ЕВРОПЕЙСКИ СЪЮЗ

ЕВРОПЕЙСКИ ПАРЛАМЕНТ **СЪВЕТ**

Брюксел, 25 септември 2024 г.
(OR. en)

2022/0272(COD) **PE-CONS 100/23**

CYBER 328
JAI 1731
DATAPROTECT 391
TELECOM 409
MI 1168
CSC 579
CSCI 215
CODEC 2601

ЗАКОНОДАТЕЛНИ АКТОВЕ И ДРУГИ ПРАВНИ ИНСТРУМЕНТИ

Относно:	РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на регламенти (ЕС) № 168/2013 и (ЕС) 2019/1020 и Директива (ЕС) 2020/1828 (Акт за киберустойчивост)

РЕГЛАМЕНТ (ЕС) 2024/...
НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

от ...

относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на регламенти (ЕС) № 168/2013 и (ЕС) 2019/1020 и Директива (ЕС) 2020/1828 (Акт за киберустойчивост)

(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],

след консултация с Комитета на регионите,

в съответствие с обикновената законодателна процедура[2],

---

1 ОВ C 100, 16.3.2023 г., стр. 101.

2 Позиция на Европейския парламент от 12 март 2024 г. (все още непубликувана в Официален вестник) и решение на Съвета от ...

като имат предвид, че:

(1) Киберсигурността е едно от ключовите предизвикателства за Съюза. Броят и многообразието на свързаните устройства ще нараства експоненциално през следващите години. Кибератаките представляват въпрос от обществен интерес, тъй като оказват решаващо въздействие не само върху икономиката на Съюза, но и върху демокрацията, както и върху безопасността на потребителите и здравето. Поради това е необходимо да се засили подходът на Съюза към киберсигурността, да се разгледа въпросът за киберустойчивостта на равнището на Съюза и да се подобри функционирането на вътрешния пазар, като се установи единна правна рамка за съществените изисквания за киберсигурност за пускането на продукти с цифрови елементи на пазара на Съюза. Следва да бъдат решени два основни проблема, които увеличават разходите за ползвателите и обществото: ниско ниво на киберсигурност на продуктите с цифрови елементи, което се изразява в широко разпространени уязвимости и недостатъчно и непоследователно предоставяне на актуализации за сигурност 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 сигурен начин.

(2) Настоящият регламент има за цел да определи граничните условия за разработването на сигурни 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, например чрез подобряване на прозрачността по отношение на периода на поддръжка за предоставяните на пазара продукти с цифрови елементи.

(3) Съответното право на Съюза, което е в сила, включва няколко набора от хоризонтални правила, които разглеждат определени аспекти, свързани с киберсигурността, от различни гледни точки, включително мерки за подобряване на сигурността на цифровата верига на доставките. Съществуващото право на Съюза, свързано с киберсигурността, включително Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета[3] и Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета[4], обаче не обхваща пряко задължителните изисквания за сигурността на продуктите с цифрови елементи.

---

[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] Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива за МИС 2) (ОВ L 333, 27.12.2022 г., стр. 80).

(4) Въпреки че съществуващото право 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 предприятията и организациите да спазват редица изисквания и задължения за подобни видове продукти. Киберсигурността на тези продукти има особено силно трансгранично измерение, тъй като продуктите с цифрови елементи, произведени в една държава членка или трета държава, често се използват от организации и потребители в целия вътрешен пазар. Именно това налага тази област да бъде регулирана на равнището на Съюза, за да се гарантира хармонизирана регулаторна рамка и правна сигурност за ползвателите, организациите и предприятията, включително микропредприятията и малките и средните предприятия съгласно определението за тях в приложението към Препоръка 2003/361/ЕО на Комисията[5]. Нормативната уредба на Съюза следва да бъде хармонизирана чрез въвеждане на хоризонтални изисквания за киберсигурност за продуктите с цифрови елементи. Също така в целия Съюз следва да се гарантира правна сигурност за икономическите оператори и ползвателите, както и по-добра хармонизация на вътрешния пазар и пропорционалност за микропредприятията и малките и средните предприятия, като се създадат по-жизнеспособни условия за икономическите оператори, които се стремят да навлязат на този пазар.

[5] Препоръка 2003/361/ЕО на Комисията от 6 май 2003 г. относно определението за микро-, малки и средни предприятия (ОВ L 124, 20.5.2003 г., стр. 36).

(5) По отношение на микропредприятията и малките и средните предприятия при определяне на категорията, в която попада дадено предприятие, разпоредбите на приложението към Препоръка 2003/361/ЕО на Комисията следва да се прилагат в тяхната цялост. Следователно при изчисляването на числеността на персонала и финансовите тавани за определяне на категориите предприятия следва също така да се прилагат разпоредбите на член 6 от приложението към Препоръка 2003/361/ЕО на Комисията относно установяването на данните за дадено предприятие, като се вземат предвид специфичните видове предприятия, като например предприятията партньори или свързаните предприятия.

(6) Комисията следва да предостави насоки с цел подпомагане на икономическите оператори, по-специално микропредприятията и малките и средните предприятия, при прилагането на настоящия регламент. Тези насоки следва да обхващат, наред с другото, приложното поле на настоящия регламент, по-специално обработването на данни от разстояние и последиците от него за разработчиците на свободен софтуер с отворен код, прилагането на критериите, използвани за определяне на периодите на поддръжка за продуктите с цифрови елементи, взаимодействието между настоящия регламент и друго право на Съюза и концепцията за съществено изменение.

(7) На равнището на Съюза в различни програмни и политически документи, като съвместното съобщение на Комисията и върховния представител на Съюза по въпросите на външните работи и политиката на сигурност от 16 декември 2020 г., озаглавено „Стратегия на ЕС за киберсигурност за цифровото десетилетие“, заключенията на Съвета от 2 декември 2020 г. относно киберсигурността на свързаните устройства и от 23 май 2022 г. относно установяването на позицията на Европейския съюз в киберпространството и резолюцията на Европейския парламент от 10 юни 2021 г. относно стратегията на ЕС за киберсигурност за цифровото десетилетие[6], се призовава за специфични изисквания на Съюза за киберсигурност за цифровите или свързаните продукти, като няколко трети държави въвеждат мерки за решаване на този въпрос по своя собствена инициатива. В заключителния доклад на Конференцията за бъдещето на Европа гражданите призоваха за „по-силна роля на ЕС в противодействието на киберзаплахите“. Важно е да се създаде амбициозна регулаторна рамка, за да може Съюзът да играе водеща международна роля в областта на киберсигурността.

(8) 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.

---

[6] ОВ C 67, 8.2.2022 г., стр. 81.

(9) 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 продукти с цифрови елементи са проектирани и разработени в съответствие със съществените изисквания за киберсигурност, определени в настоящия регламент. Това задължение се отнася както за продукти, които могат да бъдат свързани физически чрез хардуерни интерфейси, така и продукти, които са свързани логически, например чрез мрежови сокети, 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 продуктите с цифрови елементи, които са само непряко свързани с други устройства или мрежи.

(10) С определянето на изисквания за киберсигурност при пускането на пазара на продукти с цифрови елементи се цели да се повиши киберсигурността на тези продукти както за потребителите, така и за предприятията. Тези изисквания също така ще гарантират, че киберсигурността се взема предвид във всички вериги на доставки, като по този начин крайните продукти с цифрови елементи и техните компоненти ще станат по-сигурни. Това включва и изисквания за пускане на пазара на потребителски продукти с цифрови елементи, предназначени за уязвими потребители, като например играчки и системи за наблюдение на бебето. Потребителските продукти с цифрови елементи, категоризирани в настоящия регламент като важни продукти с цифрови елементи, представляват по-висок киберриск, тъй като изпълняват функция, носеща значителен риск от неблагоприятни последици поради своята интензивност и способност за причиняване на вреда на здравето, сигурността или безопасността на ползвателите на такива продукти, и следва да се подложат на по-строга процедура за оценяване на съответствието. Това се отнася за такива продукти като продуктите за дома с функционалности за сигурност, включително интелигентни ключалки за врати, системи за наблюдение на бебето и алармени системи, за свързаните играчки и личните устройства за прикрепване към тялото с цел събиране на данни за здравето. Освен това по-строгите процедури за оценяване на съответствието, на които се изисква да бъдат подложени другите продукти с цифрови елементи, категоризирани в настоящия регламент като важни или критични продукти с цифрови елементи, ще допринесат за предотвратяване на потенциалните отрицателни въздействия върху потребителите от използването на уязвимостите.

(11) Целта на настоящия регламент е да гарантира високо равнище на киберсигурност на продуктите с цифрови елементи и техните интегрирани решения за обработване на данни от разстояние. Такива решения за обработване на данни от разстояние следва да бъдат определени като обработване на данни от разстояние, за което софтуерът е проектиран и разработен от производителя на съответния продукт с цифрови елементи или от негово име и липсата на което би попречила на продукта с цифрови елементи да изпълнява някоя от функциите си. Този подход гарантира, че тези продукти са защитени по подходящ начин в тяхната цялост от техните производители, независимо дали данните се обработват или съхраняват локално на устройството на ползвателя или от разстояние от производителя. Същевременно обработването или съхранението от разстояние попада в обхвата на настоящия регламент само доколкото то е необходимо, за да може даден продукт с цифрови елементи да изпълнява своите функции. Такова обработване или съхранение от разстояние включва ситуацията, при която мобилно приложение изисква достъп до приложно-програмен интерфейс или до база данни, предоставяна чрез услуга, разработена от производителя. В такъв случай услугата попада в обхвата на настоящия регламент като решение за обработване на данни от разстояние. Следователно изискванията относно решенията за обработване на данни от разстояние, които попадат в обхвата на настоящия регламент, не включват технически, оперативни или организационни мерки, насочени към управление на рисковете за сигурността на мрежовите и информационните системи на производителя като цяло.

(12) Решенията в облак представляват решения за обработване на данни от разстояние по смисъла на настоящия регламент само ако отговарят на определението, установено в настоящия регламент. Например работещите в облак функции, предоставени от производител на интелигентни устройства за дома, които дават възможност на ползвателите да контролират устройството от разстояние, попадат в обхвата на настоящия регламент. От друга страна, уебсайтове, които не поддържат функционалността на продукт с цифрови елементи, или услуги в облак, проектирани и разработени така че да не попадат под отговорността на производител на продукт с цифрови елементи, не попадат в обхвата на настоящия регламент. Директива (ЕС) 2022/2555 се прилага за услугите в облак и моделите на услуги в облак, като например софтуер като услуга (SaaS), платформа като услуга (PaaS) или инфраструктура като услуга (IaaS). Субектите, предоставящи услуги в облак в Съюза, които се определят като средни предприятия съгласно член 2 от приложението към Препоръка 2003/361/ЕО на Комисията или надвишават праговете за средни предприятия, предвидени в параграф 1 от същия член, попадат в обхвата на посочената директива.

(13) В съответствие с целта на настоящия регламент да се премахнат пречките пред свободното движение на продукти с цифрови елементи, държавите членки следва да 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. Следователно по отношение на областите, хармонизирани с настоящия регламент, държавите членки не могат да налагат допълнителни изисквания за киберсигурност за предоставянето на пазара на продукти с цифрови елементи. Всеки публичен или частен субект обаче може да установи допълнителни изисквания към определените в настоящия регламент за възлагането на поръчки или използването на продукти с цифрови елементи за конкретните си цели и следователно може да избере да използва продукти с цифрови елементи, които отговарят на по-строги или по-специални изисквания за киберсигурност от приложимите за предоставянето на пазара съгласно настоящия регламент. Без да се засягат директиви 2014/24/ЕС[7] и 2014/25/ЕС[8] на Европейския парламент и на Съвета, при възлагането на обществени поръчки за продукти с цифрови елементи, които трябва да отговарят на съществените изисквания за киберсигурност, определени в настоящия регламент, включително свързаните с отстраняването на уязвимости, държавите членки следва да гарантират, че тези изисквания се вземат предвид в процеса на възлагане на обществени поръчки и че се взема предвид и способността на производителите ефективно да прилагат мерки за киберсигурност и да се справят с киберзаплахи.

---

7 Директива 2014/24/ЕС на Европейския парламент и на Съвета от 26 февруари 2014 г. за обществените поръчки и за отмяна на Директива 2004/18/ЕО (ОВ L 94, 28.3.2014 г., стр. 65).

8 Директива 2014/25/ЕС на Европейския парламент и на Съвета от 26 февруари 2014 г. относно възлагането на поръчки от възложители, извършващи дейност в секторите на водоснабдяването, енергетиката, транспорта и пощенските услуги и за отмяна на Директива 2004/17/ЕО (ОВ L 94, 28.3.2014 г., стр. 243).

Освен това в Директива (ЕС) 2022/2555 се определят мерки за управление на киберрисковете за съществените и важните субекти, посочени в член 3 от посочената директива, които биха могли да включват мерки за сигурност във веригата на доставки, които изискват такива субекти да използват продукти с цифрови елементи, отговарящи на по-строги изисквания за киберсигурност от определените в настоящия регламент. Поради това в съответствие с Директива (ЕС) 2022/2555 и с нейния принцип за минимална хармонизация държавите членки могат да налагат допълнителни изисквания за киберсигурност за използването на ИКТ продукти от съществени или важни субекти съгласно посочената директива, за да се гарантира по-високо ниво на киберсигурност, при условие че тези изисквания са в съответствие със задълженията на държавите членки, определени в правото на Съюза. Областите, които не са обхванати от настоящия регламент, могат да включват нетехнически фактори, свързани с продукти с цифрови елементи и техните производители. Следователно държавите членки могат да определят национални мерки, включително ограничения за продуктите с цифрови елементи или доставчиците на такива продукти, при които се вземат предвид нетехнически фактори. Националните мерки, свързани с такива фактори, се изисква да са в съответствие с правото на Съюза.

(14) Настоящият регламент следва да не засяга отговорността на държавите членки да предприемат мерки за защита на националната сигурност в съответствие с правото на Съюза. Държавите членки следва да могат да подлагат на допълнителни мерки продуктите с цифрови елементи, които се предоставят чрез обществени поръчки или използват за целите на националната сигурност или отбраната, при условие че тези мерки са в съответствие със задълженията на държавите членки, установени в правото на Съюза.

