *Официален вестник на Европейския съюз*, се приема, че съответстват на съществените изисквания, установени в приложение I, обхванати от тези стандарти или части от тях.

2. за продуктите с цифрови елементи и процесите, въведени от производителя, които отговарят на общите спецификации, посочени в член 19, се приема, че съответстват на съществените изисквания, посочени в приложение I, доколкото тези общи спецификации обхващат посочените изисквания.

3. За продуктите с цифрови елементи и процесите, въведени от производителя, за които е издадена ЕС декларация за съответствие или сертификат по европейска схема за сертифициране на киберсигурността, приета съгласно Регламент (ЕС) 2019/881 и посочена в параграф 4, се приема, че съответстват на съществените изисквания, определени в приложение I, доколкото ЕС декларацията за съответствие или сертификатът за киберсигурност, или части от тях, покриват тези изисквания.

4. Комисията има правомощието чрез актове за изпълнение да определи 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. Освен това, когато е приложимо, Комисията посочва дали сертификатът за киберсигурност, издаден по тези схеми, премахва задължението на производителя да извърши оценяване на съответствието от трета страна за съответните изисквания, както е посочено в член 24, параграф 2, букви а) и б) и член 24, параграф 3, букви а) и б). Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 51, параграф 2.

Член 19

Общи спецификации

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.

Член 20

ЕС декларация за съответствие

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

2. ЕС декларацията за съответствие се съставя по образеца, 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.

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

4. Като изготвя ЕС декларация за съответствие, производителят поема отговорността за съответствието на продукта.

5. 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 съответствие, посочено в приложение IV, за да бъде отчетено технологичното развитие.

Член 21

Основни принципи за маркировката „CE“

За маркировката „CE“, определена в член 3, параграф 32, се прилагат основните принципи, определени в член 30 от Регламент (ЕО) № 765/2008.

Член 22

Правила и условия за нанасяне на маркировката „CE“

1. Маркировката „CE“ 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 „CE“ се нанася или в ЕС декларацията за съответствие, посочена в член 20, или в уебсайта, придружаващ софтуерния продукт.

2. Поради естеството на продукта с цифрови елементи височината на маркировката „CE“, нанесена върху продукта с цифрови елементи, може да бъде по-малка от 5 mm, при условие че тя остава видима и четлива.

3. Маркировката „CE“ 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.

4. Маркировката „CE“ е следвана от идентификационния номер на нотифицирания орган, когато този орган участва в процедурата за оценяване на съответствието въз основа на пълно осигуряване на качеството (въз основа на модул H), посочено в член 24.

Идентификационният номер на нотифицирания орган се нанася от самия орган или, по негови указания, от производителя или от негов упълномощен представител.

5. Държавите членки се основават на съществуващите механизми за гарантиране на правилното прилагане на режима за маркировката „CE“ 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 „CE“, маркировката „CE“ указва, че продуктът отговаря и на изискванията на това друго законодателство.

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.

Член 23

Техническа документация

1. Техническата документация включва всички подходящи данни или подробности за средствата, използвани от производителя, за да се гарантира, че продуктът с цифрови елементи и процесите, въведени от производителя, съответстват на изискванията, определени в приложение I. Тя съдържа най-малко данните, посочени в приложение V.

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.

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.

4. Техническата документация и кореспонденцията, свързани с всяка процедура за оценяване на съответствието, се изготвят на официалния език на държавата членка, в която е установен нотифицираният орган, или на език, приемлив за този орган.

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.

Член 24

Процедури за оценяване на съответствието на продукти с цифрови елементи

1. Производителят извършва оценяване на съответствието на продукта с цифрови елементи и процесите, въведени от производителя, за да определи дали са спазени съществените изисквания, посочени в приложение I. Производителят или неговият упълномощен представител доказва съответствието със съществените изисквания, като се използва една от следните процедури:

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

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

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

2. Когато при оценяването на съответствието на даден критичен продукт с цифрови елементи от клас I, както е посочено в приложение III, и на процесите, въведени от неговия производител, със съществените изисквания, посочени в приложение I, производителят или неговият упълномощен представител не е приложил или е приложил само частично хармонизирани стандарти, общи спецификации или европейски схеми за сертифициране на киберсигурността, както е посочено в член 18, или когато такива хармонизирани стандарти, общи спецификации или европейски схеми за сертифициране на киберсигурността не съществуват, по отношение на тези съществени изисквания за съответния продукт с цифрови елементи и за процесите, въведени от производителя, се използва една от следните процедури:

   а) процедура „ЕС изследване на типа“ (въз основа на модул B), определена в приложение VI, последвана от процедура „ЕС съответствие с типа въз основа на вътрешен производствен контрол“ (въз основа на модул C), определена в приложение VI; или

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

3. Когато продуктът е критичен продукт с цифрови елементи от клас II, както е посочено в приложение III, производителят или неговият упълномощен представител доказва съответствието със съществените изисквания, посочени в приложение I, като използва една от следните процедури:

   а) процедура „ЕС изследване на типа“ (въз основа на модул B), определена в приложение VI, последвана от процедура „ЕС съответствие с типа въз основа на вътрешен производствен контрол“ (въз основа на модул C), определена в приложение VI; или

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

4. Производителите на продукти с цифрови елементи, които са класифицирани като системи за ЕЗД в обхвата на Регламент [Регламент относно европейското пространство на здравни данни], доказват съответствието със съществените

изисквания, определени в приложение I към настоящия регламент, като използват съответната процедура за оценяване на съответствието, както се изисква от Регламент [глава III от Регламент относно европейското пространство на здравни данни].

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.

ГЛАВА IV

НОТИФИЦИРАНЕ НА ОРГАНИТЕ ЗА ОЦЕНЯВАНЕ НА СЪОТВЕТСТВИЕТО

Член 25

Нотифициране

Държавите членки нотифицират Комисията и другите държави членки относно органите за оценяване на съответствието, които са упълномощени да извършват оценяване на съответствието в съответствие с настоящия регламент.

Член 26

Нотифициращи органи

1. Държавите членки определят нотифициращ орган, отговорен за установяването и провеждането на необходимите процедури за оценка и нотифициране на органите за оценяване на съответствието, както и за наблюдението на нотифицираните органи, включително съответствието с член 31.

2. Държавите членки могат да решат, че оценката и наблюдението, посочени в параграф 1, се провеждат от национален орган по акредитация по смисъла и в съответствие с Регламент (ЕО) № 765/2008.

Член 27

Изисквания, свързани с нотифициращите органи

1. Нотифициращият орган се създава по такъв начин, че да няма конфликт на интереси с органите за оценяване на съответствието.

2. Нотифициращият орган се организира и работи така, че да се запази обективността и безпристрастността на дейността си.

3. Нотифициращият орган се организира по такъв начин, че всяко решение, свързано с нотифицирането на органа за оценяване на съответствието, да се взема от компетентни лица, различни от тези, които са извършили оценката.

4. Нотифициращият орган не предлага и не извършва дейности, осъществявани от органите за оценяване на съответствието, или консултантски услуги с търговска цел или на конкурентен принцип.

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

6. Нотифициращият орган разполага с достатъчен брой компетентен персонал за правилното изпълнение на своите задачи.

Член 28

Задължение за предоставяне на информация относно нотифициращите органи

1. Държавите членки информират Комисията за своите процедури за оценка и нотифициране на органите за оценяване на съответствието и за наблюдение на нотифицираните органи, както и за всякакви промени във връзка с това.

2. Комисията прави тази информация обществено достояние.

Член 29

Изисквания, свързани с нотифицираните органи

1. За целите на нотифицирането органите за оценяване на съответствието отговарят на изискванията, определени в параграфи 2—12.

2. Органът за оценяване на съответствието се създава съгласно вътрешното право и е юридическо лице.

3. Органът за оценяване на съответствието е трета страна, независима от организацията или от продукта, които оценява.

   Орган, който принадлежи към стопанска асоциация и/или професионална федерация, представляващи предприятия, участващи в проектирането, разработването, производството, доставката, сглобяването, използването или поддръжката на продукти с цифрови елементи, които този орган оценява, може да се счита за такъв орган, при условие че са доказани неговата независимост и липсата на конфликт на интереси.