(15) Настоящият регламент се прилага за икономическите оператори само по отношение на продуктите с цифрови елементи, които са предоставени на пазара и следователно са доставени за разпространение или използване на пазара на Съюза в процеса на търговска дейност. Доставянето в процеса на търговска дейност може да се характеризира не само с начисляване на цена за продукт с цифрови елементи, но и с начисляване на цена за услуги по техническа поддръжка, когато това не служи само за възстановяване на действителните разходи, с намерение за извличане на печалба, например с предоставяне на софтуерна платформа, чрез която производителят печели от други услуги, изисквайки като условие за използване да се обработват лични данни по причини, различни от такива, свързани изключително с подобряване на сигурността, съвместимостта или оперативната съвместимост на софтуера, или приемайки дарения, надвишаващи разходите, свързани с проектирането, разработването и предоставянето на продукт с цифрови елементи. Приемането на дарения без намерение за извличане на печалба не следва да се счита за търговска дейност.

(16) Продуктите с цифрови елементи, предоставени като част от предоставянето на услуга, за която се начислява такса единствено за възстановяване на действителните разходи, пряко свързани с предоставянето на тази услуга, какъвто може да е случаят с определени продукти с цифрови елементи, предоставяни от органи на публичната администрация, не следва да се считат само на тези основания за търговска дейност за целите на настоящия регламент. Освен това продукти с цифрови елементи, които са разработени или изменени от орган на публичната администрация изключително за собствено ползване, не следва да се считат за предоставени на пазара по смисъла на настоящия регламент.

(17) Софтуерът и данните, които се споделят открито и до които ползвателите имат свободен достъп и свободно могат да използват, изменят и разпространяват същите или техни изменени версии, могат да допринесат за научните изследвания и иновациите на пазара. За да се насърчава разработването и внедряването на свободен софтуер с отворен код, по-специално от микропредприятия и малки и средни предприятия, включително стартиращи предприятия, физически лица, организации с нестопанска цел и академични научноизследователски организации, при прилагането на настоящия регламент за продукти с цифрови елементи, отговарящи на критериите за свободен софтуер с отворен код, доставени за разпространение или използване в процеса на търговска дейност, следва да се вземе предвид естеството на различните модели за разработване на софтуер, разпространяван и разработван с лицензи за свободен софтуер с отворен код.

(18) Под свободен софтуер с отворен код се разбира софтуер, чийто изходен код е открито споделян и чийто лиценз предоставя всички права, които го правят свободно достъпен, използваем, модифицируем и преразпределяем. Свободният софтуер с отворен код се разработва, поддържа и разпространява открито, включително чрез онлайн платформи. По отношение на икономическите оператори, които попадат в обхвата на настоящия регламент, само свободният софтуер с отворен код, който е предоставен на пазара и следователно е доставен за разпространение или използване в процеса на търговска дейност, следва да попада в обхвата на настоящия регламент. Следователно самите обстоятелства, при които е разработен продуктът с цифрови елементи, или начинът, по който е финансирано разработването, не следва да се вземат предвид при определяне на търговския или нетърговския характер на тази дейност. По-конкретно, за целите на настоящия регламент и по отношение на икономическите оператори, които попадат в неговия обхват, за да се гарантира, че е налице ясно разграничение между етапите на разработване и доставяне, предоставянето на продукти с цифрови елементи, квалифицирани като свободен софтуер с отворен код, от които техните производители извличат печалба, не следва да се счита за търговска дейност. Освен това доставянето на продукти с цифрови елементи, квалифицирани като компоненти на свободен софтуер с отворен код, предназначени за интегриране от други производители в техните собствени продукти с цифрови елементи, следва да се счита за предоставяне на пазара само ако първоначалният производител на компонента извлича печалба от него. Например самият факт, че продукт с цифрови елементи и със софтуер с отворен код получава финансова подкрепа от производителите или че производителите допринасят за разработването на такъв продукт, не следва сам по себе си да означава, че дейността има търговски характер.

Освен това самото наличие на редовни актуализации не следва само по себе си да води до заключението, че даден продукт с цифрови елементи е доставен в процеса на търговска дейност. И накрая, за целите на настоящия регламент разработването на продукти с цифрови елементи, отговарящи на критериите за свободен софтуер с отворен код, от организации с нестопанска цел не следва да се счита за търговска дейност, при условие че организацията е създадена по начин, който гарантира, че всички печалби след разходите се използват за постигането на нестопански цели. Настоящият регламент не се прилага за физически или юридически лица, които допринасят с изходен код за продукти с цифрови елементи, отговарящи на критериите за свободен софтуер с отворен код, които не са под тяхна отговорност.

(19) Като се има предвид значението за киберсигурността на много продукти с цифрови елементи, отговарящи на критериите за свободен софтуер с отворен код, които се публикуват, но не се предоставят на пазара по смисъла на настоящия регламент, юридическите лица, които предоставят устойчива подкрепа за разработването на такива продукти, предназначени за търговски дейности, и които играят основна роля за гарантиране на жизнеспособността на тези продукти (попечители на софтуер с отворен код), следва да подлежат на облекчен и индивидуализиран регулаторен режим. Попечителите на софтуер с отворен код включват определени фондации, както и субекти, които разработват и публикуват свободен софтуер с отворен код в бизнес контекст, включително образувания с нестопанска цел. Регулаторният режим следва да отчита техния специфичен характер и съвместимост с вида на наложените задължения. Той следва да обхваща само продукти с цифрови елементи, отговарящи на критериите за свободен софтуер с отворен код, които в крайна сметка са предназначени за търговски дейности, като например интегриране в търговски услуги или в продукти с цифрови елементи, от които се извлича печалба. За целите на посочения регулаторен режим намерението за интегриране в продукти с цифрови елементи, от които се извлича печалба, включва случаи, в които производителите, които интегрират компонент в своите собствени продукти с цифрови елементи, допринасят за разработването на този компонент по редовен начин или предоставят редовна финансова помощ, за да се гарантира непрекъснатостта на даден софтуерен продукт. Предоставянето на устойчива подкрепа за разработването на продукт с цифрови елементи включва, но не се ограничава до хостинг и управление на платформи за сътрудничество при разработването на софтуер, хостинг на изходен код или софтуер, администриране или управление на продукти с цифрови елементи, квалифицирани като свободен софтуер с отворен код, както и направляване на разработването на такива продукти. Като се има предвид, че облекченият и индивидуализиран регулаторен режим не подлага лицата, действащи като попечители на софтуер с отворен код, на същите задължения като лицата, осъществяващи дейност като производители съгласно настоящия регламент, те не следва да имат право да нанасят маркировката „CE“ върху продуктите с цифрови елементи, за чието разработване предоставят подкрепа.

(20) Хостингът на продукти с цифрови елементи в хранилища със свободен достъп, включително чрез системи за управление на софтуерни пакети или на платформи за сътрудничество, сам по себе си не представлява предоставяне на пазара на продукт с цифрови елементи. Доставчиците на такива услуги следва да се считат за дистрибутори само ако предоставят такъв софтуер на пазара и следователно го доставят за разпространение или използване на пазара на Съюза в процеса на търговска дейност.

(21) За да се подкрепи и улесни полагането на дължима грижа от страна на производителите, които интегрират в своите продукти с цифрови елементи компоненти на свободен софтуер с отворен код, които не са предмет на съществените изисквания за киберсигурност, определени в настоящия регламент, Комисията следва да може да създава доброволни програми за удостоверяване на сигурността чрез делегиран акт за допълване на настоящия регламент или чрез искане за европейска схема за сертифициране на киберсигурността съгласно член 48 от Регламент (ЕС) 2019/881, която взема предвид особеностите на моделите за разработване на свободен софтуер с отворен код. Програмите за удостоверяване на сигурността следва да бъдат замислени по такъв начин, че не само физическите или юридическите лица, разработващи или допринасящи за разработването на продукт с цифрови елементи, отговарящи на критериите за свободен софтуер с отворен код, да могат да инициират или финансират удостоверяване на сигурността, но и трети страни, като например производителите, които интегрират такива продукти в своите собствени продукти с цифрови елементи, ползвателите или публичните администрации на Съюза и националните публични администрации.

(22) С оглед на целите на настоящия регламент в областта на обществената киберсигурност и за да се подобри ситуационната осведоменост на държавите членки по отношение на зависимостта на Съюза от софтуерни компоненти, и по-специално от компоненти на потенциално свободен софтуер с отворен код, създадената с настоящия регламент специализирана група за административно сътрудничество (ADCO група) следва да може да реши да извърши съвместно оценка на зависимостта на Съюза. Органите за надзор на пазара следва да могат да изискват от производителите на установените от ADCO групата категории продукти с цифрови елементи да представят описи на софтуерните компоненти, които са създали съгласно настоящия регламент. За да се защити поверителността на описите на софтуерните компоненти, органите за надзор на пазара следва да предоставят на ADCO групата съответната информация за зависимостите по анонимен и обобщен начин.

(23) Ефективността на прилагането на настоящия регламент ще зависи и от наличието на достатъчно умения в областта на киберсигурността. На равнището на Съюза в различни програмни и политически документи, включително съобщението на Комисията от 18 април 2023 г. относно преодоляването на недостига на таланти в областта на киберсигурността за повишаване на конкурентоспособността, растежа и устойчивостта на ЕС и заключенията на Съвета от 22 май 2023 г. относно политиката на ЕС за киберотбрана, се признава недостигът на умения в областта на киберсигурността в Съюза и необходимостта тези предизвикателства да бъдат разгледани приоритетно както в публичния, така и в частния сектор. За да се гарантира ефективното прилагане на настоящия регламент, държавите членки следва да гарантират наличието на достатъчно ресурси за обезпечаване с подходящ персонал на органите за надзор на пазара и на органите за оценяване на съответствието, така че да могат да изпълняват задачите си, както са определени в настоящия регламент. Тези мерки следва да подобрят мобилността на работната сила в областта на киберсигурността и свързаните с нея кариери. Те следва също така да допринасят за повишаване на устойчивостта и приобщаващия характер на работната сила в областта на киберсигурността, включително по отношение на пола. Поради това държавите членки следва да предприемат мерки, за да гарантират, че тези задачи се изпълняват от подходящо обучени специалисти с необходимите умения в областта на киберсигурността. По същия начин производителите следва да гарантират, че техният персонал притежава необходимите умения, за да изпълнява задълженията си, както са определени в настоящия регламент. Държавите членки и Комисията, в съответствие със своите прерогативи и компетентности и специфичните задачи, които са им възложени с настоящия регламент, следва да предприемат мерки в подкрепа на производителите, и по-специално микропредприятията и малките и средните предприятия, включително стартиращите предприятия, и в области като развитието на умения, за да спазят задълженията си, определени в настоящия регламент. Освен това, тъй като Директива (ЕС) 2022/2555 изисква от държавите членки да приемат в рамките на своите национални стратегии за киберсигурност политики за насърчаване и развиване на обучение и умения в областта на киберсигурността, при приемането на такива стратегии държавите членки могат да обмислят също така дали да разгледат и потребностите от умения в областта на киберсигурността, произтичащи от настоящия регламент, включително потребностите, свързани с преквалификация и повишаване на квалификацията.

(24) Сигурният интернет е незаменим за функционирането на критичните инфраструктури и за обществото като цяло. Директива (ЕС) 2022/2555 има за цел да осигури високо ниво на киберсигурност на услугите, предоставяни от съществени и важни субекти, както са посочени в член 3 от посочената директива, включително доставчици на цифрова инфраструктура, които поддържат основните функции на отворения интернет, осигуряват достъп до интернет и предоставят 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 (ЕС) 2022/2555, 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 за сигурност на тези продукти.

(25) В Регламент (ЕС) 2017/745 на Европейския парламент и на Съвета[9] са определени правилата за медицинските изделия, а в Регламент (ЕС) 2017/746 на Европейския парламент и на Съвета[10] са определени правилата за медицинските изделия за инвитро диагностика. В посочените регламенти 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 видове невграден софтуер и подходът на целия жизнен цикъл също са обхванати от посочените 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, установени в приложение I към посочените регламенти по отношение на киберсигурността. Поради това продуктите с цифрови елементи, за които се прилага някой от посочените регламенти, следва да не бъдат предмет на настоящия регламент.

---

9 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).

10 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).

(26) Продуктите с цифрови елементи, които са разработени или изменени изключително за целите на националната сигурност или отбраната, или продуктите, специално предназначени за обработване на класифицирана информация, попадат извън обхвата на настоящия регламент. Държавите членки се насърчават да осигурят за тези продукти същото ниво на защита, каквото се осигурява за продуктите, попадащи в обхвата на настоящия регламент, или дори по-високо ниво.

(27) С Регламент (ЕС) 2019/2144 на Европейския парламент и на Съвета[11] 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 относно 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, и по-специално Правило № 155 на ООН – Единни предписания за одобрение на превозни средства по отношение на киберсигурността и системата за управление на киберсигурността, и се предвиждат специфични процедури за оценяване на съответствието.

---

[11] 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).

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 и оборудване, включително софтуер, която включва задълженията за защита срещу заплахи за информационната сигурност. Процесът на сертифициране съгласно Регламент (ЕС) 2018/1139 гарантира нивото на увереност, което се цели с настоящия регламент. Поради това продуктите с цифрови елементи, за които се прилага Регламент (ЕС) 2019/2144, и продуктите, сертифицирани в съответствие с Регламент (ЕС) 2018/1139, следва да не бъдат предмет на съществените изисквания за киберсигурност и процедурите за оценяване на съответствието, определени в настоящия регламент.

[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).

(28) С настоящия регламент се установяват хоризонтални правила за киберсигурност, които не са специфични за отделни сектори или за 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 за киберсигурност, определени 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 някои от рисковете, обхванати от съществените изисквания за киберсигурност, посочени в 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 поне същото ниво на защита като предвиденото в настоящия регламент. Комисията следва да бъде оправомощена да приема делегирани актове за допълване на настоящия регламент чрез определяне на такива продукти и правила. По отношение на съществуващото право на Съюза, за което следва да се прилага такова ограничение или изключение, настоящият регламент съдържа специални разпоредби, за да се изясни връзката му с това право на Съюза.

(29) За да се гарантира, че предоставяните на пазара продукти с цифрови елементи могат да бъдат ефективно ремонтирани и че тяхната трайност може да бъде удължавана, следва да се предвиди освобождаване за резервните части. Това освобождаване следва да обхваща както резервните части за ремонт на заварени модели продукти, предоставени преди датата на прилагане на настоящия регламент, така и за резервните части, които вече са преминали процедура за оценяване на съответствието съгласно настоящия регламент.

(30) В Делегиран регламент (ЕС) 2022/30 на Комисията[13] се уточнява, че редица от съществените изисквания, определени в член 3, параграф 3, букви г), д) и е) от Директива 2014/53/ЕС на Европейския парламент и на Съвета[14], свързани с вредите за мрежата и неправилното използване на мрежови ресурси, личните данни и неприкосновеността на личния живот и измамите, се прилагат за определени радиосъоръжения. В Решение за изпълнение C(2022)5637 на Комисията от 5 август 2022 г. относно искане за стандартизация до Европейския комитет за стандартизация и Европейския комитет за стандартизация в електротехниката, се определят изисквания за разработване на специфични стандарти, в които допълнително се уточнява как следва да се отговори на тези съществени изисквания. Съществените изисквания за киберсигурност, определени в 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 за киберсигурност, определени в настоящия регламент, са съгласувани с целите на изискванията за специфични стандарти, включени в посоченото искане за стандартизация. Поради това, когато 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. По време на преходния период за прилагането на настоящия регламент Комисията следва да предостави насоки на попадащите в обхвата на настоящия регламент производители, за които се прилага и Делегиран регламент (ЕС) 2022/30, с цел улесняване на доказването на съответствие с двата регламента.

---

13 Делегиран регламент (ЕС) 2022/30 на Комисията от 29 октомври 2021 г. за допълнение на Директива 2014/53/ЕС на Европейския парламент и на Съвета по отношение на прилагането на съществените изисквания, посочени в член 3, параграф 3, букви г), д) и е) от същата директива (ОВ L 7, 12.1.2022 г., стр. 6).

14 Директива 2014/53/ЕС на Европейския парламент и на Съвета от 16 април 2014 г. за хармонизирането на законодателствата на държавите членки във връзка с предоставянето на пазара на радиосъоръжения и за отмяна на Директива 1999/5/ЕО (ОВ L 153, 22.5.2014 г., стр. 62).

(31) Директива (ЕС) 2024/... на Европейския парламент и на Съвета[15+] допълва настоящия регламент. В посочената 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 недостатъчната безопасност на неговия продукт, независимо от вината („обективна отговорност“). Когато тази недостатъчна безопасност представлява липсата на актуализации за сигурност 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 за сигурност, следва да бъдат определени в настоящия регламент.

---

15 Директива (ЕС) 2024/... на Европейския парламент и на Съвета от ... относно ... (ОВ L, ..., ELI: ...).

\+ ОВ: Моля, въведете в текста номера на директивата, съдържаща се в документ (2022/0302(COD), и добавете в бележката под линия номера, датата, заглавието и данните за публикуването в ОВ на тази директива.

(32) Настоящият регламент не следва да засяга Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета[16], включително разпоредбите, свързани със създаването 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, 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, осъществяващи надзор за прилагането 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.

[16] 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).

(33) Доколкото техните продукти попадат в обхвата на настоящия регламент, доставчиците на европейски портфейли за цифрова самоличност, съгласно посоченото в член 5а, параграф 2 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета[17], следва да отговарят както на хоризонталните съществени изисквания за киберсигурност, определени в настоящия регламент, така и на специфичните изисквания за сигурност, определени в член 5а от Регламент (ЕС) № 910/2014. За да се улесни спазването на изискванията, доставчиците на портфейли следва да могат да докажат съответствието на европейските портфейли за цифрова самоличност с изискванията, определени съответно в настоящия регламент и в Регламент (ЕС) № 910/2014, като сертифицират своите продукти по европейска схема за сертифициране на киберсигурността, създадена съгласно Регламент (ЕС) 2019/881 и за която Комисията е определила чрез делегирани актове презумпция за съответствие с настоящия регламент, доколкото сертификатът или части от него покриват тези изисквания.

[17] Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ L 257, 28.8.2014 г., стр. 73).

(34) Когато интегрират компоненти, доставени от трети страни, в продукти с цифрови елементи по време на етапите на проектиране и разработване, за да гарантират, че продуктите са проектирани, разработени и произведени в съответствие със съществените изисквания за киберсигурност, определени в настоящия регламент, производителите следва да полагат дължимата грижа по отношение на тези компоненти, включително компонентите на свободен софтуер с отворен код, които не са били предоставени на пазара. Подходящото равнище на дължима грижа зависи от естеството и нивото на киберриска, свързан с даден компонент, и за тази цел следва да взема предвид едно или повече от следните действия: проверка, според случая, дали производителят на компонент е доказал съответствие с настоящия регламент, включително чрез проверка дали компонентът вече носи маркировката „CE“; проверка дали даден компонент получава редовни актуализации за сигурност, например чрез проверка на предходните актуализации за сигурност; проверка дали даден компонент няма уязвимости, регистрирани в европейската база данни за уязвимости, създадена съгласно член 12, параграф 2 от Директива (ЕС) 2022/2555, или в други публично достъпни бази данни за уязвимости; или извършване на допълнителни изпитвания във връзка със защитата. Задълженията за отстраняване на уязвимостите, определени в настоящия регламент, които производителите трябва да спазват при пускането на продукт с цифрови елементи на пазара и за периода на поддръжка, се прилагат за продуктите с цифрови елементи в тяхната цялост, включително за всички интегрирани компоненти. Когато при полагането на дължима грижа производителят на продукта с цифрови елементи установи уязвимост в даден компонент, включително в свободен компонент с отворен код, той следва да информира лицето или субекта, който произвежда или поддържа компонента, да предприеме мерки и да отстрани уязвимостта, а когато е приложимо, да предостави на лицето или субекта приложените корекции по отношение на защитата.

(35) Непосредствено след преходния период за прилагането на настоящия регламент производител на продукт с цифрови елементи, който интегрира един или няколко компонента, доставени от трети страни, които също са предмет на настоящия регламент, може да не е в състояние да провери като част от задължението си за дължима грижа дали производителите на тези компоненти са доказали съответствие с настоящия регламент, например чрез проверка дали компонентите вече носят маркировката „CE“. Такъв може да бъде случаят, когато компонентите са били интегрирани преди настоящият регламент да стане приложим за производителите на тези компоненти. В такъв случай производителят, който интегрира такива компоненти, следва да полага дължима грижа чрез други средства.

(36) Продуктите с цифрови елементи следва да носят маркировката „CE“, указваща по видим, четлив и незаличим начин тяхното съответствие с настоящия регламент с цел свободно движение в рамките на вътрешния пазар. Държавите членки следва да не създават необосновани пречки пред пускането на пазара на продукти с цифрови елементи, които съответстват на изискванията, предвидени в настоящия регламент, и носят маркировката „CE“. Освен това по време на търговски панаири, изложения, демонстрации или други подобни събития държавите членки следва да не възпрепятстват представянето или използването на даден продукт с цифрови елементи, който не отговаря на изискванията на настоящия регламент, включително негови прототипи, при условие че продуктът се представя с видим знак, който ясно показва, че продуктът не съответства на настоящия регламент и няма да се предоставя на пазара, докато не бъде приведен в такова съответствие.

(37) За да се гарантира, че производителите могат да пускат софтуер за целите на изпитването, преди да подложат своите продукти с цифрови елементи на оценяване на съответствието, държавите членки следва да не възпрепятстват предоставянето на незавършен софтуер, като например алфа версии, бета версии или кандидати за пускане на пазара, при условие че незавършеният софтуер се предоставя само за времето, необходимо за неговото 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, установени в 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.

(38) 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 киберсигурност за такива продукти. Тези съществени изисквания за киберсигурност, включително изискванията за управление на уязвимостите, се прилагат за всеки отделен продукт с цифрови елементи, когато се пуска на пазара, независимо дали продуктът с цифрови елементи е произведен като отделна единица или серийно. Когато става въпрос за даден вид продукти например, всеки отделен продукт с цифрови елементи, който се пуска на пазара, следва да е преминал през всички налични софтуерни поправки или актуализации на защитата, за да се преодолеят съответните проблеми със сигурността. Когато продуктите с цифрови елементи впоследствие бъдат изменени с физически или цифрови средства по начин, който не е предвиден от производителя в първоначалната оценка на риска, и това може да означава, че те вече не отговарят на съответните съществени изисквания за киберсигурност, изменението следва да се смята за съществено. Например ремонтите биха могли да бъдат приравнени към операциите по поддръжка, при условие че те не променят вече пуснатия на пазара продукт с цифрови елементи по начин, по който може да бъде засегнато съответствието с приложимите изисквания или да бъде променено предназначението, за което продуктът е бил оценен.

(39) 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 предназначението на този продукт и тези промени не са били предвидени от производителя в първоначалната оценка на риска или когато естеството на опасността се е променило или нивото на киберриска се е увеличило поради актуализацията на софтуера и актуализираната версия на продукта е предоставена на пазара. Когато актуализация за сигурност, която е предназначена да намали нивото на киберриска на даден продукт с цифрови елементи, не променя предназначението на продукт с цифрови елементи, тя не се счита за съществено изменение. Това обикновено включва ситуации, при които актуализация за сигурност води само до незначителни корекции на изходния код. Такъв може да бъде случаят например, когато актуализацията за сигурност е насочена към уязвимост, която е известна, включително чрез промяна на функциите или показателите на продукт с цифрови елементи единствено с цел намаляване на нивото на киберриска. По подобен начин незначителна актуализация на функционалните възможности, като например визуално подобрение или добавяне на нови пиктограми или езици към потребителския интерфейс, по принцип не следва да се счита за съществено изменение. Обратно, когато актуализация на характеристиките променя първоначално предвидените функции или типа или показателите на даден продукт с цифрови елементи и отговаря на горепосочените критерии, тя следва да се счита за съществено изменение, тъй като добавянето на нови характеристики обикновено води до увеличаване на повърхността, уязвима за атаки, и по този начин засилва киберрриска. Такъв може да бъде случаят например, когато към дадено приложение се добавя нов входящ елемент, което налага производителят да осигури подходящо валидиране на входящите данни. Когато се преценява дали дадена актуализация на характеристиките се счита за съществено изменение, не е от значение дали тя се предоставя като отделна актуализация или в комбинация с актуализация за сигурност. Комисията следва да издаде насоки за това как да се определи какво съставлява съществено изменение.

(40) Като се има предвид повторяемият характер на разработването на софтуер, производителите, които са пуснали на пазара последващи версии на софтуерен продукт в резултат на последващо съществено изменение на този продукт, следва да могат да предоставят актуализации за сигурност за периода на поддръжка само за последната версия на софтуерния продукт, която са пуснали на пазара. Те следва да могат да правят това само ако ползвателите на съответните предишни версии на продукта имат безплатен достъп до версията на продукта, която последно е пусната на пазара, и не се налага да правят допълнителни разходи за адаптиране на хардуерната или софтуерната среда, в която използват продукта. Такъв например би могъл да бъде случаят, когато модернизирането на настолната операционна система не изисква нов хардуер като по-бърз централен процесор или по-голяма памет. Въпреки това производителят следва да продължи да спазва през периода на поддръжка други изисквания за отстраняване на уязвимости, като например трябва да има политика за координирано оповестяване на уязвимости или установени мерки за улесняване на обмена на информация за потенциални уязвимости за всички последващи съществено изменени версии на софтуерния продукт, пуснат на пазара. Производителите следва да могат да предоставят незначителни актуализации на защитата или на функционалните възможности, които не представляват съществено изменение, само за последната версия или подверсия на софтуерен продукт, който не е бил съществено изменен. Същевременно, когато хардуерен продукт като смартфон не е съвместим с последната версия на операционната система, с която първоначално е бил доставен, производителят следва да продължи да предоставя актуализации за сигурност поне за последната съвместима версия на операционната система през периода на поддръжка.

(41) В съответствие с общоприетата концепция 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 цифрови елементи с настоящия регламент, или когато се промени предназначението на този продукт, е целесъобразно да се провери съответствието на продукта с цифрови 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, третата страна следва да бъде уведомявана за промените, които могат да доведат до съществени изменения.

(42) Когато продукт с цифрови елементи се подлага на „обновяване“, „поддръжка“ и „ремонт“, както са определени в член 2, точки 18, 19 и 20 от Регламент (ЕС) 2024/1781 на Европейския парламент и на Съвета[18], това не води непременно до съществено изменение на продукта, например ако предназначението и функционалните възможности не се променят и нивото на риска остава същото. Осъвременяването на продукт с цифрови елементи от страна на производителя обаче може да доведе до промени в проектирането и разработването на продукта и следователно може да повлияе на неговото предназначение и съответствие с определените в настоящия регламент изисквания.

---

[18] Регламент (ЕС) 2024/1781 на Европейския парламент и на Съвета от 13 юни 2024 г. за създаване на рамка за определяне на изискванията за екопроектиране за устойчиви продукти, за изменение на Директива (ЕС) 2020/1828 и Регламент (ЕС) 2023/1542 и за отмяна на Директива 2009/125/ЕО (ОВ L, 2024/1781, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

(43) Продуктите с цифрови елементи следва да се считат за важни, ако отрицателното въздействие от използването на потенциални уязвимости на продукта може да бъде сериозно поради, наред с другото, функционалните възможности, свързани с киберсигурността, или функция, носеща значителен риск от неблагоприятни последици поради своята интензивност и способност за нарушаване, контрол или причиняване на вреди на голям брой други продукти с цифрови елементи или на здравето, сигурността или безопасността на ползвателите чрез пряко манипулиране, като например функция на централна система, включително управление на мрежата, контрол на конфигурацията, виртуализация или обработка на лични данни. По-специално, уязвимостите в продуктите с цифрови елементи, които имат свързани с киберсигурността функционални възможности, като например мениджъри за зареждане, могат да доведат до разпространение на проблеми със сигурността по цялата верига на доставките. Сериозността на въздействието на даден инцидент може да се увеличи и когато продуктът изпълнява предимно функция на централна система, включително управление на мрежата, контрол на конфигурацията, виртуализация или обработване на лични данни.

(44) Някои категории продукти с цифрови елементи следва да подлежат на по-строги процедури за оценяване на съответствието, като се запази пропорционален подход. За тази цел важните продукти с цифрови елементи следва да бъдат разделени на два класа, които отразяват нивото на киберриска, свързан с тези категории продукти. Инцидент, свързан с важни продукти с цифрови елементи от клас II, може да доведе до по-големи отрицателни въздействия, отколкото инцидент, свързан с важни продукти с цифрови елементи от клас I, например поради естеството на тяхната функция, свързана с киберсигурността, или изпълнението на друга функция, която носи значителен риск от неблагоприятни последици. За да се указва, че са възможни такива по-големи отрицателни въздействия, продуктите с цифрови елементи от клас II биха могли или да имат функционални възможности, свързани с киберсигурността, или да изпълняват друга функция, която носи значителен риск от неблагоприятни последици, който е по-висок, отколкото за продуктите, изброени в клас I, или да отговарят и на двата горепосочени критерия. Поради това важните продукти с цифрови елементи от клас II следва да подлежат на по-строга процедура за оценяване на съответствието.