4. Органът за оценяване на съответствието, неговите ръководители и персонал, отговорен за изпълнение на задачите по оценяване на съответствието, не могат да бъдат проектант, програмист, производител, снабдител, лице, което монтира, купувач, собственик, ползвател или структура по поддръжка на продуктите с цифрови елементи, които се оценяват, нито упълномощени представители на някое от тези лица. Това не изключва използването на оценявани продукти, които са необходими за дейностите на органа за оценяване на съответствието или използването на такива продукти за лични цели.

   Органът за оценяване на съответствието, неговото висше ръководство и персоналът, отговорен за изпълнение на задачите по оценяване на съответствието, не вземат пряко участие в проектирането, разработването, производството, продажбата, монтирането, използването или поддръжката на тези продукти, нито представляват лицата, ангажирани в тези дейности. Те нямат право да участват в никаква дейност, която може да е в противоречие с тяхната независима преценка или почтено поведение по отношение на дейностите по оценяване на съответствието, за които са нотифицирани. Това се прилага по-конкретно към консултантски услуги.

   Органите за оценяване на съответствието гарантират, че дейностите на техните поделения или подизпълнители не влияят върху поверителността,

обективността или безпристрастността на техните дейности по оценяване на съответствието.

5. Органите за оценяване на съответствието и техният персонал осъществяват дейностите по оценяване на съответствието с най-висока степен на почтено професионално поведение и необходимата техническа компетентност в определената област и са напълно освободени от всякакъв натиск и облаги, най-вече финансови, които биха могли да повлияят на тяхната преценка или на резултатите от техните дейности по оценяване на съответствието, особено по отношение на лица или групи лица, заинтересовани от резултатите от тези дейности.

6. Органът за оценяване на съответствието е в състояние да осъществява всички задачи по оценяване на съответствието, посочени в приложение VI и по отношение на които органът е бил нотифициран, независимо дали тези задачи се изпълняват от самия орган за оценяване на съответствието или от негово име и на негова отговорност.

По всяко време и за всяка процедура за оценяване на съответствието, и за всеки вид или категория продукти с цифрови елементи, за които органът за оценяване на съответствието е нотифициран, той разполага с необходимите:

а) персонал с технически знания и достатъчен и подходящ опит за изпълнение на задачите за оценяване на съответствието;

б) описания на процедурите, в съответствие с които се извършва оценяването на съответствието, гарантиращи прозрачността и възможността за повтаряне на тези процедури. Той прилага подходящи политика и процедури, които да позволяват разграничение между задачите, които изпълнява като нотифициран орган, и всички други дейности;

в) процедури за изпълнение на дейности, които надлежно отчитат размера на дадено предприятие, сектора в който осъществява дейност и неговата структура, степента на сложност на съответната технология на продукта и масовия или сериен характер на производството.

Той разполага със средствата, необходими за изпълнение на техническите и административни задачи, свързани с дейностите по оценяване на съответствието по подходящ начин, както трябва да разполага и с достъп до необходимото оборудване или помощни средства.

7. Персоналът, отговорен за провеждането на дейностите по оценяване на съответствието, разполага със следното:

а) добро техническо и професионално обучение, което обхваща всички дейности по оценяване на съответствието, по отношение на които органът за оценяване на съответствието е бил нотифициран;

б) задоволително познаване на изискванията за оценяването, което извършва, както и подходящи правомощия за извършването на такова оценяване;

в) подходящи знания и разбиране на съществените изисквания, на приложимите хармонизирани стандарти и на разпоредбите на законодателството на Съюза за хармонизация, както и актовете за изпълнението му;

г) способност за изготвяне на сертификати, отчети и доклади, които доказват, че оценяванията са извършени.

8. Осигурява се безпристрастността на органите за оценяване на съответствието, на тяхното висше ръководство и на персонала, отговорен за оценяването.

Възнаграждението на ръководителите и на персонала, отговорен за оценките, на органа за оценяване на съответствието не зависи от броя на извършените оценки или от резултатите от тях.

9. Органите за оценяване на съответствието сключват застраховка за покриване на отговорността им, освен ако отговорността се поема от държавата съгласно националното право или държавата членка е пряко отговорна за оценяване на съответствието.

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 документирани процедури, гарантиращи спазването на настоящия параграф.

11. Органите за оценяване на съответствието участват във или гарантират, че персоналът, отговорен за оценките, е информиран за съответните дейности по стандартизация и дейностите на координационната група на нотифицираните органи, създадена съгласно член 40, и прилагат като общи насоки административните решения и документи, приети в резултат от работата на тази група.

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.

Член 30

Презумпция за съответствие на нотифицираните органи

Когато органът за оценяване на съответствието доказва своето съответствие с критериите, определени в съответните хармонизирани стандарти или части от тях, данните за които са били публикувани в *Официален вестник на Европейския съюз*, се приема, че той отговаря на изискванията, установени в член 29, доколкото приложимите хармонизирани стандарти обхващат тези изисквания.

Член 31

Поделения и възлагане на подизпълнители от страна на нотифицираните органи

1. В случаите, в които нотифициран орган възлага на подизпълнители конкретни задачи, свързани с оценяване на съответствието, или използва поделенията си, той гарантира, че подизпълнителят или поделението отговаря на изискванията, определени в член 29, и надлежно информира нотифициращия орган.

2. Нотифицираните органи носят пълна отговорност за дейността, извършена от подизпълнители или дъщерни организации в случаите, когато такива съществуват.

3. Дейностите могат да бъдат възлагани на подизпълнители или изпълнявани от поделения само със съгласието на производителя.

4. Нотифицираните органи съхраняват на разположение на нотифициращия орган съответните документи относно оценката на квалификацията на подизпълнителя или на поделението и работата, извършена от тях съгласно настоящия регламент.

Член 32

Заявление за нотифициране

1. Органът за оценяване на съответствието подава заявление за нотифициране до нотифициращия орган на държавата членка, в която е установен.

2. Това заявление се придружава от описание на дейностите по оценяване на съответствието, процедурата или процедурите за оценяване на съответствието и продукта или продуктите, за които органът заявява компетентност, както и от сертификат за акредитация, когато има такъв, издаден от националния орган по акредитация и удостоверяващ, че органът за оценяване на съответствието отговаря на изискванията, предвидени в член 29.

3. Когато органът за оценяване на съответствието не може да предостави сертификат за акредитация, той представя пред нотифициращия орган всички документи, необходими за проверката, признаването и редовното наблюдение на неговото съответствие с изискванията, посочени в член 29.

Член 33

Процедура по нотифициране

1. Нотифициращите органи могат да нотифицират само органи за оценяване на съответствието, които отговарят на изискванията, установени в член 29.

2. Нотифициращият орган уведомява Комисията и другите държави членки, като използва информационната система NANDO (информационна система за нотифицираните и определените организации по Новия подход), разработена и управлявана от Комисията.

3. Нотифицирането включва всички подробности за дейностите по оценяване на съответствието, модула или модулите за оценяване на съответствието и съответния продукт или продукти, както и съответното удостоверение за компетентност.

4. Когато нотифицирането не се основава на сертификат за акредитация, посочен в член 32, параграф 2, нотифициращият орган предоставя на Комисията и на другите държави членки документите, които удостоверяват компетентността на органа за оценяване на съответствието и съществуващите правила, гарантиращи, че органът ще бъде редовно наблюдаван и ще продължи да отговаря на изискванията, установени в член 29.

5. Съответният орган може да изпълнява дейностите на нотифициран орган само ако от Комисията или от другите държави членки не са повдигнати възражения

в срок от две седмици от нотифицирането — в случай че е използван сертификат за акредитация, или в срок от два месеца от нотифицирането — в случай че не е използвана акредитация.

Само такъв орган се счита за нотифициран орган за целите на настоящия регламент.

6. Комисията и другите държави членки се уведомяват за всякакви последващи промени, свързани с нотификацията.

Член 34

Идентификационни номера и списъци на нотифицираните органи

1. Комисията определя идентификационен номер на нотифицирания орган.

Тя определя само един такъв номер дори когато органът е нотифициран съгласно няколко акта на Съюза.

2. Комисията прави обществено достояние списъка на нотифицираните съгласно настоящия регламент органи, включително определените им идентификационни номера и дейностите, за които те са били нотифицирани.

Комисията прави необходимото за актуализирането на този списък.