(45) Важните продукти с цифрови елементи, посочени в настоящия регламент, следва да се разбират като продукти, които имат основните функционални възможности на категория важни продукти с цифрови елементи, посочена в настоящия регламент. Например в настоящия регламент се посочват категории важни продукти с цифрови елементи, които по своите функционални възможности се определят като защитни стени или системи за установяване или предотвратяване на проникване от клас II. В резултат на това защитните стени или системите за установяване или предотвратяване на проникване подлежат на задължително оценяване на съответствието от трета страна. Това не се отнася за други продукти с цифрови елементи, които не са категоризирани като важни продукти с цифрови елементи, които могат да включват защитни стени или системи за откриване или предотвратяване на проникване. Комисията следва да приеме акт за изпълнение, за да уточни техническото описание на категориите важни продукти с цифрови елементи, които попадат в клас I и в клас II, както е посочено в настоящия регламент.

(46) Категориите критични продукти с цифрови елементи, посочени в настоящия регламент, имат функционални възможности, свързани с киберсигурността, и изпълняват функция, носеща значителен риск от неблагоприятни последици, поради своята интензивност и способност за нарушаване, контрол или причиняване на вреди на голям брой други продукти с цифрови елементи чрез пряко манипулиране. Освен това тези категории продукти с цифрови елементи се считат за критични зависимости за съществените субекти, посочени в член 3, параграф 1 от Директива (ЕС) 2022/2555. Категориите критични продукти с цифрови елементи, посочени в приложение към настоящия регламент, вече широко използват поради критичното си естество различни форми на сертифициране и също така са обхванати от европейската схема за сертифициране на киберсигурността, основана на общи критерии (ЕССК), установена с Регламент за изпълнение (ЕС) 2024/482 на Комисията[19]. Поради това, за да се гарантира обща адекватна защита на киберсигурността на критичните продукти с цифрови елементи в Съюза, би било целесъобразно и пропорционално тези категории продукти да подлежат, посредством делегиран акт, на задължително европейско сертифициране на киберсигурността, когато съответната европейска схема за сертифициране на киберсигурността, обхващаща тези продукти, вече е въведена и Комисията е извършила оценка на потенциалното въздействие на предвиденото задължително сертифициране върху пазара. При тази оценка следва да се вземат предвид както предлагането, така и търсенето, включително дали е налице достатъчно търсене на съответните продукти с цифрови елементи от държавите членки и от ползвателите, за да се изисква европейско сертифициране на киберсигурността, както и целите, за които е предвидено да се използват продуктите с цифрови елементи, включително критичните зависимости от тях на съществени субекти, както са посочени в член 3, параграф 1 от Директива (ЕС) 2022/2555. В оценката следва също така да се анализират потенциалните последици от задължителното сертифициране върху наличността на тези продукти на вътрешния пазар, както и капацитетът и готовността на държавите членки за прилагането на съответните европейски схеми за сертифициране на киберсигурността.

---

[19] Регламент за изпълнение (ЕС) 2024/482 на Комисията от 31 януари 2024 г. за определяне на правила за прилагането на Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета по отношение на приемането на европейската схема за сертифициране на киберсигурността, основана на общи критерии (ЕССК) (ОВ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(47) В делегираните актове, които изискват задължително европейско сертифициране на киберсигурността, следва да се определят продуктите с цифрови елементи, които имат основните функционални възможности на категория критични продукти с цифрови елементи, посочена в настоящия регламент, и които трябва да бъдат предмет на задължително сертифициране, както и изискваното ниво на увереност, което следва да бъде поне „съществено“. Изискваното ниво на увереност следва да бъде пропорционално на нивото на киберриска, свързан с продукта с цифрови елементи. Например, когато продуктът с цифрови елементи има основните функционални възможности на категория критични продукти с цифрови елементи, посочена в настоящия регламент, и е предназначен за употреба в чувствителна или критична среда, като например продукти, предназначени за използване от съществените субекти, посочени в член 3, параграф 1 от Директива (ЕС) 2022/2555, за него може да се изисква най-високо ниво на увереност.

(48) За да се гарантира в Съюза обща адекватна защита на киберсигурността на продуктите с цифрови елементи, които имат основните функционални възможности на категория критични продукти с цифрови елементи, определена в настоящия регламент, Комисията следва също така да бъде оправомощена да приема делегирани актове за изменение на настоящия регламент чрез добавяне или оттегляне на категории критични продукти с цифрови елементи, за които производителите да трябва да получат европейски сертификат за киберсигурност в рамките на европейска схема за сертифициране на киберсигурността съгласно Регламент (ЕС) 2019/881, за да докажат съответствие с настоящия регламент. Към тези категории може да бъде добавена нова категория критични продукти с цифрови елементи, ако е налице критична зависимост от тях на съществени субекти, както са посочени в член 3, параграф 1 от Директива (ЕС) 2022/2555, или когато тези продукти са засегнати от инциденти или съдържат използвани уязвимости и това би могло да доведе до смущения на критичните вериги на доставки. Когато оценява необходимостта от добавяне или оттегляне на категории критични продукти с цифрови елементи чрез делегиран акт, Комисията следва да може да вземе предвид дали държавите членки са установили на национално равнище продукти с цифрови елементи, които имат критично важна роля за устойчивостта на съществените субекти, както са посочени в член 3, параграф 1 от Директива (ЕС) 2022/2555, и които все по-често са изложени на кибератаки по веригата на доставки с потенциални сериозни неблагоприятни последици. Освен това Комисията следва да може да вземе предвид резултатите от координираната на равнището на Съюза оценка на риска за критичните вериги на доставки, извършена в съответствие с член 22 от Директива (ЕС) 2022/2555.

(49) Комисията следва да гарантира, че при подготовката на мерките за прилагане на настоящия регламент се провеждат структурирани и редовни консултации с широк кръг заинтересовани страни. Такъв следва да бъде по-специално случаят, когато Комисията прави оценка дали е необходимо евентуално да се актуализират списъците на категориите важни или критични продукти с цифрови елементи; тогава следва да се направят консултации със съответните производители и техните становища следва да бъдат взети предвид, за да се анализират киберрисковете, както и балансът на разходите и ползите от определянето на такива категории продукти като важни или критични.

(50) В настоящия регламент са целенасочено разгледани киберрисковете. Продуктите с цифрови елементи обаче могат да създават и други рискове за безопасността, които не винаги са свързани с киберсигурността, но могат да бъдат следствие от нарушение на сигурността. Тези рискове следва да продължат да се регулират от съответното законодателство на Съюза за хармонизация, различно от настоящия регламент. Ако не е приложимо законодателство на Съюза за хармонизация, различно от настоящия регламент, спрямо тях следва да се прилага Регламент (ЕС) 2023/988 на Европейския парламент и на Съвета[20]. Поради това, с оглед на целевия характер на настоящия регламент, като изключение от член 2, параграф 1, трета алинея, буква б) от Регламент (ЕС) 2023/988, глава III, раздел 1, глави V и VII и глави IX—XI от Регламент (ЕС) 2023/988 следва да се прилагат за продукти с цифрови елементи по отношение на рисковете за сигурността, които не са обхванати от настоящия регламент, ако тези продукти не са предмет на специфични изисквания, наложени от законодателство на Съюза за хармонизация, различно от настоящия регламент, по смисъла на член 3, точка 27 от Регламент (ЕС) 2023/988.

---

[20] Регламент (ЕС) 2023/988 на Европейския парламент и на Съвета от 10 май 2023 г. относно общата безопасност на продуктите, за изменение на Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета и на Директива (ЕС) 2020/1828 на Европейския парламент и на Съвета и за отмяна на Директива 2001/95/ЕО на Европейския парламент и на Съвета и на Директива 87/357/ЕИО на Съвета (ОВ L 135, 23.5.2023 г., стр. 1).

(51) Продуктите с цифрови елементи, класифицирани като високорискови системи с ИИ съгласно член 6 от Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета[21], които попадат в обхвата на настоящия регламент, следва да отговарят на съществените изисквания за киберсигурност, определени в настоящия регламент. Когато тези високорискови системи с ИИ отговарят на съществените изисквания за киберсигурност, определени в настоящия регламент, те следва да се считат за съответстващи на изискванията за киберсигурност, определени в член 15 от Регламент (ЕС) 2024/..., доколкото тези изисквания са обхванати от ЕС декларацията за съответствие, издадена съгласно настоящия регламент, или от части от нея. За тази цел оценката на киберрисковете, свързани с продукт с цифрови елементи, класифицирани като високорискови системи с ИИ съгласно Регламент (ЕС) 2024/1689, които трябва да бъдат взети предвид на етапите на планиране, проектиране, разработване, производство, доставка и поддръжка на такъв продукт, както се изисква съгласно настоящия регламент, следва да отчита рисковете за киберустойчивостта на дадена система с ИИ по отношение на опити на неоправомощени трети лица да променят нейното използване, поведение или ефективност, включително специфични уязвимости на ИИ, като например заразяване на данни или враждебни атаки, както и по целесъобразност рисковете за основните права, в съответствие с Регламент (ЕС) 2024/1689. По отношение на процедурите за оценяване на съответствието, свързани със съществените изисквания за киберсигурност за даден продукт с цифрови елементи, който попада в обхвата на настоящия регламент и е класифициран като високорискова система с ИИ, по правило следва да се прилага член 43 от Регламент (ЕС) 2024/1689 вместо съответните разпоредби на настоящия регламент.

---

[21] Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 г. за установяване на хармонизирани правила относно изкуствения интелект и за изменение на регламенти (ЕО) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и директиви 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828 (Акт за изкуствения интелект) (ОВ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

Това правило обаче следва да не води до намаляване на необходимото ниво на увереност за важните или критичните продукти с цифрови елементи, посочени в настоящия регламент. Поради това, като изключение от това правило, за високорисковите системи с ИИ, които попадат в обхвата на Регламент (ЕС) 2024/1689 и са определени също като важни или критични продукти с цифрови елементи, посочени в настоящия регламент, и за които се прилага процедурата за оценяване на съответствието въз основа на вътрешен контрол, посочена в приложение VI към Регламент (ЕС) 2024/1689, следва да се прилагат процедурите за оценяване на съответствието, предвидени в настоящия регламент, доколкото това се отнася до съществените изисквания за киберсигурност, установени в настоящия регламент. В такъв случай за всички останали аспекти, обхванати от Регламент (ЕС) 2024/1689, следва да се прилагат съответните разпоредби за оценяване на съответствието въз основа на вътрешен контрол, посочени в приложение VI към посочения регламент.

(52) За да се подобри сигурността на продуктите с цифрови елементи, пуснати на вътрешния пазар, е необходимо да се определят съществени изисквания за киберсигурност, приложими за тези продукти. Тези съществени изисквания за киберсигурност следва да не засягат координираните на равнището на Съюза оценки на риска за сигурността на критичните вериги на доставките, предвидени в член 22 от Директива (ЕС) 2022/2555, 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 те не следва да 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 на Комисията[22], в координираната оценка на ЕС на риска за киберсигурността на 5G мрежите и в набора от инструменти на ЕС за киберсигурност на 5G, договорени от групата за сътрудничество, създадена съгласно член 14 от Директива (ЕС) 2022/2555.

[22] Препоръка (ЕС) 2019/534 на Комисията от 26 март 2019 г. относно киберсигурността на 5G мрежите (ОВ L 88, 29.3.2019 г., стр. 42).

(53) Производителите на продукти, попадащи в обхвата на Регламент (ЕС) 2023/1230 на Европейския парламент и на Съвета[23], които са също така продукти с цифрови елементи по смисъла на настоящия регламент, следва да отговарят както на съществените изисквания за киберсигурност, определени в настоящия регламент, така и на съществените изисквания за безопасност и опазване на здравето, посочени в Регламент (ЕС) 2023/1230. Съществените изисквания за киберсигурност, определени в настоящия регламент, и някои съществени изисквания, установени в Регламент (ЕС) 2023/1230, могат да се прилагат по отношение на сходни рискове за киберсигурността. Поради това спазването на съществените изисквания за киберсигурност, определени в настоящия регламент, би могло да улесни спазването на съществените изисквания, които обхващат и определени рискове за киберсигурността, посочени в Регламент (ЕС) 2023/1230, и по-специално тези относно защитата срещу корупция, безопасността и надеждността на системите за контрол, посочени в раздели 1.1.9 и 1.2.1 от приложение III към въпросния регламент. Тези полезни взаимодействия трябва да бъдат доказани от производителя, например като се прилагат, когато са налични, хармонизирани стандарти или други технически спецификации, обхващащи съответните съществени изисквания за киберсигурност, след оценка на риска, обхващаща тези киберрискове. Производителят следва също така да спазва приложимите процедури за оценяване на съответствието, посочени в настоящия регламент и в Регламент (ЕС) 2023/1230. В подготвителната работа за подпомагане на прилагането на настоящия регламент и на Регламент (ЕС) 2023/1230 и свързаните процеси по стандартизация Комисията и европейските организации за стандартизация следва да насърчават последователността при оценяването на киберрисковете и начина, по който тези рискове трябва да бъдат обхванати от хармонизирани стандарти по отношение на съответните съществени изисквания.

---

[23] Регламент (ЕС) 2023/1230 на Европейския парламент и на Съвета от 14 юни 2023 г. относно машините и за отмяна на Директива 2006/42/ЕО на Европейския парламент и на Съвета и на Директива 73/361/ЕИО на Съвета (ОВ L 165, 29.6.2023 г., стр. 1).

Комисията и европейските организации за стандартизация следва по-специално да вземат предвид настоящия регламент при подготовката и разработването на хармонизирани стандарти за улесняване на прилагането на Регламент (ЕС) 2023/1230, по-конкретно по отношение на аспектите на киберсигурността, свързани със защитата срещу корупция и безопасността и надеждността на системите за управление, посочени в раздели 1.1.9 и 1.2.1 от приложение III към посочения регламент. Комисията следва да предостави насоки, за да подпомогне попадащите в обхвата на настоящия регламент производители, за които се прилага и Регламент (ЕС) 2023/1230, и по-специално с цел улесняване на доказването на съответствие със съответните съществени изисквания, посочени в настоящия регламент и в Регламент (ЕС) 2023/1230.