Член 35

Промени в нотификациите

1. Когато нотифициращият орган е констатирал или е бил информиран, че даден нотифициран орган вече не отговаря на изискванията, установени в член 29, или че не изпълнява задълженията си, нотифициращият орган ограничава, спира действието или оттегля нотификацията, според случая, в зависимост от сериозността на неспазването на изискванията или на неизпълнението на задълженията. Съответно той незабавно информира за това Комисията и другите държави членки.

2. В случай на ограничение на обхвата, спиране на действието или отмяна на нотификацията или когато нотифицираният орган е прекратил дейността си, нотифициращата държава членка предприема съответните стъпки, за да гарантира, че досиетата на този орган или ще бъдат обработени от друг нотифициран орган, или ще бъдат запазени на разположение на отговорните нотифициращи органи и органи за надзор на пазара, по тяхно искане.

Член 36

Оспорване на компетентността на нотифицирани органи

1. Комисията разследва всички случаи, в които има съмнения или пред нея са изразени съмнения относно компетентността на нотифициран орган или относно непрекъснатото изпълнение от страна на нотифициран орган на изискванията и възложените му отговорности.

2. Нотифициращата държава членка предоставя на Комисията при поискване цялата информация, свързана с основанията за нотификацията или за запазването на компетентността на съответния орган.

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

4. Когато Комисията констатира, че нотифицираният орган не отговаря или престане да отговаря на изискванията за нотифицирането му, тя информира нотифициращата държава членка за това и отправя искане държавата членка да предприеме необходимите корективни мерки, включително, ако е необходимо, отмяна на нотификацията.

Член 37

Задължения на нотифицираните органи при осъществяване на дейността им

1. Нотифицираните органи осъществяват оценяване на съответствието съгласно процедурите за оценяване на съответствието, предвидени в член 24 и приложение VI.

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 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.

3. Въпреки това нотифицираните органи спазват степента на взискателност и равнището на защита, необходими за съответствието на продукта с разпоредбите на регламента.

4. Когато нотифицираният орган прецени, че определен производител не е изпълнил изискванията, предвидени в приложение I или в съответстващите им хармонизирани стандарти или в общите спецификации, посочени в член 19, той изисква от този производител да предприеме подходящите корективни мерки и не издава сертификат за съответствие.

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.

6. Когато не са предприети корективни мерки или те не дадат необходимия резултат, нотифицираният орган ограничава, спира действието или отнема всякакви сертификати, в зависимост от случая.

Член 38

Задължения на нотифицираните органи за предоставяне на информация

1. Нотифицираният орган информира нотифициращите органи за:

   а) всякакъв отказ, ограничаване, спиране на действието или отнемане на сертификати;

   б) всякакви обстоятелства, които влияят върху обхвата и условията на нотифициране;

в) всякакви искания за информация, получени от органите за надзор на пазара, във връзка с дейности за оценка на съответствието;

г) при поискване — за дейностите по оценка на съответствието, извършени в обхвата на тяхната нотификация, и всякакви други извършени дейности, включително трансгранични, и дейности по възлагане на подизпълнители.

2. Нотифицираните органи предоставят на другите органи, нотифицирани съгласно настоящия регламент, осъществяващи подобни дейности по оценяване на съответствието, чийто предмет са същите продукти, съответна информация по проблеми, свързани с отрицателни и, при поискване, положителни резултати от оценяване на съответствието.

Член 39

Обмен на опит

Комисията създава организация за обмен на опит между националните органи на държавите членки, отговорни за политиката по нотификация.

Член 40

Координация на нотифицираните органи

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

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

ГЛАВА V

НАДЗОР НА ПАЗАРА И ПРАВОПРИЛАГАНЕ

Член 41

Надзор на пазара и контрол на продуктите с цифрови елементи, които се въвеждат на пазара на Съюза

1. Регламент (ЕС) 2019/1020 се прилага за продуктите с цифрови елементи в обхвата на настоящия регламент.

2. Всяка държава членка определя един или повече органи за надзор на пазара с цел да се гарантира ефективното прилагане на настоящия регламент. Държавите членки могат да определят съществуващ или нов орган, който да действа като орган за надзор на пазара за целите на настоящия регламент.

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.

4. Когато е приложимо, органите за надзор на пазара си сътрудничат с други органи за надзор на пазара, определени въз основа на друго законодателство на Съюза за хармонизация на други продукти, и редовно обменят информация.

5. Органите за надзор на пазара си сътрудничат по целесъобразност с органите, които упражняват надзор върху правото на Съюза в областта на защитата на личните данни. Това сътрудничество включва информиране на тези органи за всички констатации, които са от значение за изпълнението на техните правомощия, включително при издаването на насоки и съвети съгласно параграф 8 от настоящия член, ако тези насоки и съвети се отнасят до обработването на лични данни.

   Органите, които упражняват надзор върху правото на Съюза в областта на защитата на личните данни, имат правомощието да изискват и получават достъп до всяка документация, създадена или поддържана съгласно настоящия регламент, когато достъпът до тази документация е необходим за осъществяването на задачите им. Те информират определените органи за надзор на пазара на съответната държава членка за всяко такова искане.

6. Държавите членки гарантират, че на определените органи за надзор на пазара се предоставят подходящи финансови и човешки ресурси за изпълнение на задачите им съгласно настоящия регламент.

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

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

9. Органите за надзор на пазара докладват на Комисията на годишна база резултатите от съответните дейности по надзор на пазара. Определените органи за надзор на пазара докладват незабавно на Комисията и на съответните национални органи за защита на конкуренцията всяка информация, установена в хода на дейностите по надзор на пазара, която може да представлява потенциален интерес за прилагането на правото на Съюза в областта на конкуренцията.

10. По отношение на продуктите с цифрови елементи в обхвата на настоящия регламент, класифицирани като високорискови системи с ИИ съгласно член [член 6] от Регламента [Регламента относно ИИ], органите за надзор на пазара, определени за целите на Регламента [Регламент относно ИИ], са органите, които отговарят за дейностите по надзор на пазара, изисквани съгласно настоящия регламент. Органите за надзор на пазара, определени за целите на Регламент [Регламента относно ИИ], си сътрудничат по целесъобразност с органите за надзор на пазара, определени за целите на настоящия регламент, а по отношение на надзора на изпълнението на задълженията за докладване съгласно член 11 — с ENISA. Органите за надзор на пазара, определени в съответствие с Регламент [Регламента относно ИИ], информират по-специално органите за надзор на пазара, определени в съответствие с настоящия регламент, за всички констатации, които са от значение за изпълнението на техните задачи във връзка с прилагането на настоящия регламент.

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.

Член 42

Достъп до данни и документи

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.

Член 43

Процедура на национално равнище по отношение на продукти с цифрови елементи, представляващи значителен киберриск

1. Когато органът за надзор на пазара на дадена държава членка има достатъчно основания да счита, че даден продукт с цифрови елементи, включително отстраняването на уязвимости, представлява значителен киберриск, той извършва оценка на съответния продукт с цифрови елементи по отношение на съответствието му с всички изисквания, установени в настоящия регламент. Съответните икономически оператори оказват необходимото съдействие на органа за надзор на пазара.

   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 коригиращи действия, за да приведе продукта в съответствие с тези изисквания или да го изтегли от пазара, или да го изземе в определен от него разумен срок, съобразен с естеството на риска.

   Органът за надзор на пазара надлежно информира съответния нотифициран орган. За подходящите коригиращи действия се прилага член 18 от Регламент (ЕС) 2019/1020.

2. Когато органът за надзор на пазара счита, че несъответствието не е ограничено само до националната му територия, той информира Комисията и другите държави членки за резултатите от оценката и за действията, които той е изискал да бъдат предприети от оператора.

3. Производителят гарантира, че са предприети всички подходящи коригиращи действия по отношение на всички съответни продукти с цифрови елементи, които той предоставя на пазара в целия Съюз.

4. Когато производителят на даден продукт с цифрови елементи не предприеме подходящи коригиращи 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.

Този орган незабавно информира Комисията и другите държави членки за тези мерки.

5. Информацията, посочена в параграф 4, включва всички налични подробни данни, по-специално данните, необходими за идентифицирането на несъответстващия продукт с цифрови елементи, произхода на продукта с цифрови елементи, естеството на предполагаемото несъответствие и съпътстващия риск, естеството и продължителността на предприетите на национално равнище мерки, както и аргументите, изтъкнати от съответния оператор. По-специално органите за надзор на пазара посочват дали несъответствието се дължи на една или няколко от следните причини:

   а) несъответствие на продукта или на процесите, въведени от производителя, със съществените изисквания, посочени в приложение I;

   б) недостатъци в хармонизираните стандарти, схемите за сертифициране на киберсигурността или общите спецификации, посочени в член 18.