(54) За да се гарантира, че продуктите с цифрови елементи са безопасни както в момента на пускането им на пазара, така и през целия период, през който се очаква продуктът с цифрови елементи да се използва, е необходимо да се определят съществени изисквания за киберсигурност за отстраняване на уязвимостите и съществени изисквания за киберсигурност, свързани с характеристиките на продуктите с цифрови елементи. Въпреки че производителите следва да спазват всички съществени изисквания за киберсигурност, свързани с отстраняването на уязвимостите през целия период на поддръжка, те следва да определят кои други съществени изисквания за киберсигурност, свързани с характеристиките на продукта, са приложими за съответния вид продукт с цифрови елементи. 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 за киберсигурност, така че да предоставят своите продукти с цифрови елементи без вече известни уязвимости, които могат да бъдат използвани и да окажат въздействие върху сигурността на тези продукти, както и за да приложат по уместен начин подходящи хармонизирани стандарти, общи спецификации или европейски или международни стандарти.

(55) Когато някои съществени изисквания за киберсигурност не са приложими към продукт с цифрови елементи, производителят следва да включи ясна обосновка в оценката на киберриска, включително в техническата документация. Такъв би могъл да бъде случаят, когато съществено изискване за киберсигурност е несъвместимо с естеството на продукта с цифрови елементи. Например предназначението на даден продукт с цифрови елементи може да изисква производителят да следва широко признати стандарти за оперативна съвместимост, дори ако вече не се счита, че неговите защитени елементи са на съвременно техническо равнище. По сходен начин друго законодателство на Съюза изисква от производителите да прилагат специфични изисквания за оперативна съвместимост. Когато съществено изискване за киберсигурност не е приложимо за даден продукт с цифрови елементи, но производителят е установил киберрискове във връзка с това съществено изискване за киберсигурност, той следва да предприеме мерки за справяне с тези рискове чрез други средства, например чрез ограничаване на предназначението на продукта до надеждна среда или чрез информиране на ползвателите за тези рискове.

(56) Една от най-важните мерки, които ползвателите трябва да предприемат, за да защитят своите продукти с цифрови елементи от кибератаки, е да инсталират най-новите налични актуализации за сигурност във възможно най-кратък срок. Поради това производителите следва да проектират своите продукти и да въведат процеси, така че да гарантират, че продуктите с цифрови елементи включват функции, които позволяват автоматичното уведомяване, разпространение, изтегляне и инсталиране на актуализации за сигурност, по-специално в случай на потребителски продукти. Те следва също така да предоставят възможността за одобряване на изтеглянето и инсталирането на актуализациите за сигурност като последна стъпка. Ползвателите следва да продължат да имат възможността да дезактивират автоматичните актуализации благодарение на ясен и лесен за използване механизъм, придружен с ясни инструкции за това как те могат да се откажат от тези актуализации. Изискванията, свързани с автоматичните актуализации, както са установени в приложение към настоящия регламент, не са приложими за продукти с цифрови елементи, чието основно предназначение е да бъдат интегрирани като компоненти в други продукти. Те също така не се прилагат за продукти с цифрови елементи, за които ползвателите не биха могли разумно да очакват автоматични актуализации, включително продукти с цифрови елементи, предназначени за използване в професионални ИКТ мрежи, и по-специално в критични и промишлени среди, където автоматичното актуализиране би могло да доведе до смущения в операциите. Независимо дали даден продукт с цифрови елементи е проектиран така, че да получава автоматични актуализации, или не, неговият производител следва да информира ползвателите за уязвимостите и без забавяне да предоставя актуализации за сигурност. Когато продукт с цифрови елементи има потребителски интерфейс или подобни технически средства, позволяващи пряко взаимодействие с неговите ползватели, производителят следва да използва тези характеристики, за да информира ползвателите, че техният продукт с цифрови елементи е достигнал края на периода на поддръжка. Уведомленията следва да бъдат ограничени до необходимото, за да се гарантира ефективното получаване на тази информация, и не следва да оказват отрицателно въздействие върху използването на продукта с цифрови елементи от страна на ползвателите.

(57) За да се подобри прозрачността на процесите на отстраняване на уязвимостите и да се гарантира, че от ползвателите не се изисква да инсталират нови актуализации на функционалните възможности единствено с цел получаване на последните актуализации за сигурност, производителите следва да гарантират, когато това е технически осъществимо, че новите актуализации за сигурност се предоставят отделно от актуализациите на функционалните възможности.

(58) В съвместното съобщение на Комисията и върховния представител на Съюза по въпросите на външните работи и политиката на сигурност от 20 юни 2023 г., озаглавено „Европейска стратегия за икономическа сигурност“, се посочва, че Съюзът трябва да увеличи максимално ползите от отворения характер на своята икономика, като същевременно сведе до минимум рисковете от икономическата зависимост от високорискови доставчици чрез обща стратегическа рамка за икономическата сигурност на Съюза. Зависимостта от високорискови доставчици на продукти с цифрови елементи може да представлява стратегически риск, който трябва да се разглежда на равнището на Съюза, особено когато продуктите с цифрови елементи са предназначени за използване от съществени субекти, както са посочени в член 3, параграф 1 от Директива (ЕС) 2022/2555. Тези рискове могат да бъдат свързани, наред с другото, и с юрисдикцията, приложима за производителя, характеристиките на неговата корпоративна собственост и връзките на контрол с правителството на третата държава, в която е установен, по-специално когато дадена трета държава участва в икономически шпионаж или няма отговорно поведение в киберпространството и нейното законодателство позволява произволен достъп до всякакъв вид операции или данни на дружествата, включително чувствителни от търговска гледна точка данни, и може да налага задължения за целите на разузнаването без демократични механизми за взаимозависимост и взаимоограничаване, механизми за надзор, надлежно провеждане на съдебните процеси или право на обжалване пред независим съд. При определяне на значимостта на киберриск по смисъла на настоящия регламент Комисията и органите за надзор на пазара, съгласно отговорностите си, посочени в настоящия регламент, следва да вземат предвид и нетехническите рискови фактори, по-специално тези, установени в резултат на координирани на равнището на Съюза оценки на риска за сигурността на критични вериги за доставка, извършени в съответствие с член 22 от Директива (ЕС) 2022/2555.

(59) С цел да се гарантира сигурността на продуктите с цифрови елементи след пускането им на пазара, производителите следва да определят периода на поддръжка, които следва да отразяват времето, през което се очаква продуктът с цифрови елементи да бъде в употреба. При определянето на период на поддръжка производителят следва да вземе предвид по-специално разумните очаквания на ползвателите, естеството на продукта, както и съответното законодателство на Съюза, определящо жизнения цикъл на продуктите с цифрови елементи. Производителите следва също така да могат да вземат предвид и други значими фактори. Критериите следва да се прилагат по начин, който гарантира пропорционалност при определянето на периода на поддръжка. При поискване производителят следва да предостави на органите за надзор на пазара информацията, която е била взета предвид при определянето на периода на поддръжка на даден продукт с цифрови елементи.

(60) Периодът на поддръжка, през който производителят гарантира ефективното отстраняване на уязвимостите, не следва да бъде по-кратък от пет години, освен ако жизненият цикъл на продукта с цифрови елементи е по-кратък от пет години, като в този случай производителят следва да гарантира отстраняването на уязвимостите за този жизнен цикъл. Когато е разумно да се очаква продуктът с цифрови елементи да се използва повече от пет години, какъвто често е случаят с хардуерните компоненти като дънни платки или микропроцесори, мрежови устройства като маршрутизатори, модеми или комутатори, както и софтуер като операционни системи или инструменти за обработване на видеоматериали, производителите следва съответно да гарантират по-дълги периоди на поддръжка. По-специално продуктите с цифрови елементи, предназначени за използване в промишлени условия, като например системи за промишлен контрол, често се използват за значително по-дълги периоди от време. Производителят следва да може да определи период на поддръжка, по-кратък от пет години, само когато това е оправдано поради естеството на съответния продукт с цифрови елементи и когато се очаква този продукт да се използва по-малко от пет години, като в този случай периодът на поддръжка следва да съответства на очакваното време на използване. Например жизненият цикъл на приложение за проследяване на контакти, предназначено за да се използва по време на пандемия, може да бъде ограничен до продължителността на пандемията. Освен това някои софтуерни приложения поради естеството си могат да се предоставят само въз основа на абонаментен модел, по-специално когато след изтичането на абонамента приложението става недостъпно за ползвателя и следователно няма повече да бъде използвано.

(61) Когато продуктите с цифрови елементи достигнат края на периода си на поддръжка, за да се гарантира, че уязвимостите могат да бъдат отстранявани след края на периода на поддръжка, производителите следва да предвидят предоставянето на изходния код на такива продукти с цифрови елементи или на други предприятия, които се ангажират да удължат предоставянето на услуги за отстраняване на уязвимости, или на обществеността. Когато предоставят изходния код на други предприятия, производителите следва да могат да защитят собствеността върху продукта с цифрови елементи и да предотвратят разпространението на изходния код сред обществеността, например чрез договорни споразумения.

(62) За да се гарантира, че производителите в целия Съюз определят сходни периоди на поддръжка за сравними продукти с цифрови елементи, ADCO групата следва да публикува статистически данни за средните периоди на поддръжка, определени от производителите за категориите продукти с цифрови елементи, и да издаде насоки, указващи подходящите периоди на поддръжка за тези категории. Освен това, за да се гарантира хармонизиран подход в рамките на целия вътрешен пазар, Комисията следва да може да приема делегирани актове за определяне на минимални периоди на поддръжка за конкретни категории продукти, когато данните, предоставени от органите за надзор на пазара, показват, че периодите на поддръжка, определени от производителите, системно не съответстват на критериите за определяне на периодите на поддръжка, установени в настоящия регламент, или че производителите в различни държави членки неоснователно определят различни периоди на поддръжка.

(63) Производителите следва да създадат единно звено за контакт, което да дава възможност на ползвателите да комуникират лесно с тях, включително с цел сигнализиране и получаване на информация относно уязвимостите на продукта с цифрови елементи. Те следва да направят така, че единното звено за контакт да е леснодостъпно за ползвателите, да посочват ясно съществуването му и да поддържат информацията актуална. Когато производителите решат да предлагат автоматизирани инструменти, като например чатове, те следва да предлагат също така и телефонен номер или други цифрови средства за контакт като адрес на електронна поща или формуляр за контакт. Единното звено за контакт не следва да разчита изключително на автоматизирани инструменти.

(64) Производителите следва да предоставят на пазара своите продукти с цифрови елементи с конфигурация с настройки за сигурност по подразбиране и да предоставят безплатно на потребителите актуализации за сигурност. Производителите следва да могат да се отклоняват от съществените изисквания за киберсигурност в случай на специално създадени продукти, които са пригодени за конкретна цел за конкретен бизнес ползвател, и когато както производителят, така и ползвателят изрично са се съгласили с различен набор от договорни условия.

(65) Производителите следва да нотифицират едновременно, чрез единната платформа за докладване, екипа за реагиране при инциденти с компютърната сигурност (ЕРИКС), определен за координатор, и ENISA за активно използвани уязвимости, съдържащи се в продукти с цифрови елементи, както и за сериозни инциденти, които оказват въздействие върху сигурността на тези продукти. Нотификациите следва да се подават, като се използва крайната точка за електронно нотифициране на определен за координатор ЕРИКС, и следва да бъдат едновременно достъпни за ENISA.

(66) Производителите следва да подават нотификации за активно използваните уязвимости, за да се гарантира, че определените за координатори ЕРИКС и ENISA имат ясна картина по отношение на тези уязвимости и получават необходимата информация за изпълнение на техните задачи, определени в Директива (ЕС) 2022/2555, и да се повиши цялостното ниво на киберсигурност на съществените и важните субекти, както са посочени в член 3 от същата директива, както и за да се осигури ефективното функциониране на органите за надзор на пазара. 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. ENISA следва, със съгласието на производителя, да оповестява фиксирани уязвимости в европейската база данни за уязвимости, създадена съгласно член 12, параграф 2 от Директива (ЕС) 2022/2555. Европейската база данни за уязвимости ще подпомага производителите да откриват вече известни уязвимости в своите продукти, за да се гарантира, че на пазара се предоставят безопасни продукти.

(67) Производителите следва също така да нотифицират определения за координатор ЕРИКС и ENISA за всеки сериозен инцидент, който оказва въздействие върху сигурността на продукта с цифрови елементи. С цел да се гарантира, че ползвателите могат да реагират бързо на сериозни инциденти, които оказват въздействие върху сигурността на техните продукти с цифрови елементи, производителите следва също така да информират своите ползватели за всеки такъв инцидент и когато е приложимо, за всички корективни мерки, които ползвателите могат да приложат, за да намалят въздействието на инцидента, например като публикуват съответната информация на своите уебсайтове или, когато производителите са в състояние да се свържат с ползвателите и когато това е оправдано от киберрисковете, като се обърнат директно към ползвателите.

(68) Активно използваните уязвимости се отнасят до случаи, в които производител установи, че нарушение на сигурността, засягащо ползвателите на неговите продукти или други физически или юридически лица, е причинено от злонамерен участник, който се е възползвал от недостатък в един от продуктите с цифрови елементи, предоставени на пазара от производителя. Примери за такива уязвимости могат да бъдат слабости във функциите на продукта за идентификация и удостоверяване на автентичността. Уязвимостите, които се откриват без злонамереност за целите на добросъвестното изпитване, разследване, коригиране или оповестяване, за да се насърчава сигурността или безопасността на собственика на системата и нейните ползватели, не следва да подлежат на задължение за нотифициране. Сериозните инциденти, които оказват въздействие върху сигурността на продукта с цифрови елементи, от друга страна, се отнасят до ситуации, при които киберинцидент засяга процесите на производителя по разработване, производство или поддръжка по такъв начин, че може да доведе до повишен киберриск за ползвателите или други лица. Такъв сериозен инцидент би могъл да включва ситуация, когато извършващият атаката успешно е въвел злонамерен код в канала, чрез който производителят предоставя на ползвателите актуализации за сигурност.

(69) За да се гарантира, че нотификациите могат да се разпространяват бързо до всички съответни ЕРИКС, определени за координатори, и за да се даде възможност на производителите да подават една-единствена нотификация на всеки етап от процеса на нотифициране, ENISA следва да създаде единна платформа за докладване с национални крайни точки за електронно нотифициране. Ежедневните операции на единната платформа за докладване следва да се управляват и поддържат от ENISA. Определените за координатори ЕРИКС следва да информират съответните органи за надзор на пазара за уязвимостите или инцидентите, за които са подадени нотификации. Единната платформа за докладване следва да бъде проектирана по такъв начин, че да гарантира поверителността на нотификациите, по-специално по отношение на уязвимостите, за които все още не е налична актуализация за сигурност. Освен това ENISA следва да въведе процедури за обработване на информацията в условия на сигурност и поверителност. Въз основа на информацията, която е събрала, 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, създадена съгласно член 14 от Директива (ЕС) 2022/2555.

(70) При изключителни обстоятелства и по-специално по искане на производителя определеният за координатор ЕРИКС, който първоначално получава нотификация, следва да може да реши да забави нейното разпространение до другите съответни ЕРИКС, определени за координатори, чрез единната платформа за докладване, когато това може да бъде обосновано от съображения, свързани с киберсигурността, и за период от време, който е строго необходим. Определеният за координатор ЕРИКС следва незабавно да информира ENISA за решението за забавяне и за неговите основания, както и кога възнамерява да продължи разпространението. Комисията следва да разработи чрез делегиран акт спецификации относно реда и условията за прилагане на основания, свързани с киберсигурността, и следва да си сътрудничи с мрежата на ЕРИКС, създадена съгласно член 15 от Директива (ЕС) 2022/2555, и с ENISA при изготвянето на проекта на делегиран акт. Примерите за основания, свързани с киберсигурността, включват текуща координирана процедура за оповестяване на уязвимости или ситуации, при които се очаква производителят скоро да предостави смекчаваща мярка и когато киберрисковете от незабавно разпространение чрез единната платформа за докладване надвишават неговите ползи. Ако определеният за координатор ЕРИКС поиска това, ENISA следва да може да подпомага този ЕРИКС при прилагането на основания, свързани с киберсигурността, във връзка със забавяне на разпространението на нотификацията въз основа на информацията, която ENISA е получила от посочения ЕРИКС, във връзка с решението за непредоставяне на нотификация относно тези основания, свързани с киберсигурността.

Освен това при особено изключителни обстоятелства ENISA не следва да получава едновременно всички подробности за нотификация за активно използвана уязвимост. Такъв би бил случаят, когато производителят отбелязва в своята нотификация, че нотифицираната уязвимост е била активно използвана от злонамерен участник и че според наличната информация тя не е била използвана в никоя друга държава членка, различна от тази на определения за координатор ЕРИКС, на който производителят е нотифицирал уязвимостта, когато всяко незабавно по-нататъшно разпространение на нотифицираната уязвимост вероятно би довело до предоставянето на информация, чието разкриване би било в противоречие с основните интереси на посочената държава членка, или когато нотифицираната уязвимост съставлява непосредствен висок киберриск, произтичащ от по-нататъшното разпространение. В такива случаи ENISA ще получи само едновременен достъп до информацията, че е направена нотификация от производителя, обща информация за съответния продукт с цифрови елементи, информация за общия характер на експлойта и информация относно факта, че тези съображения за сигурност са били повдигнати от производителя и че поради това пълното съдържание на нотификацията не е било публикувано. След това пълната нотификация следва да се предостави на ENISA и на други определени за координатори относими ЕРИКС, когато определеният за координатор ЕРИКС, който първоначално получава нотификацията, установи, че тези основания за сигурност, отразяващи особено извънредните обстоятелства, установени в настоящия регламент, престават да съществуват. Когато въз основа на наличната информация ENISA счита, че съществува системен риск, засягащ сигурността на вътрешния пазар, ENISA следва да препоръча на получаващия ЕРИКС да разпространи пълната нотификация до другите определени за координатори ЕРИКС и до самата ENISA.

(71) Когато производителите нотифицират активно използвана уязвимост или сериозен инцидент, оказващ въздействие върху сигурността на продукта с цифрови елементи, те следва да посочат до каква степен считат нотифицираната информация за чувствителна. Определеният за координатор ЕРИКС, който първоначално получава нотификацията, следва да вземе предвид тази информация, когато преценява дали нотификацията поражда извънредни обстоятелства, които оправдават забавяне на разпространението на уведомлението до другите съответни определени за координатори ЕРИКС, въз основа на обосновка, свързана с киберсигурността. Той следва също така да вземе предвид тази информация, когато преценява дали нотифицирането на активно използвана уязвимост поражда особено изключителни обстоятелства, които оправдават факта, че пълната нотификация не се предоставя едновременно на ENISA. И накрая, определените за координатори ЕРИКС следва да могат да вземат предвид тази информация, когато определят подходящи мерки за смекчаване на рисковете, произтичащи от такива уязвимости и инциденти.

(72) За да се опрости докладването на информацията, изисквана съгласно настоящия регламент, като се вземат предвид други допълнителни изисквания за докладване, установени в правото на Съюза, като например Регламент (ЕС) 2016/679, Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета[24], Директива № 2002/58/ЕО на Европейския парламент и на Съвета[25] и Директива (ЕС) 2022/2555, както и за да се намали административната тежест за субектите, държавите членки се насърчават да обмислят възможността за предоставяне на национално равнище на единни входящи точки за такива изисквания за докладване. Използването на такива национални входящи точки за докладване на инциденти, свързани със сигурността, съгласно Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО не следва да засяга прилагането на разпоредбите на Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО, по-специално тези, свързани с независимостта на посочените в тях органи. При създаването на единната платформа за докладване, посочена в настоящия регламент, ENISA следва да вземе предвид възможността националните крайни точки за електронно нотифициране, посочени в настоящия регламент, да бъдат интегрирани в националните единни входни точки, които могат да включват и други нотификации, изисквани съгласно правото на Съюза.

---

[24] Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 (ОВ L 333, 27.12.2022 г., стр. 1).

[25] Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (ОВ L 201, 31.7.2002 г., стр. 37).

(73) При създаването на единната платформа за докладване, посочена в настоящия регламент, и за да се възползва от натрупания опит, ENISA следва да се консултира с други институции или агенции на Съюза, които управляват платформи или бази данни, подлежащи на строги изисквания за сигурност, като например Агенцията на Европейския съюз за оперативното управление на широкомащабни информационни системи в пространството на свобода, сигурност и правосъдие (eu-LISA). ENISA следва също така да анализира потенциално взаимно допълване с европейската база данни за уязвимости, създадена съгласно член 12, параграф 2 от Директива (ЕС) 2022/2555.

(74) Производителите и другите физически и юридически лица следва да могат да уведомяват определения за координатор ЕРИКС или ENISA, на доброволна основа, за всяка уязвимост, съдържаща се в продукт с цифрови елементи, за киберзаплахи, които биха могли да засегнат рисковия профил на продукт с цифрови елементи, за всеки инцидент, който оказва въздействие върху сигурността на продукта с цифрови елементи, както и за ситуациите, близки до инциденти, които са могли да доведат до такъв инцидент.

(75) Държавите членки следва да се стремят да вземат мерки, доколкото е възможно, срещу предизвикателствата, пред които са изправени изследователите в областта на уязвимостта, включително потенциалната опасност да им бъде търсена наказателна отговорност, в съответствие с националното право. Като се има предвид, че физическите и юридическите лица, които изследват уязвимости, биха могли в някои държави членки да бъдат изложени на наказателна и гражданска отговорност, държавите членки се насърчават да приемат насоки по отношение на отказа от наказателно преследване на изследователите в областта на информационната сигурност и освобождаването от гражданска отговорност за тези дейности.

(76) 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 или пряко на производителя, или непряко, а при поискване анонимно — чрез определените за координатори ЕРИКС за целите на координираното оповестяване на уязвимости в съответствие с член 12, параграф 1 от Директива (ЕС) 2022/2555. В политиката на производителите 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. Освен това производителите следва също да обмислят публикуването на своите политики за сигурност в машинночетим формат. 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. Това се отнася до т.нар. „програми за награда за откриване на уязвимости“.

(77) 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. Опис 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 по-специално помага на производителите и ползвателите да проследяват нововъзникващи уязвимости и рискове за киберсигурността. Особено важно е производителите да гарантират, че техните продукти с цифрови елементи не съдържат уязвими компоненти, разработени от трети страни. Производителите не следва да бъдат задължени да публикуват описа на софтуерните компоненти.

(78) При новите сложни бизнес модели, свързани с онлайн продажбите, дружество, което извършва дейност онлайн, може да предлага редица услуги. В зависимост от естеството на услугите, предоставяни във връзка с даден продукт с цифрови елементи, един и същ субект може да попада в различни категории бизнес модели или икономически оператори. Когато даден субект предоставя само посреднически онлайн услуги за даден продукт с цифрови елементи и е само доставчик на онлайн място за търговия съгласно определението в член 3, точка 14 от Регламент (ЕС) 2023/988, той не се счита за един от видовете икономически оператори, определени в настоящия регламент. Когато един и същ субект е доставчик на онлайн място за търговия и действа като икономически оператор съгласно определението в настоящия регламент за продажбата на конкретни продукти с цифрови елементи, той следва да подлежи на задълженията, посочени в настоящия регламент за този тип икономически оператори. Например, ако доставчикът на онлайн място за търговия разпространява и продукт с цифрови елементи, тогава по отношение на продажбата на посочения продукт той ще се счита за дистрибутор. По подобен начин, ако въпросният субект продава свои собствени маркови продукти с цифрови елементи, той ще се определя като производител и следователно ще трябва да спазва приложимите към производителите изисквания. Също така, някои субекти могат да се определят като доставчици на услуги за обработка на поръчки съгласно определението в член 3, точка 11 от Регламент (ЕС) 2019/1020 на Европейския парламент и на Съвета[26], ако предлагат такива услуги. Такива случаи ще трябва да бъдат преценявани поотделно. Като се има предвид важната роля на онлайн местата за търговия за създаването на условия за електронна търговия, те следва да се стремят да си сътрудничат с органите за надзор на пазара на държавите членки, за да се помогне за гарантиране на това продуктите с цифрови елементи, закупени чрез онлайн места за търговия, да отговарят на изискванията за киберсигурност, определени в настоящия регламент.

---

[26] 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).

(79) 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 за киберсигурност, определени в настоящия регламент, в подробни технически спецификации и които са приети в съответствие с Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета[27]. Посоченият регламент предвижда процедура за възражения срещу хармонизирани стандарти, когато тези стандарти не отговарят напълно на изискванията, установени в настоящия регламент. Процесът на стандартизация следва да гарантира балансирано представяне на интересите и ефективно участие на заинтересованите страни от гражданското общество, включително организациите на потребителите. Международните стандарти, които са в съответствие с нивото на киберзащита, предвидено в съществените изисквания за киберсигурност, определени в настоящия регламент, също следва да бъдат взети предвид, за да се улеснят разработването на хармонизирани стандарти и прилагането на настоящия регламент, както и за да се улесни спазването на изискванията от страна на дружествата, по-специално микропредприятията и малките и средните предприятия, както и тези, които извършват дейност в световен мащаб.

---

[27] 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).

(80) Навременното разработване на хармонизирани стандарти по време на преходния период за прилагането на настоящия регламент и тяхната наличност преди датата на прилагане на настоящия регламент ще бъде от особено значение за ефективното му прилагане. Такъв е по-специално случаят с важни продукти с цифрови елементи, които попадат в клас I. Наличието на хармонизирани стандарти ще даде възможност на производителите на такива продукти да извършват оценките на съответствието чрез процедурата за вътрешен контрол и следователно така могат да се избегнат затруднения и забавяния в дейностите на органите за оценяване на съответствието.

(81) С Регламент (ЕС) 2019/881 се създава доброволна Европейска рамка за сертифициране на киберсигурността на продукти в областта на ИКТ, процеси в областта на ИКТ и услуги в областта на ИКТ. Европейските схеми за сертифициране на киберсигурността осигуряват обща рамка на доверие, за да могат потребителите да използват продуктите с цифрови елементи, които попадат в обхвата на настоящия регламент. Ето защо 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 декларация за съответствие по европейска 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 за киберсигурност, определени в настоящия регламент, доколкото европейският сертификат 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, включително при подготовката на непрекъснатата работна програма на Съюза в съответствие с Регламент (ЕС) 2019/881. Когато е необходима нова схема, обхващаща продукти с цифрови елементи, включително за да се улесни спазването на настоящия регламент, Комисията може да поиска от ENISA да изготви проекти за схеми в съответствие с член 48 от Регламент (ЕС) 2019/881. Такива бъдещи европейски схеми за сертифициране на киберсигурността, които обхващат продукти с цифрови елементи, следва да отчитат съществените изисквания за киберсигурност и процедурите за оценяване на съответствието, както са определени в настоящия регламент, и да улесняват съответствието с него. За европейските схеми за сертифициране на киберсигурността, които влизат в сила преди влизането в сила на настоящия регламент, може да са необходими допълнителни спецификации относно подробните аспекти на начина, по който може да се прилага презумпцията за съответствие.

На Комисията следва да бъде предоставено правомощието да определи чрез делегирани актове при какви условия европейските схеми за сертифициране на киберсигурността могат да се използват за доказване на съответствие със съществените изисквания за киберсигурност, определени в настоящия регламент. Освен това, за да се избегне ненужна административна тежест, не следва да има задължение за производителите да извършват оценка на съответствието от трета страна, както е предвидено в настоящия регламент за съответните изисквания, когато съгласно такива европейски схеми за сертифициране на киберсигурността е издаден европейски сертификат за киберсигурност поне с ниво на увереност „съществено“.

(82) След влизането в сила на Регламент за изпълнение (ЕС) 2024/482, който се отнася до продукти, които попадат в обхвата на настоящия регламент, като например хардуерни модули за сигурност и микропроцесори, Комисията следва да може да уточни чрез делегиран акт по какъв начин ЕССК предоставя презумпция за съответствие със съществените изисквания за киберсигурност, определени в настоящия регламент, или с части от тях. Освен това в такъв делегиран акт може да се уточни по какъв начин сертификат, издаден съгласно ЕССК, премахва задължението за производителите да извършват изискваната съгласно настоящия регламент оценка от трета страна за съответните изисквания.

(83) Настоящата европейска рамка за стандартизация, която се основава на принципите на т.нар. „нов подход“, посочени в резолюцията на Съвета от 7 май 1985 г. относно нов подход за техническа хармонизация и стандарти, и на Регламент (ЕС) № 1025/2012, представлява по подразбиране рамката за разработване на стандарти, които осигуряват презумпция за съответствие с приложимите съществени изисквания за киберсигурност, определени в настоящия регламент. Европейските стандарти следва да се определят от потребностите на пазара, да отчитат обществения интерес, както и целите на политиките, ясно посочени в искането на Комисията до една или няколко европейски организации за стандартизация да изготвят хармонизирани стандарти, в определен срок, и следва да се основават на консенсус. При липса обаче на публикуване на данните за съответни хармонизирани стандарти Комисията следва да може да приема актове за изпълнение за определяне на общи спецификации за съществените изисквания за киберсигурност, определени в настоящия регламент, при условие че при това надлежно зачита ролята и функциите на организациите за стандартизация, като резервно решение по изключение за улесняване на задължението на производителя да спазва тези съществени изисквания за киберсигурност, когато процесът по стандартизация е блокиран или когато има забавяне при създаването на подходящи хармонизирани стандарти. В случай че забавянето се дължи на техническата сложност на стандарта, това следва да се вземе предвид от Комисията, преди да се обмисля дали да бъдат определени общи спецификации.