6. Органите за надзор на пазара на държавите членки, различни от органа за надзор на пазара на държавата членка, започнала процедурата, без забавяне информират Комисията и другите държави членки за всички приети мерки и за всяка допълнителна информация, с която разполагат за несъответствието на съответната система с ИИ, и в случай на несъгласие с нотифицираната национална мярка — за своите възражения.

7. Когато в срок от три месеца от получаването на информацията, посочена в параграф 4, не е повдигнато възражение нито от държава членка, нито от Комисията във връзка с временна мярка, предприета от държава членка, тази мярка се счита за обоснована. Това не засяга процедурните права на съответния оператор в съответствие с член 18 от Регламент (ЕС) 2019/1020.

8. Органите за надзор на пазара на всички държави членки гарантират, че без забавяне се вземат подходящите ограничителни мерки по отношение на въпросния продукт, като например изтеглянето на продукта от пазарите им.

Член 44

Предпазна процедура на Съюза

1. Когато в срок от три месеца след получаване на уведомлението по член 43, параграф 4 държава членка е повдигнала възражения срещу мярка, предприета от друга държава членка, или когато Комисията счита, че мярката противоречи на законодателството на Съюза, тя незабавно започва консултации със съответната държава членка и съответния(те) икономически оператор(и) и извършва оценка на тази национална мярка. Въз основа на резултатите от тази оценка Комисията решава дали националната мярка е оправдана или не в срок от девет месеца от уведомлението, посочено в член 43, параграф 4, и уведомява съответната държава членка за това решение.

2. Ако бъде преценено, че националната мярка е оправдана, всички държави членки предприемат необходимите мерки да осигурят изтеглянето от своя пазар на несъответстващия продукт с цифрови елементи и информират Комисията за това. Ако бъде преценено, че националната мярка не е оправдана, съответната държава членка оттегля мярката.

3. Когато се прецени, че националната мярка е оправдана и несъответствието на продукта с цифрови елементи се дължи на недостатъци в хармонизираните стандарти, Комисията прилага процедурата, предвидена в член 10 от Регламент (ЕС) № 1025/2012.

4. Когато се прецени, че националната мярка е оправдана и несъответствието на продукта с цифрови елементи се дължи на недостатъци в европейска схема за сертифициране на киберсигурността, както е посочено в член 18, Комисията преценява дали да измени или отмени акта за изпълнение, както е посочено в член 18, параграф 4, който определя презумпцията за съответствие по отношение на тази схема за сертифициране.

5. Когато националната мярка се счита за оправдана и несъответствието на продукта с цифрови елементи се дължи на недостатъци в общите спецификации, както е посочено в член 19, Комисията преценява дали да измени или отмени акта за изпълнение, посочен в член 19, с който се определят тези общи спецификации.

Член 45

Процедура на равнището на ЕС по отношение на продукти с цифрови елементи, представляващи значителен киберриск

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.

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.

3. Въз основа на оценката на ENISA Комисията може да реши, че е необходима корективна или ограничителна мярка на равнището на Съюза. За тази цел тя незабавно се консултира със съответните държави членки и със съответния(те) икономически оператор(и).

4. Въз основа на консултацията, посочена в параграф 3, Комисията може да приеме актове за изпълнение, за да вземе решение за корективни или ограничителни мерки на равнището на Съюза, включително разпореждане за изтегляне от пазара или изземване, в разумен срок, съобразен с естеството на риска. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 51, параграф 2.

5. Комисията незабавно съобщава решението, посочено в параграф 4, на съответния(те) икономически оператор(и). Държавите членки незабавно

изпълняват актовете, посочени в параграф 4, и надлежно информират Комисията.

6. Параграфи 2—5 се прилагат за срока на извънредната ситуация, която е оправдала намесата на Комисията, и докато съответният продукт не бъде приведен в съответствие с настоящия регламент.

Член 46

Съответстващи продукти с цифрови елементи, които представляват значителен киберриск

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 изземе в разумен срок, съобразен с естеството на риска.

2. Производителят или други съответни оператори гарантират, че се предприемат коригиращи 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.

3. Държавата членка незабавно информира Комисията и другите държави членки за предприетите по параграф 1 мерки. Тази информация включва всички налични подробни данни, по-специално данните, необходими за идентифицирането на съответните продукти с цифрови елементи, произхода и веригата на доставка на тези продукти с цифрови елементи, естеството на съпътстващия риск и естеството и продължителността на взетите на национално равнище мерки.

4. Комисията без забавяне започва консултации с държавите членки и съответния икономически оператор и оценява предприетата национална мярка. Въз основа на резултатите от тази оценка Комисията взема решение дали мярката е оправдана или не и когато е необходимо, предлага подходящи мерки.

5. Комисията адресира решението си до държавите членки.

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.

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.

8. Въз основа на оценката на ENISA, посочена в параграф 7, Комисията може да определи, че е необходима корективна или ограничителна мярка на равнището на Съюза. За тази цел тя незабавно се консултира със съответните държави членки и със съответния(те) оператор(и).

9. Въз основа на консултацията, посочена в параграф 8, Комисията може да приеме актове за изпълнение, за да вземе решение за корективни или ограничителни мерки на равнището на Съюза, включително разпореждане за изтегляне от пазара или изземване, в разумен срок, съобразен с естеството на риска. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 51, параграф 2.

10. Комисията незабавно съобщава решението, посочено в параграф 9, на съответния(те) оператор(и). Държавите членки изпълняват такива актове без забавяне — и уведомяват Комисията за това.

11. Параграфи 6—10 се прилагат за срока на извънредната ситуация, която е оправдала намесата на Комисията, и докато съответният продукт продължава да носи рисковете, посочени в параграф 1.

Член 47

Официално несъответствие

1. Когато органът за надзор на пазара на дадена държава членка направи някоя от следните констатации, той изисква от съответния производител да прекрати въпросното несъответствие:

   а) маркировката за съответствие е нанесена в нарушение на членове 21 и 22;

   б) маркировката за съответствие не е нанесена;

   в) ЕС декларацията за съответствие не е съставена;

   г) ЕС декларацията за съответствие е съставена неправилно;

   д) идентификационният номер на нотифицирания орган, участващ в процедурата за оценка на съответствието, когато е приложимо, не е нанесен.

   е) техническата документация не е налице или не е пълна.

2. Когато несъответствието, посочено в параграф 1, продължи, съответната държава членка предприема всички подходящи мерки да ограничи или да забрани предоставянето на продукта с цифрови елементи на пазара, или да осигури неговото изземване или изтегляне от пазара.

Член 48

Съвместни дейности на органите за надзор на пазара

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.

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.

3. Когато е приложимо, органите за надзор на пазара и Комисията гарантират, че споразумението за извършване на съвместни дейности не води до нелоялна конкуренция между икономическите оператори и не засяга по отрицателен начин обективността, независимостта и безпристрастността на страните по споразумението.

4. Органът за надзор на пазара може да използва всяка информация, получена в резултат на дейностите, извършени като част от предприето от него разследване.

5. Когато е приложимо, съответният орган за надзор на пазара и Комисията правят споразумението за съвместни дейности, включително имената на участващите страни, достъпно за обществеността.

Член 49

Мащабни проверки

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.

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.

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.

4. Когато провеждат мащабни проверки, участващите органи за надзор на пазара могат да използват правомощията за разследване, предвидени в членове 41—

47, и всички други правомощия, предоставени им по силата на националното право.

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

ГЛАВА VI

ДЕЛЕГИРАНИ ПРАВОМОЩИЯ И ПРОЦЕДУРА НА КОМИТЕТ

Член 50

Упражняване на делегирането

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

2. Правомощието да приема делегирани актове, посочено в член 2, параграф 4, член 6, параграфи 2, 3 и 5, член 20, параграф 5 и член 23, параграф 5 се предоставя на Комисията.