(84) С оглед на определянето по най-ефикасен начин на общи спецификации, които обхващат съществените изисквания за киберсигурност, определени в настоящия регламент, Комисията следва да включи в процеса съответните заинтересовани лица.

(85) „Разумен срок“, във връзка с публикуването на данните за хармонизираните стандарти в *Официален вестник на Европейския съюз* в съответствие с Регламент (ЕС) № 1025/2012, има значението на срок, в рамките на който се очаква публикуването в *Официален вестник на Европейския съюз* на данните за стандарта, на неговата поправка или на изменението му и който не следва да надвишава една година след крайния срок за изготвяне на европейски стандарт, определен в съответствие с Регламент (ЕС) № 1025/2012.

(86) С цел да се улесни оценяването на съответствието със съществените изисквания за киберсигурност, определени в настоящия регламент, следва да има презумпция за съответствие за продуктите 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.

(87) Прилагането на хармонизирани стандарти, общи спецификации или европейски схеми за сертифициране на киберсигурността, приети съгласно Регламент (ЕС) 2019/881, осигуряващи презумпция за съответствие по отношение на съществените изисквания за киберсигурност, приложими за продукти с цифрови елементи, ще улесни оценяването на съответствието от страна на производителите. Ако производителят избере да не прилага такива средства за определени изисквания, той трябва да посочи в техническата си документация как по друг начин се постига съответствието. Освен това прилагането на хармонизирани стандарти, общи спецификации или европейски схеми за сертифициране на киберсигурността, приети съгласно Регламент (ЕС) 2019/881, които осигуряват презумпция за съответствие от страна на производителите, би улеснило проверката на съответствието на продуктите с цифрови елементи от страна на органите за надзор на пазара. Поради това производителите на продукти с цифрови елементи се насърчават да прилагат такива хармонизирани стандарти, общи спецификации или европейски схеми за сертифициране на киберсигурността.

(88) 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 за киберсигурност, определени в настоящия регламент и, когато е приложимо, на другото приложимо законодателство на Съюза за хармонизация, което обхваща продукта с цифрови елементи. От производителите може също така да се изисква да изготвят ЕС декларация за съответствие съгласно други правни актове 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 правни 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.

(89) 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[28]. 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, посочени в настоящия регламент.

---

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

(90) За да се даде възможност на икономическите оператори да докажат съответствието си със съществените изисквания за киберсигурност, 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[29] 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 за киберсигурност, определени в настоящия регламент, следва да 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 с цифрови елементи.

[29] . Решение № 768/2008/ЕО на Европейския парламент и на 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).

(91) Оценяването на съответствието на продукти с цифрови елементи, които не са изброени като важни или критични продукти с цифрови елементи в настоящия регламент, може да се извършва от производителя на негова отговорност като се следва процедурата за вътрешен контрол, основана на модул А от Решение № 768/2008/ЕО в съответствие с настоящия регламент. Това се прилага и в случаите, когато производител избере да не прилага изцяло или частично приложим хармонизиран стандарт, обща спецификация или европейска схема за сертифициране на киберсигурността. Производителят запазва гъвкавостта си да избере по-строга процедура за оценяване на съответствието с участието на трета страна. Съгласно процедурата за оценяване на съответствието за вътрешен контрол производителят гарантира и декларира на своя отговорност, че продуктът с цифрови елементи и процесите на производителя отговарят на приложимите съществени изисквания за киберсигурност, определени в настоящия регламент. Ако важен продукт с цифрови елементи е класифициран в клас I, се изисква допълнителна гаранция за доказване на съответствието със съществените изисквания за киберсигурност, определени в настоящия регламент. Производителят следва да прилага хармонизирани стандарти, общи спецификации или европейски схеми за сертифициране на киберсигурността, приети съгласно Регламент (ЕС) 2019/881, които са били посочени 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 европейски схеми за сертифициране на киберсигурността, той следва да извърши оценяване на съответствието с участието на трета страна (въз основа на модули В и С или модул Н). 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 на модули В и С или модул Н от Решение № 768/2008/ЕО, бяха избрани като най-подходящи за оценяване на съответствието на важни 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 на проектиране и производство. Като се има предвид още по-големият киберриск, свързан с използването на важни продукти с цифрови елементи, които попадат в клас II, оценяването на съответствието следва винаги да включва трета страна, дори когато продуктът отговаря изцяло или частично на хармонизирани стандарти, общи спецификации или европейски схеми за сертифициране на киберсигурността. Производителите на важни продукти с цифрови елементи, квалифицирани като свободен софтуер с отворен код, следва да могат да следват процедурата за вътрешен контрол въз основа на модул А, при условие че предоставят техническата документация на разположение на обществеността.

(92) 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 за киберсигурност, определени в настоящия регламент, през етапите на проектиране, разработване и производство.

(93) По отношение на микропредприятията и малките предприятия, за да се гарантира пропорционалност, е целесъобразно да се намалят административните разходи, без да се засягат нивото на защита на киберсигурността на продуктите с цифрови елементи, които попадат в обхвата на настоящия регламент, или еднаквите условия на конкуренция между производителите. Поради това е целесъобразно Комисията да установи опростен формуляр за техническа документация, насочен към нуждите на микропредприятията и малките предприятия. Опростеният формуляр за техническа документация, приет от Комисията, следва да обхваща всички приложими елементи, свързани с техническата документация, определени в настоящия регламент, и да посочва как дадено микропредприятие или малко предприятие може да предостави исканите елементи в сбита форма, като например описанието на проектирането, разработването и производството на продукта с цифрови елементи. По този начин формулярът ще допринесе за облекчаване на административната тежест за привеждане в съответствие, като предостави на засегнатите предприятия правна сигурност относно обхвата и подробностите на информацията, която трябва да бъде предоставена. Микропредприятията и малките предприятия следва да могат да изберат да предоставят в подробен вид приложимите елементи, свързани с техническата документация, и да не се възползват от опростения формуляр за техническата документация, който е на тяхно разположение.

(94) За да се насърчават и защитават иновациите, е важно да се обърне специално внимание на интересите на производителите, които са микропредприятия или малки или средни предприятия, и по-специално микропредприятия и малки предприятия, включително новосъздадени предприятия. За тази цел държавите членки биха могли да разработят инициативи, насочени към производителите, които са микропредприятия или малки предприятия, включително относно обучението, повишаването на осведомеността, съобщаването на информация, изпитването и дейностите по оценяване на съответствието от трета страна, както и създаването на регулаторни лаборатории. Разходите за превод, свързани със задължителната документация, като например техническата документация и информацията и инструкциите за ползвателя, изисквани съгласно настоящия регламент, както и комуникацията с органите, могат да съставляват значителен разход за производителите, по-специално за тези с по-малък размер. Ето защо държавите членки следва да могат да приемат, че един от езиците, определени и приети от тях за съответната документация на производителите и за комуникация с производителите, е език, който в значителна степен се разбира от възможно най-голям брой ползватели.

(95) За да се гарантира безпроблемното прилагане на настоящия регламент, държавите членки следва да се стремят да гарантират, преди датата на прилагане на настоящия регламент, че е налице достатъчен брой нотифицирани органи за извършване на оценки на съответствието от трета страна. Комисията следва да се стреми да подпомага държавите членки и други относими страни в това начинание, за да се избегнат затруднения и пречки пред производителите за навлизането на пазара. Целенасочените дейности за обучение, ръководени от държавите членки, включително, когато е целесъобразно, с подкрепата на Комисията, могат да допринесат за наличието на квалифицирани специалисти, включително в подкрепа на дейностите на нотифицираните органи съгласно настоящия регламент. Освен това, като се имат предвид разходите, до които може да доведе оценяването на съответствието от трета страна, следва да се обмислят инициативи за финансиране на равнището на Съюза и на национално равнище, които имат за цел да намалят тези разходи за микропредприятията и малките предприятия.

(96) За да се гарантира пропорционалност, при определянето на таксите за процедурите за оценяване на съответствието органите за оценяване на съответствието следва да вземат предвид специфичните интереси и нужди на микропредприятията и малките и средните предприятия, включително новосъздадените предприятия. По-специално органите за оценяване на съответствието следва да прилагат съответната процедура по разглеждане и изпитвания, предвидена в настоящия регламент, само когато е целесъобразно и като следват основан на риска подход.

(97) Целите на регулаторните лаборатории следва да бъдат насърчаване на иновациите и конкурентоспособността на предприятията чрез създаване на контролирана среда за изпитване преди пускането на пазара на продукти с цифрови елементи. Регулаторните лаборатории следва да допринесат за подобряване на правната сигурност за всички участници, които попадат в обхвата на настоящия регламент, и за улесняване и ускоряване на достъпа до пазара на Съюза за продукти с цифрови елементи, по-специално когато се предоставят от микропредприятия и малки предприятия, включително новосъздадени предприятия.

(98) 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.

(99) 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.

(100) Органите за оценяване на съответствието, които са акредитирани и нотифицирани съгласно правото на Съюза, с което се определят изисквания, подобни на предвидените в настоящия регламент, като например орган за оценяване на съответствието, който е нотифициран за европейска схема за сертифициране на киберсигурността, приета съгласно Регламент (ЕС) 2019/881, или нотифицирани съгласно Делегиран регламент (ЕС) 2022/30, следва да бъдат оценени и нотифицирани съгласно настоящия регламент. Съответните органи обаче могат да определят полезни взаимодействия по отношение на всички припокриващи се изисквания, за да се предотврати ненужна финансова и административна тежест и да се гарантира гладък и навременен процес на нотифициране.

(101) 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.

(102) 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 продукт с цифрови елементи, който се пуска 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.

(103) 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.

(104) 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.

(105) 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.

(106) Надзорът на пазара е основно средство при осигуряването на правилно и еднакво прилагане на правото 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, се прилагат за продуктите с цифрови елементи, които попадат в обхвата на настоящия регламент.

(107) В съответствие с Регламент (ЕС) 2019/1020 орган за надзор на пазара осъществява надзор на пазара на територията на държавата членка, която го определя. Настоящият регламент следва да не възпрепятства държавите членки при избора на компетентни органи за изпълнение на задачите по надзор на пазара. Всяка държава членка следва да определи един или повече органи за надзор на пазара на своята територия. Държавите членки следва да могат да изберат да определят всеки съществуващ или нов орган, който да действа като орган за надзор на пазара, включително компетентни органи, определени или създадени съгласно член 8 от Директива (ЕС) 2022/2555, национални органи за сертифициране на киберсигурността, определени съгласно член 58 от Регламент (ЕС) 2019/881, или органи за надзор на пазара, определени за целите на Директива 2014/53/ЕС. 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 на пазара, 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.

(108) Следва да бъде създадена специализирана група за административно сътрудничество (ADCO група) за киберустойчивостта на продукти с цифрови елементи за еднакво прилагане на настоящия регламент в съответствие с член 30, параграф 2 от Регламент (ЕС) 2019/1020. ADCO групата 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 съгласно член 29 от Регламент (ЕС) 2019/1020 и състояща се от представители на всяка държава членка, включително представител на всяка единна служба за връзка, както е посочена в член 10 от същия регламент, и национален експерт по избор, председателите на ADCO групи и представители на Комисията. Комисията следва да участва в заседанията на Мрежата на Съюза за съответствието на продуктите, нейните подгрупи и ADCO групата. Тя следва също така да подпомага ADCO групата чрез изпълнителен секретариат, който да осигурява техническа и логистична подкрепа. ADCO групата може също така да кани независими експерти да участват и да поддържат връзка с други ADCO групи, като например създадената съгласно Директива 2014/53/ЕС.

(109) Органите за надзор на пазара, чрез създадената съгласно настоящия регламент ADCO група, следва да си сътрудничат тясно и следва да могат да разработват документи с насоки за улесняване на дейностите по надзор на пазара на национално равнище, например чрез разработване на най-добри практики и показатели за ефективна проверка на съответствието на продуктите с цифрови елементи с настоящия регламент.

(110) 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 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.

(111) 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 съществени субекти, както са посочени в член 3, параграф 1 от Директива (ЕС) 2022/2555, 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 продукт с цифрови елементи 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 с цифрови елементи, 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 и да го съобщи незабавно на тях и на съответния(те) икономически оператор(и). Ако мярката бъде счетена за обоснована, Комисията следва също така да обмисли дали да приеме предложения за преразглеждане на относимото право на Съюза.

(112) 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, за спазването на задължения съгласно правото на Съюза или националното право, целящи защитата на основните права, или за наличността, автентичността, целостта или поверителността на услуги, предоставяни чрез електронна информационна система от съществени субекти, посочени в член 3, параграф 1 от Директива (ЕС) 2022/2555, Комисията следва да може да поиска от ENISA да извърши оценка. Въз основа на тази оценка Комисията следва да може да приеме, посредством актове за изпълнение, корективни или ограничителни мерки на равнището на Съюза, включително с изискване засегнатите продукти с цифрови елементи да бъдат изтеглени от пазара или иззети, в разумен срок, съобразен с естеството на риска. Комисията следва да може да прибягва до такава намеса само при извънредни обстоятелства, които оправдават незабавна намеса за запазване на правилното функциониране на вътрешния пазар, и само когато органите за надзор на пазара не са предприели ефективни мерки за коригиране на ситуацията. Такива извънредни обстоятелства могат да бъдат извънредни ситуации, когато например несъответстващ на изискванията продукт с цифрови елементи е широко предлаган от производителя в няколко държави членки, използва се също така в ключови сектори от субекти, които попадат в обхвата на Директива (ЕС) 2022/2555, като същевременно съдържа известни уязвимости, които се използват от злонамерени участници и за които производителят не предоставя налични корекции. Комисията следва да 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.

(113) 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.

(114) 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 с цифрови елементи често са свързани с киберрискове. Освен това при определянето на категориите продукти, които да бъдат обект на мащабни проверки, органите за надзор на пазара следва също така да вземат предвид обстоятелствата, свързани с нетехнически рискови фактори. За тази цел органите за надзор на пазара следва да могат да вземат предвид резултатите от координираните на равнището на Съюза оценки на риска за сигурността на веригите на критични доставки, извършени в съответствие с член 22 от Директива (ЕС) 2022/2555, включително обстоятелства, свързани с нетехнически рискови фактори. ENISA следва да представя на органите за надзор на пазара предложения за категории продукти с цифрови елементи, за които могат да бъдат организирани мащабни проверки, като тези предложения се изготвят, наред с другото, въз основа на получените уведомления за уязвимости и инциденти с продукти.