3. Делегирането на правомощия, посочено в член 2, параграф 4, член 6, параграфи 2, 3 и 5, член 20, параграф 5 и член 23, параграф 5 може да бъде оттеглено по всяко време от Европейския парламент или от Съвета. С решението за оттегляне се прекратява посоченото в него делегиране на правомощия. Оттеглянето поражда действие в деня след публикуването на решението в *Официален вестник на Европейския съюз* или на по-късна дата, посочена в решението. То не засяга действителността на делегираните актове, които вече са в сила.

4. Преди приемането на делегиран акт Комисията се консултира с експерти, определени от всяка държава членка в съответствие с принципите, залегнали в Междуинституционалното споразумение от 13 април 2016 г. за по-добро законотворчество.

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

6. Делегиран акт, приет съгласно член 2, параграф 4, член 6, параграфи 2, 3 и 5, член 20, параграф 5 и член 23, параграф 5 влиза в сила единствено ако нито Европейският парламент, нито Съветът не са представили възражения в срок от два месеца след нотифицирането на същия акт на Европейския парламент и Съвета или ако преди изтичането на този срок и Европейският парламент, и Съветът са уведомили Комисията, че няма да представят възражения. Този срок се удължава с два месеца по инициатива на Европейския парламент или на Съвета.

Член 51

Процедура на комитет

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

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

3. Когато становището на комитета трябва да бъде получено по писмена процедура, тази процедура се прекратява без резултат, ако в рамките на срока за даване на становище председателят на комитета вземе такова решение или член на комитета отправи такова искане.

ГЛАВА VII

ПОВЕРИТЕЛНОСТ И САНКЦИИ

Член 52

Поверителност

1. Всички страни, участващи в прилагането на настоящия регламент, зачитат поверителността на информацията и данните, получавани при изпълнение на техните задачи и дейности, така че да защитават по-специално:

   а) правата върху интелектуалната собственост и поверителната търговска информация или търговски тайни на дадено физическо или юридическо лице, включително изходния код, освен в случаите, посочени в член 5 от Директива 2016/943 на Европейския парламент и на Съвета[24];

   б) ефективното прилагане на настоящия регламент, по-конкретно при проверките, разследванията или одитите;

   в) обществения интерес и националната сигурност;

   г) независимостта на наказателните или административните производства.

2. Без да се засяга параграф 1, информацията, обменена на поверителна основа между самите органи за надзор на пазара и между органите за надзор на пазара и Комисията, не се разкрива без предварителното съгласие на предоставилия тази информация орган за надзор на пазара.

3. Параграфи 1 и 2 не засягат правата и задълженията на Комисията, държавите членки и нотифицираните органи по отношение на обмена на информация и разпространяването на предупреждения, нито задълженията на засегнатите лица за представяне на информация съгласно наказателното право на държавите членки.

4. Комисията и държавите членки могат при необходимост да обменят чувствителна информация със съответните органи на трети държави, с които са сключили двустранни или многостранни споразумения, като гарантират адекватно равнище на защита.

Член 53

Санкции

[24] Директива (ЕС) 2016/943 на Европейския парламент и на Съвета от 8 юни 2016 г. относно защитата на неразкрити ноу-хау и търговска информация (търговски тайни) срещу тяхното незаконно придобиване, използване и разкриване (ОВ L 157, 15.6.2016 г., стр. 1).

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.

2. Държавите членки незабавно съобщават на Комисията тези правила и мерки и незабавно я уведомяват за всяко последващо изменение, което ги засяга.

3. Неспазването на съществените изисквания за киберсигурност, посочени в приложение I, и на задълженията, посочени в членове 10 и 11, подлежи на административни глоби в размер до 15 000 000 EUR или, ако нарушителят е дружество, до 2,5 % от общия му годишен световен оборот за предходната финансова година, в зависимост от това коя от двете суми е по-висока.

4. Неспазването на всякакви други изисквания съгласно настоящия регламент подлежи на административни глоби в размер до 10 000 000 EUR или, ако нарушителят е дружество, до 2 % от общия му годишен световен оборот за предходната финансова година, в зависимост от това коя от двете суми е по-висока.

5. Предоставянето на неправилна, непълна или подвеждаща информация в отговор на искане от нотифицираните органи и органите за надзор на пазара подлежи на административни глоби в размер до 5 000 000 EUR или, ако нарушителят е дружество, до 1 % от общия му годишен световен оборот за предходната финансова година, в зависимост от това коя от двете суми е по-висока.

6. При вземането на решение относно размера на административната глоба във всеки отделен случай се вземат предвид всички обстоятелства от значение за конкретната ситуация и се обръща надлежно внимание на следното:

   а) естеството, тежестта и продължителността на нарушението и последиците от него;

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

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

7. Органите за надзор на пазара, които налагат административни глоби, споделят тази информация с органите за надзор на пазара на други държави членки чрез информационната и комуникационната система, посочена в член 34 от Регламент (ЕС) 2019/1020.

8. Всяка държава членка определя правила за това дали и до каква степен могат да бъдат налагани административни глоби на публични органи и структури, установени в тази държава членка.

9. В зависимост от правната система на държавите членки правилата относно административните глоби могат да се прилагат по такъв начин, че глобите да се налагат от компетентните национални съдилища или други органи в съответствие с компетентностите, определени на национално равнище в тези държави членки. Прилагането на тези правила в тези държави членки има равностоен ефект.

10. В зависимост от обстоятелствата на всеки отделен случай могат да бъдат наложени административни глоби в допълнение към други корективни или

ограничителни мерки, приложени от органите за надзор на пазара за същото нарушение.

Глава VIII

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 54

Изменение на Регламент (ЕС) 2019/1020

В приложение I към Регламент (ЕС) 2019/1020 се добавя следната точка:

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

Член 55

Преходни разпоредби

1. Сертификатите за „ЕС изследване на типа“ и решенията за одобрение, издадени по отношение на изискванията за киберсигурност за продукти с цифрови елементи, които са предмет на друго законодателство на Съюза за хармонизация, остават валидни до [42 месеца след датата на влизане в сила на настоящия регламент], освен ако срокът им на валидност изтича преди тази дата или ако няма други разпоредби в друго законодателство на Съюза, в който случай те остават валидни, както е посочено в това законодателство на Съюза.
2. Продукти с цифрови елементи, които са пуснати на пазара преди [дата на прилагане на настоящия регламент, посочена в член 57], подлежат на изискванията на настоящия регламент само ако от тази дата тези продукти са предмет на съществени изменения в техния проект или предвидена употреба.
3. Като изключение от параграф 2, определените в член 11 задължения се прилагат за всички продукти с цифрови елементи в обхвата на настоящия регламент, които са били пуснати на пазара преди [дата на прилагане на настоящия регламент, посочена в член 57].

Член 56

Оценка и преглед

В срок до [36 месеца след датата на прилагане на настоящия регламент] и на всеки четири години след това, Комисията представя на Европейския парламент и на Съвета доклад относно оценката и прегледа на настоящия регламент. Тези доклади се публикуват.

Член 57

Влизане в сила и прилагане

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

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].

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

Съставено в Брюксел на […] година.

За Европейския парламент	*За Съвета*
Председател	*Председател*

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1. Наименование на предложението/инициативата

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

1.3. Предложението/инициативата е във връзка с:

1.4. Цел(и)

1.4.1. Обща(и) цел(и)

1.4.2. Специфична(и) цел(и)

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

1.4.4. Показатели за изпълнението

1.5. Мотиви за предложението/инициативата

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

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

1.5.3. Изводи от подобен опит в миналото

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

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

1.6. Продължителност и финансово отражение на предложението/инициативата

1.7. Планиран(и) метод(и) на управление

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

2.2. Системи за управление и контрол

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

2.2.2. Информация относно установените рискове и системата(ите) за вътрешен контрол, създадена(и) с цел намаляването им

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

2.3. Мерки за предотвратяване на измами и нередности

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

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

3.2. Очаквано финансово отражение на предложението върху бюджетните кредити

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

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

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

3.2.4. Съвместимост с настоящата многогодишна финансова рамка

3.2.5. Финансов принос от трети страни

3.3. Очаквано отражение върху приходите

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1. Наименование на предложението/инициативата

Предложение за регламент относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи (Законодателен акт за киберустойчивост)

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

Съобщителни мрежи, съдържание и технологии

1.3. Предложението/инициативата е във връзка с:

× **ново действие**

☐ **ново действие след пилотен проект/подготвително действие**[37]

☐ **продължаване на съществуващо действие**

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

1.4. Цел(и)

1.4.1. Обща(и) цел(и)

Предложението има две основни цели, които трябва да осигурят правилното функциониране на вътрешния пазар: 1) **създаване на условия за разработване на защитени продукти с цифрови елементи**, като се гарантира, че на пазара се пускат хардуерни и софтуерни продукти с по-малко уязвимости, както и че производителите се отнасят сериозно към защитата през целия жизнен цикъл на продукта; и 2) **създаване на условия, които позволяват на ползвателите да вземат предвид киберсигурността при избора и използването на продукти с цифрови елементи**.

1.4.2. Специфична(и) цел(и)

Определени бяха **четири специфични цели** за предложението: i) да се гарантира, че производителите подобряват защитата на продуктите с цифрови елементи още от етапа на проектиране и разработване и през целия жизнен цикъл; ii) да се осигури съгласувана рамка за киберсигурност, която улеснява спазването на изискванията от производителите на хардуер и софтуер; iii) да се повиши прозрачността на характеристиките за защитата на продуктите с цифрови елементи и iv) да се даде възможност на предприятията и потребителите да използват продуктите с цифрови елементи по безопасен начин.

Очакван(и) резултат(и) и въздействие

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

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

Предложението би донесло значителни ползи за различните заинтересовани страни. За предприятията то би предотвратило различаващите се правила за сигурността за продукти с цифрови елементи и би намалило разходите за привеждане в съответствие със свързаното законодателство в областта на киберсигурността. То би намалило броя на киберинцидентите, разходите за действията при инцидент и накърняването на репутацията. За целия ЕС се смята, че инициативата би могла да доведе до намаляване на разходите от инциденти, засягащи дружествата приблизително със 180—290 млрд. евро годишно[38]. В резултат на това би се увеличил оборотът поради повишеното търсене на продукти с цифрови елементи. Съответно би се подобрила репутацията на дружествата в световен мащаб, което води до увеличаване на търсенето и извън ЕС. За ползвателите предпочитаният вариант би повишил прозрачността на характеристиките на сигурността и би улеснил използването на продуктите с цифрови елементи. Потребителите и гражданите ще се възползват и от по-добрата защита на основните си права, като неприкосновеност на личния живот и защита на личните данни.

В същото време предложението ще увеличи разходите за спазване и прилагане на законодателството за предприятията, нотифицираните органи и публичните органи, включително органите за акредитация и надзор на пазара. За разработчиците на софтуер и производителите на хардуер то ще увеличи преките разходи за спазване на новите изисквания за сигурност, за оценяването на съответствието, за документацията и задълженията за докладване, което ще доведе до съвкупни разходи за спазване на изискванията, възлизащи приблизително на 29 млрд. евро при приблизителна пазарна стойност на оборота от 1485 млрд. евро[39]. Ползвателите, включително стопанските ползватели, потребителите и гражданите, може да се изправят пред по-високи цени на продуктите с цифрови елементи. Тези цени обаче следва да се разглеждат на фона на значителните ползи, описани по-горе.

1.4.3. Показатели за изпълнението

Посочете показателите за проследяване на напредъка и на постиженията.

За да се провери дали производителите подобряват защитата на своите продукти с цифрови елементи още на етапа на проектиране и разработване и през целия жизнен цикъл на тези продукти, могат да се вземат предвид няколко показателя. Това биха могли да бъдат броят на значителните инциденти в Съюза, причинени от уязвимости, делът на производителите на хардуер и софтуер, които систематично се придържат към безопасен жизнен цикъл на разработване, качествен анализ на сигурността на продуктите с цифрови елементи, количествена и качествена оценка на базите данни за уязвимости, честотата на предоставяните от производителите актуализации в областта на сигурността или средният брой дни между откриването на уязвимост и предоставянето на корекции.

[38] Вж. [Работен документ на службите на Комисията относно доклада за оценка на въздействието, придружаващ Регламента относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи].

[39] Вж. [Работен документ на службите на Комисията относно доклада за оценка на въздействието, придружаващ Регламента относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи].

Показател за съгласувана рамка за киберсигурност може да бъде липсата на целенасочено национално законодателство за киберсигурност, специфично за даден продукт.

Показател за повишена прозрачност по отношение на характеристиките за сигурност на продуктите с цифрови елементи може да бъде делът на продуктите с цифрови елементи, които се доставят с информация за характеристиките за сигурност. Освен това делът на продуктите с цифрови елементи, които се доставят с инструкции за безопасно използване, би могъл да се използва като показател за това дали организациите и потребителите имат възможност да използват продуктите с цифрови елементи по безопасен начин.

Що се отнася до наблюдението на въздействието на регламента, за тази цел ще се обмислят определени показатели, които ще бъдат оценявани от Комисията, по целесъобразност с подкрепата на ENISA. В зависимост от оперативната цел, която трябва да бъде постигната, някои от показателите за наблюдение, въз основа на които ще се оценява успехът на хоризонталните изисквания за киберсигурност, са следните:

За оценяване на нивото на киберсигурност на продуктите с цифрови елементи:

— Статистически данни и качествен анализ на инцидентите, засягащи продукти с цифрови елементи, и начина, по който са били отстранени. Те могат да бъдат събирани и оценявани от Комисията с подкрепата на ENISA.

— Регистри на известни уязвимости и анализи на начина, по който са били отстранени. Такъв анализ би могъл да бъде извършен от ENISA въз основа на европейската база данни за уязвимости, създадена въз основа на [Директива XXX/XXXX (МИС 2)].

— Проучвания сред производителите на хардуер и софтуер за проследяване на напредъка.

За оценяване на нивото на информация относно защитените елементи, поддръжката на сигурността, края на експлоатационния срок и задължението за полагане на дължима грижа: резултати от проучвания, които Комисията ще проведе с подкрепата на ENISA както сред ползвателите, така и сред предприятията.

За оценяване на изпълнението Комисията ще се стреми да гарантира, че оценките на съответствието се извършват ефективно. За тази цел ще бъде отправено искане за стандартизация и ще бъде проследено неговото изпълнение. Комисията също така ще провери капацитета на нотифицираните органи и, ако е приложимо, на сертифициращите органи.

Що се отнася до прилагането, чрез докладите на държавите членки Комисията ще проверява дали националните инициативи не засягат аспекти, обхванати от регламента.

1.5. Мотиви за предложението/инициативата

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

Регламентът следва да започне да се прилага изцяло 24 месеца след влизането му в сила. Елементите на управленската структура обаче следва да бъдат въведени преди това. По-специално държавите членки са определили съществуващи органи и/или са създали нови органи, които да изпълняват задачите, определени в законодателството.

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

Силно изразеният трансграничен характер на киберсигурността и нарастващият брой инциденти, които се разпространяват в други държави, сектори и продукти, означават, че целите не могат да бъдат постигнати ефективно само от държавите членки. Предвид глобалния характер на пазарите на продукти с цифрови елементи, държавите членки са изправени пред едни и същи рискове за един и същ продукт с цифрови елементи на тяхна територия. Възникващата разнородна рамка от потенциално различаващи се национални правила също създава риск да попречи на отворения и конкурентен единен пазар за продукти с цифрови елементи. Следователно са необходими съвместни действия на равнището на ЕС, за да се повиши доверието на ползвателите и привлекателността на продуктите с цифрови елементи в ЕС. Те ще бъдат от полза и за вътрешния пазар, тъй като ще осигурят правна сигурност и равнопоставеност на доставчиците на продукти с цифрови елементи.

1.5.3. Изводи от подобен опит в миналото

Законодателният акт за киберустойчивост е първият по рода си нормативен акт, който въвежда изисквания за киберсигурност при пускането на пазара на продукти с цифрови елементи. Той обаче се основава на начина на работа по новата законодателна рамка и на изводите, направени в процеса на прилагане на съществуващото законодателство на Съюза за хармонизация на различни продукти, особено по отношение на подготовката за прилагане, в това число аспекти като изготвянето на хармонизирани стандарти.

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

Регламентът относно хоризонталните изисквания за киберсигурност за продукти с цифрови елементи определя нови изисквания за киберсигурност за всички продукти с цифрови елементи, пуснати на пазара на ЕС, които надхвърлят изискванията, предвидени в съществуващото законодателство. Същевременно предложението се основава на съществуващия начин на работа за законодателство от новата законодателна рамка (НЗР). Следователно то ще

се основава на съществуващите структури и процедури на НЗР, като например сътрудничеството между нотифицираните органи и надзора на пазара, модулите за оценяване на съответствието, разработването на хармонизирани стандарти. Новото предложение ще се основава и на някои структури, разработени съгласно друго законодателство в областта на киберсигурността, като Директива (ЕС) 2016/1148 (Директива за МИС), съответно [Директива XXX/XXXX (МИС 2)], или Регламент (ЕС) 2019/881 (Акт за киберсигурността).

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

Управлението на областите на действие, възложени на ENISA, съответства на нейния съществуващ мандат и общи задачи. Тези области на действие може да изискват специфични профили или нови задачи, но те няма да бъдат значими и могат да бъдат поети от съществуващите ресурси на ENISA чрез преразпределение или свързване на различни задачи. Например една от основните области на действие, възложени на ENISA, е свързана със събирането и обработването на уведомления от производители за използвани уязвимости на продукти. С [Директива XXX/XXXX (МИС 2)] на ENISA вече е възложено да създаде европейска база данни за уязвимости, в която обществено известни уязвимости могат да бъдат оповестявани и регистрирани доброволно с цел да се даде възможност на ползвателите да предприемат смекчаващи мерки. Ресурсите, отпуснати за тази цел, биха могли да се използват и за горепосочените нови задачи, свързани с уведомленията за уязвимости на продукти. Така би могло да се гарантира ефективното използване на съществуващите ресурси, както и да се създадат необходимите полезни взаимодействия между такива задачи, чрез които ENISA може да получава по-добра информация за своите анализи на киберрисковете и заплахите за киберсигурността.

1.6. Продължителност и финансово отражение на предложението/инициативата

☐ **ограничен срок на действие**

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

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

× **неограничен срок на действие**

– Осъществяване с период на започване на дейност от 2025 г.

– последван от функциониране с пълен капацитет.

1.7. Планиран(и) метод(и) на управление[40]

☐ **Пряко управление** от Комисията

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

– ☐ от изпълнителните агенции

☐ **Споделено управление** с държавите членки

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

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

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

– ☐ ЕИБ и Европейския инвестиционен фонд;

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

– ☐ публичноправни органи;

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

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

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

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

Забележки

С настоящия регламент на ENISA се възлагат определени действия в съответствие със съществуващия ѝ мандат, и по-специално член 3, параграф 2 от Регламент 2019/881, с който се установява, че ENISA следва да изпълнява задачите, възложени ѝ чрез правни

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

актове на Съюза, с които се определят мерки за сближаване на свързаните с киберсигурността законови, подзаконови и административни разпоредби на държавите членки. По-специално ENISA ще получава уведомления от производителите за активно използвани уязвимости, които се съдържат в продуктите 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 ЕРИКС или съответно до съответното единно звено за контакт, определено в съответствие с член [член X] от Директива [Директива XXX/XXXX (МИС 2)], на държавите членки, както и да информира органите за надзор на пазара. 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. Освен това, като се има предвид експертният опит на ENISA, събраната информация и анализите на заплахите, ENISA може да подкрепи процеса на прилагане на настоящия регламент, като предложи съвместни дейности, които да бъдат проведени от националните органи 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 могат да бъдат организирани едновременни координирани действия за контрол. Комисията може да поиска от ENISA да извършва оценки на конкретни продукти при извънредни обстоятелства във връзка с продукти с цифрови елементи, които представляват значителен киберриск и когато е необходима незабавна намеса за запазване на доброто функциониране на вътрешния пазар.

Всички тези задачи се оценяват на около 4,5 ЕПРВ от съществуващите ресурси на ENISA, като се основават на експертния опит и подготвителната работа, която понастоящем се извършва от ENISA, наред с другото, в подкрепа на предстоящото прилагане на [Директива XXX/XXXX (МИС 2)], за което ресурсите на ENISA бяха допълнени.

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

Да се посочат честотата и условията.

В срок до [36 месеца след датата на прилагане на настоящия регламент] и на всеки четири години след това, Комисията ще представя на Европейския парламент и на Съвета доклад относно оценката и прегледа му. Тези доклади се публикуват.

2.2. Системи за управление и контрол

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

С настоящия регламент се установява нова политика по отношение на хармонизираните изисквания за киберсигурност за продукти с цифрови елементи, които се пускат на вътрешния пазар, през целия им жизнен цикъл. Правният акт ще бъде последван от искания от страна на Комисията към европейските органи за стандартизация за разработване на стандарти. За да се отговори на тези нови задачи, е необходимо да се осигурят подходящи ресурси за службите на Комисията. Изчислено е, че за прилагането на новия регламент ще са необходими 7 ЕПРВ (от които един КНЕ), за да се обхванат следните задачи:

- Изготвяне на искане за стандартизация и/или общи спецификации чрез актове за изпълнение при липса на успешен процес на стандартизация;
- Изготвяне на делегиран акт [в срок от 12 месеца от влизането в сила на регламента], в който се посочват определенията на критичните продукти с цифрови елементи;
- Потенциално изготвяне на делегирани актове за актуализиране на списъка с критични продукти от клас I и II; уточняване дали е необходимо ограничение или изключване за продукти с цифрови елементи, обхванати от други правила на Съюза, с които се определят изисквания, постигащи същото ниво на защита като настоящия регламент; налагане на задължение за сертифициране на някои продукти с цифрови елементи с висока степен на критичност въз основа на критериите, определени в настоящия регламент; уточняване на минималното съдържание на ЕС декларацията за съответствие и допълване на елементите, които трябва да бъдат включени в техническата документация;
- Потенциално изготвяне на актове за изпълнение, свързани с формата или елементите на задълженията за докладване, описа на софтуерните компоненти, общите спецификации или поставянето на маркировката „CE“;
- Потенциална подготовка на незабавна намеса за налагане на корективни или ограничителни мерки при извънредни обстоятелства с цел запазване на доброто функциониране на вътрешния пазар, включително изготвяне на акт за изпълнение;

– Организиране и координиране на уведомленията от страна на държавите членки за нотифицирани органи и координиране на нотифицираните органи;

– Подпомагане на координацията на органите за надзор на пазара на държавите членки.

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

С цел да се гарантира, че нотифицираните органи и органите за надзор на пазара обменят информация и си сътрудничат добре, Комисията отговаря за тяхната координация. По отношение на техническия и пазарния експертен опит ще бъде създадена експертна група.

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

2.3. По отношение на разходите за срещи, като се има предвид ниската стойност на трансакция (напр. възстановяване на пътни разходи на делегат за среща), стандартните процедури за контрол изглеждат достатъчни. Мерки за предотвратяване на измами и нередности

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

Съществуващите мерки за предотвратяване на измами, приложими за Комисията, ще покрият допълнителните бюджетни кредити, необходими за настоящия регламент.

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

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

- Съществуващи бюджетни редове

Схема

- Поискани нови бюджетни редове

Неприложимо

3.2. Очаквано финансово отражение на предложението върху бюджетните кредити

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

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

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

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

Функция от многогодишната финансова рамка	Номер	

ГД: <…….>			Година **N**[41]	Година **N+1**	Година **N+2**	Година **N+3**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)			**ОБЩО**
• Оперативни бюджетни кредити										
Бюджетен ред[42]	Поети задължения	1а)								
	Плащания	2а)								
Бюджетен ред	Поети задължения	1б)								
	Плащания	2б)								
Бюджетни кредити за административни разходи, финансирани от пакета за определени програми[43]										

41 Година N е годината, през която започва да се изпълнява предложението/инициативата. Моля, заменете буквата N с очакваната първа година от изпълнението (например: 2021). Същото за следващите години.

42 Съгласно официалната бюджетна номенклатура.

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

Бюджетен ред		3)								
ОБЩО бюджетни кредити за ГД <…….>	Поети задължения	=1а+1б +3								
	Плащания	=2а+2б +3								

• ОБЩО бюджетни кредити за оперативни операции	Поети задължения	4)								
	Плащания	5)								
• ОБЩО бюджетни кредити за административни разходи, финансирани от пакета за определени програми		6)								
ОБЩО бюджетни кредити за ФУНКЦИЯ <….> от многогодишната финансова рамка	Поети задължения	=4+6								
	Плащания	=5+6								

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

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

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

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

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

		Година **2024**	Година **2025**	Година **2026**	Година **2027**	**ОБЩО**
ГД: ГД „Съобщителни мрежи, съдържание и технологии“ (CNECT)						
• Човешки ресурси		1,030	1,030	1,030	1,030	**4,120**
• Други административни разходи		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
ОБЩО за ГД „Съобщителни мрежи, съдържание и технологии“ (CNECT)	Бюджетни кредити	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

ОБЩО бюджетни кредити за ФУНКЦИЯ 7 от многогодишната финансова рамка	(Общо поети задължения = Общо плащания)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

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

		Година **2024**	Година **2025**	Година **2026**	Година **2027**	**ОБЩО**
ОБЩО бюджетни кредити за ФУНКЦИИ 1—7 от многогодишната финансова рамка	Поети задължения	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Плащания	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

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

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

Да се посочат целите и резултатите ⇩			Година **N**		Година **N+1**		Година **N+2**		Година **N+3**		Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)						**ОБЩО**	
	РЕЗУЛТАТИ																	
	Вид[44]	Среден разход	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Общ бр.	Общо разходи
СПЕЦИФИЧНА ЦЕЛ № 1[45] …																		
— Резултат																		
— Резултат																		
— Резултат																		
Междинен сбор за специфична цел № 1																		
СПЕЦИФИЧНА ЦЕЛ № 2 …																		
— Резултат																		
Междинен сбор за специфична цел № 2																		
ОБЩО																		

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

[45] Съгласно описанието в точка 1.4.2. „Специфична(и) цел(и)...“

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

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

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

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

	Година **2024**	Година **2025**	Година **2026**	Година **2027**	
ФУНКЦИЯ 7 от многогодишната финансова рамка					
Човешки ресурси	1,030	1,030	1,030	1,030	**4,120**
Други административни разходи	0,222	0,222	0,222	0,222	**0,888**
Междинен сбор за ФУНКЦИЯ 7 от многогодишната финансова рамка	1,252	1,252	1,252	1,252	**5,008**

Извън ФУНКЦИЯ 7[46] **от многогодишната финансова рамка**					
Човешки ресурси					
Други разходи с административен характер					
Междинен сбор извън ФУНКЦИЯ 7 от многогодишната финансова рамка					

ОБЩО	1,252	1,252	1,252	1,252	**5,008**

Бюджетните кредити, необходими за човешки ресурси и други разходи с административен характер, ще бъдат покрити от бюджетни кредити на ГД, които вече са определени за управлението на действието и/или които са преразпределени в рамките на ГД, при необходимост заедно с допълнително отпуснати ресурси, които могат да бъдат предоставени на управляващата ГД в рамките на годишната процедура за отпускане на средства и като се имат предвид бюджетните ограничения.

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

3.2.3.1. Очаквани нужди от човешки ресурси

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

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

Оценката се посочва в еквиваленти на пълно работно време

		Година 2024	Година 2025	Година 2026	Година 2027
20 01 02 01 (Централа и представителства на Комисията)		6	6	6	6
20 01 02 03 (Делегации)					
01 01 01 01 (Непреки научни изследвания)					
01 01 01 11 (Преки научни изследвания)					
Други бюджетни редове (да се посочат)					
• Външен персонал (в еквивалент на пълно работно време: ЕПРВ)[47]					
20 02 01 (ДНП, КНЕ, ПНА от общия финансов пакет)		1	1	1	1
20 02 03 (ДНП, МП, КНЕ, ПНА и МЕД в делегациите)					
XX 01 xx **yy zz** [48]	— в централата				
	— в делегациите				
01 01 01 02 (ДНП, КНЕ, ПНА — Непреки научни изследвания)					
01 01 01 12 (ДНП, КНЕ, ПНА — Преки научни изследвания)					
Други бюджетни редове (да се посочат)					
ОБЩО		**7**	**7**	**7**	**7**

XX е съответната област на политиката или бюджетен дял.

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

Описание на задачите, които трябва да се изпълнят:

Длъжностни лица и срочно наети служители 6 ЕПРВ x 157 000 EUR/година = 942 000 EUR	Както е описано в 2.2.1: – Изготвяне на искане за стандартизация и/или общи спецификации чрез актове за изпълнение при липса на успешен процес на стандартизация; – Изготвяне на делегиран акт [в срок от 12 месеца от влизането в сила на регламента], в който се посочват определенията на критичните продукти с цифрови елементи; – Потенциално изготвяне на делегирани актове за актуализиране на списъка с критични продукти от клас I и II; уточняване дали е необходимо ограничение или изключване за продукти с цифрови елементи, обхванати от други правила на Съюза, с които се определят изисквания, постигащи същото ниво на защита като настоящия

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

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

	регламент; налагане на задължение за сертифициране на някои продукти с цифрови елементи с висока степен на критичност въз основа на критериите, определени в настоящия регламент; уточняване на минималното съдържание на ЕС декларацията за съответствие и допълване на елементите, които трябва да бъдат включени в техническата документация; – Потенциално изготвяне на актове за изпълнение, свързани с формата или елементите на задълженията за докладване, описа на софтуерните компоненти, общите спецификации или поставянето на маркировката „CE“; – Потенциална подготовка на незабавна намеса за налагане на корективни или ограничителни мерки при извънредни обстоятелства с цел запазване на доброто функциониране на вътрешния пазар, включително изготвяне на акт за изпълнение; – Организиране и координиране на уведомленията от страна на държавите членки за нотифицирани органи и координиране на нотифицираните органи; – Подпомагане на координацията на органите за надзор на пазара на държавите членки.
Външен персонал 1 КНЕ x 88 000 EUR/година	Както е описано в 2.2.1: – Изготвяне на искане за стандартизация и/или общи спецификации чрез актове за изпълнение при липса на успешен процес на стандартизация; – Изготвяне на делегиран акт [в срок от 12 месеца от влизането в сила на регламента], в който се посочват определенията на критичните продукти с цифрови елементи; – Потенциално изготвяне на делегирани актове за актуализиране на списъка с критични продукти от клас I и II; уточняване дали е необходимо ограничение или изключване за продукти с цифрови елементи, обхванати от други правила на Съюза, с които се определят изисквания, постигащи същото ниво на защита като настоящия регламент; налагане на задължение за сертифициране на някои продукти с цифрови елементи с висока степен на критичност въз основа на критериите, определени в настоящия регламент; уточняване на минималното съдържание на ЕС декларацията за съответствие и допълване на елементите, които трябва да бъдат включени в техническата документация; – Потенциално изготвяне на актове за изпълнение, свързани с формата или елементите на задълженията за докладване, описа на софтуерните компоненти, общите спецификации или поставянето на маркировката „CE“; – Потенциална подготовка на незабавна намеса за налагане на корективни или ограничителни мерки при извънредни обстоятелства с цел запазване на доброто функциониране на вътрешния пазар, включително изготвяне на акт за изпълнение; – Организиране и координиране на уведомленията от страна на държавите членки за нотифицирани органи и координиране на нотифицираните органи; – Подпомагане на координацията на органите за надзор на пазара на държавите членки.

3.2.4. Съвместимост с настоящата многогодишна финансова рамка

Предложението/инициативата:

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

Не се налага препрограмиране.

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

—

– ☐ налага преразглеждане на МФР.

—

3.2.5. Финансов принос от трети страни

Предложението/инициативата:

– × не предвижда съфинансиране от трети страни

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

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

	Година **N**[49]	Година **N+1**	Година **N+2**	Година **N+3**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)			Общо
Да се посочи съфинансиращият орган								
ОБЩО съфинансирани бюджетни кредити								

[49] Година N е годината, през която започва да се осъществява предложението/инициативата. Моля, заменете буквата N с очакваната първа година от изпълнението (например: 2021). Същото за следващите години.

3.3. Очаквано отражение върху приходите

– ☐ Предложението/инициативата няма финансово отражение върху приходите.

– ☐ Предложението/инициативата има следното финансово отражение:

  – ☐ върху собствените ресурси

  – ☐ върху другите приходи

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

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

Приходен бюджетен ред:	Налични бюджетни кредити за текущата финансова година	Отражение на предложението/инициативата[50]						
		Година **N**	Година **N+1**	Година **N+2**	Година **N+3**	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)		
Статия …….								

За целевите приходи да се посочат съответните разходни бюджетни редове.

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

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