(115) Като се имат предвид нейният експертен опит и мандат, ENISA следва да може да подкрепя процеса по правоприлагането на настоящия регламент. По-специално, ENISA 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 мащабни проверки. При извънредни обстоятелства ENISA следва да може да извършва по искане на Комисията оценки по отношение на конкретни продукти с цифрови елементи, които представляват значителен киберриск, когато е необходима незабавна намеса за запазване на правилното функциониране на вътрешния пазар.

(116) С настоящия регламент на ENISA се възлагат определени задачи, които изискват подходящи ресурси от гледна точка на експертен опит и на човешки ресурси, за да може ENISA да изпълнява ефективно тези задачи. При изготвянето на проекта за общ бюджет на Съюза Комисията ще предложи бюджетните средства, необходими за щатното разписание на ENISA, в съответствие с процедурата, посочена в член 29 от Регламент (ЕС) 2019/881. По време на тази процедура Комисията ще разгледа общите ресурси на ENISA, за да може тя да изпълнява своите задачи, включително задачите, които са ѝ възложени съгласно настоящия регламент.

(117) С цел да се гарантира, че регулаторната рамка може да бъде адаптирана, когато е необходимо, на Комисията следва да бъде предоставено правомощието да приема актове в съответствие с член 290 от Договора за функционирането на Европейския съюз (ДФЕС) за актуализиране на приложение, съдържащо списък с важните продукти с цифрови елементи. 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 в тях бъде уточнено 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 по европейска схема за сертифициране на киберсигурността за продукти с цифрови елементи и с висока степен на критичност, посочени в приложение към настоящия регламент, както и за актуализиране на списъка на продукти с цифрови елементи с висока степен на критичност въз основа на критериите за критичност, определени в настоящия регламент, и за уточняване на европейските схеми за сертифициране на киберсигурността, приети съгласно Регламент (ЕС) 2019/881, които могат да се използват за доказване на съответствие със съществените изисквания за киберсигурност или с части от тях, посочени в приложение към настоящия регламент.

На Комисията следва също така да бъде делегирано правомощието да приема актове за определяне на минималния период на поддръжка за конкретни категории продукти, когато данните от надзора на пазара предполагат неподходящи периоди на поддръжка, както и за определяне на реда и условията за прилагане на основанията, свързани с киберсигурността, във връзка със забавянето на разпространението на уведомления за активно използвани уязвимости. Освен това на Комисията следва да бъде делегирано правомощието да приема актове за създаване на доброволни програми за удостоверяване на сигурността за оценяване на съответствието на продукти с цифрови елементи, отговарящи на критериите за свободен софтуер с отворен код, с всички или с определени съществени изисквания за киберсигурност или други задължения, предвидени в настоящия регламент, както и за определяне 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[30]. 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. Правомощието да приема делегирани актове съгласно настоящия регламент следва да бъде предоставено на Комисията за срок от пет години, считано от датата на влизане в сила на настоящия регламент. Комисията следва да изготви доклад относно делегирането на правомощия не по-късно от девет месеца преди изтичането на петгодишния срок. Делегирането на правомощия следва да се продължава мълчаливо за срокове с еднаква продължителност, освен ако Европейският парламент или Съветът не възразят срещу подобно продължаване не по-късно от три месеца преди изтичането на всеки срок.

[30] ОВ L 123, 12.5.2016 г., стр. 1.

(118) За да се гарантират еднакви условия за изпълнение на настоящия регламент, на Комисията следва да бъдат предоставени изпълнителни правомощия да определя техническото описание на категориите важни продукти с цифрови елементи, посочени в приложение към настоящия регламент, да уточнява формата и елементите на описа на софтуерните компоненти, да определя допълнително формата и процедурата за уведомленията относно активно използвани уязвимости и сериозни инциденти, които оказват въздействие върху сигурността на продуктите с цифрови елементи, представени от производителите, да установява общи спецификации, обхващащи техническите изисквания, които осигуряват средство за постигане на съответствие със съществените изисквания за киберсигурност, определени в приложение към настоящия регламент, да определя техническите спецификации за етикети, пиктограми или всякакви други знаци, свързани със сигурността на продуктите с цифрови елементи, техния период на поддръжка и механизмите за насърчаване на тяхното използване и за повишаване на обществената осведоменост относно сигурността на продуктите с цифрови елементи, да определя опростената форма на документацията, насочена към нуждите на микропредприятията и малките предприятия, и да взема решения за корективни или ограничителни мерки на равнището на Съюза при извънредни обстоятелства, които оправдават незабавна намеса за запазване на правилното функциониране на вътрешния пазар. Тези правомощия следва да бъдат упражнявани в съответствие с Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета[31].

(119) За да се гарантира основано на доверие 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.

---

[31] 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, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(120) 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 да изисква налагането на административни глоби. Поради това следва да бъдат определени максимални размери на административните глоби, които да бъдат предвидени в националното законодателство 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 най-малкото тези, които са изрично установени в настоящия регламент, включително дали производителят е микропредприятие или малко или средно предприятие, включително новосъздадено предприятие, и дали същите или други органи за надзор на пазара вече са налагали административни глоби на същия икономически оператор за подобни нарушения. Такива обстоятелства биха могли да бъдат утежняващи, когато нарушението на същия икономически оператор продължава да се извършва на територията на 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 икономически оператор за един и същ вид нарушение, следва да гарантира спазването на принципа на пропорционалност. Като се има предвид, че административните глоби не се прилагат за микропредприятия или малки предприятия за неспазване на 24-часовия срок за нотифицирането за ранно предупреждение за активно използвани уязвимости или сериозни инциденти, които оказват въздействие върху сигурността на продукта с цифрови елементи, нито за попечителите на софтуер с отворен код за нарушение на настоящия регламент, и при спазване на принципа, че санкциите следва да бъдат ефективни, пропорционални и възпиращи, държавите членки не следва да налагат други видове имуществени санкции на тези субекти.

(121) При налагане на административни глоби на лице, което не е 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.

(122) Държавите членки следва да проучат, като вземат предвид националните обстоятелства, възможността за използване на приходите от санкциите, предвидени в настоящия регламент, или техния финансов еквивалент в подкрепа на политиките за киберсигурност и за повишаване на равнището на киберсигурност в Съюза, наред с другото чрез увеличаване на броя на квалифицираните специалисти в областта на киберсигурността, укрепване на изграждането на капацитет за микропредприятията и малките и средните предприятия и подобряване на обществената осведоменост относно киберзаплахите.

(123) В отношенията си с трети държави Съюзът 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 има СВП с няколко трети държави. Тези СВП се сключват в редица специфични сектори, които могат да се различават в отделните трети 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 трети 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 Съюза, така и извън него.

(124) Потребителите следва да могат да упражняват правата си във връзка със задълженията, наложени на икономическите оператори съгласно настоящия регламент, чрез представителни искове съгласно Директива (ЕС) 2020/1828 на Европейския парламент и на Съвета[32]. За тази цел в настоящия регламент следва да се предвиди, че Директива (ЕС) 2020/1828 е приложима за представителните искове във връзка с нарушения на настоящия регламент, които увреждат или могат да увредят колективните интереси на потребителите. Поради това приложение I към посочената директива следва да бъде съответно изменено. Държавите членки трябва да гарантират, че тези изменения са отразени в мерките за транспониране, приети съгласно посочената директива, въпреки че приемането на национални мерки за транспониране във връзка с това не е условие за приложимостта на посочената директива по отношение на тези представителни искове. Приложимостта на посочената директива по отношение на представителните искове, предявени във връзка с нарушения от страна на икономически оператори на разпоредбите на настоящия регламент, които нарушения увреждат или биха могли да увредят колективните интереси на потребителите, следва да започне от ... [36 месеца от датата на влизане в сила на настоящия регламент].

(125) Комисията следва периодично да извършва оценка и преглед на настоящия регламент, като се консултира със съответните заинтересовани страни, по-специално с цел установяване на необходимостта от изменения предвид промените в обществените, политическите, технологичните или пазарните условия. Настоящият регламент ще улесни спазването на задълженията за сигурност на веригата на доставки на субектите, попадащи в обхвата на Регламент (ЕС) 2022/2554 и Директива (ЕС) 2022/2555, които използват продукти с цифрови елементи. Комисията следва да оцени, като част от този периодичен преглед, комбинираното въздействие на рамката на Съюза за киберсигурност.

---

[32] Директива (ЕС) 2020/1828 на Европейския парламент и на Съвета от 25 ноември 2020 г. относно представителни искове за защита на колективните интереси на потребителите и за отмяна на Директива 2009/22/ЕО (ОВ L 409, 4.12.2020 г., стр. 1).

(126) На икономическите оператори следва да се предостави достатъчно време, за да се адаптират към изискванията, установени в настоящия регламент. Настоящият регламент следва да се прилага от ... [36 месеца от датата на влизане в сила на настоящия регламент], с изключение на задълженията за докладване относно активно използвани уязвимости и сериозни инциденти, които оказват въздействие върху сигурността на продуктите с цифрови елементи, които следва да се прилагат от ... [21 месеца от датата на влизането в сила на настоящия регламент] и на разпоредбите относно нотифицирането на органи за оценяване на съответствието, които следва да се прилагат от ... [18 месеца от датата на влизането в сила на настоящия регламент].

(127) Важно е да се предостави подкрепа на микропредприятията и малките и средните предприятия, включително новосъздадените предприятия, при прилагането на настоящия регламент и да се сведат до минимум рисковете за изпълнението, произтичащи от липсата на знания и експертен опит на пазара, както и за да се улесни спазването от страна на производителите на техните задължения, определени в настоящия регламент. Програмата „Цифрова Европа“ и други имащи отношение програми на Съюза предоставят финансова и техническа подкрепа, която дава възможност на тези предприятия да допринесат за растежа на икономиката на Съюза и за укрепването на общото ниво на киберсигурност в Съюза. Европейският център за експертни познания в областта на киберсигурността и националните координационни центрове, както и европейските цифрови иновационни центрове, създадени от Комисията и държавите членки на равнището на Съюза или на национално равнище, също биха могли да подкрепят дружествата и организациите от публичния сектор и да допринасят за прилагането на настоящия регламент. В рамките на съответните си мисии и области на компетентност те биха могли да предоставят техническа и научна подкрепа на микропредприятията и малките и средните предприятия, например за дейности по изпитване и оценки на съответствието от трета страна. Те биха могли също така да насърчат внедряването на инструменти с цел улесняване на прилагането на настоящия регламент.

(128) Освен това държавите членки следва да обмислят предприемането на допълващи действия, насочени към предоставяне на насоки и подкрепа за микропредприятията и за малките и средните предприятия, например чрез създаването на регулаторни лаборатории и специални канали за комуникация. За да се повиши нивото на киберсигурност в Съюза, държавите членки могат също така да обмислят предоставянето на подкрепа за развиване на капацитет и умения, свързани с киберсигурността на продукти с цифрови елементи, подобряване на киберустойчивостта на икономическите оператори, по-специално на микропредприятията и малките и средните предприятия, и насърчаване на обществената осведоменост относно киберсигурността на продуктите с цифрови елементи.

(129) 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.

(130) Европейският надзорен орган по защита на данните беше консултиран в съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета[33] и прие становище на 9 ноември 2022 г.[34],

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

---

[33] 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).

[34] ОВ C 452, 29.11.2022 г., стр. 23.

Глава I
Общи разпоредби

Член 1

Предмет

С настоящия регламент се определят:

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

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

в) съществени изисквания за киберсигурност за процесите за отстраняване на уязвимостите, въведени от производителите, за да се гарантира киберсигурността на продуктите с цифрови елементи за времето, през което се очаква продуктите да бъдат в употреба, и задължения за икономическите оператори във връзка с тези процеси;

г) правила за надзор на пазара, включително мониторинг, и прилагане на правилата и изискванията, посочени в настоящия член.

Член 2

Обхват

1. Настоящият регламент се прилага за предоставяните на пазара продукти с цифрови елементи, чието предназначение 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 законодателни 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.

4. Настоящият регламент не се прилага за оборудване, което попада в обхвата на Директива 2014/90/ЕС на Европейския парламент и на Съвета[35].

[35] Директива 2014/90/ЕС на Европейския парламент и на Съвета от 23 юли 2014 г. относно морското оборудване и за отмяна на Директива 96/98/ЕО на Съвета (ОВ L 257, 28.8.2014 г., стр. 146).

5. 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 за киберсигурност, посочени в приложение I, може да бъде ограничено или изключено, когато:

   а) такова ограничаване или изключване е в съответствие с общата регулаторна рамка, която се прилага за тези продукти; и

   б) секторните правила постигат същото или по-високо ниво на защита спрямо предвиденото в настоящия регламент.

   На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 61, за да допълва настоящия регламент, като посочва дали е необходимо такова ограничение или изключване, съответните продукти и правила, както и обхвата на ограничението, ако е приложимо.

6. Настоящият регламент не се прилага за резервни части, които се предоставят на пазара за замяна на идентични компоненти в продукти с цифрови елементи и които са произведени съгласно същите спецификации като компонентите, които са предназначени да заменят.

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

8. Задълженията, предвидени в настоящия регламент, не водят до предоставянето на информация, разкриването на която противоречи на основните интереси на държавите членки, свързани с националната сигурност, обществената сигурност или отбраната.

Член 3

Определения

За целите на настоящия регламент се прилагат следните определения:

1) „продукт с цифрови елементи“ означава софтуерен или хардуерен продукт и неговите решения за обработване на данни от разстояние, включително софтуерни или хардуерни компоненти, пускани на пазара поотделно;

2) „обработване на данни от разстояние“ означава 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) „киберсигурност“ означава киберсигурност съгласно определението в член 2, точка 1 от Регламент (ЕС) 2019/881;

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

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

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

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

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

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

10) „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;

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

12) „икономически оператор“ означава производителят, упълномощеният представител, вносителят, дистрибуторът или друго физическо или юридическо лице, на което са наложени задължения във връзка с производството на продукти с цифрови елементи или предоставянето на пазара на продукти с цифрови елементи в съответствие с настоящия регламент;

13) „производител“ означава 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, с цел печалба или безвъзмездно;

14) „попечител на софтуер с отворен код“ означава юридическо лице, различно от производител, което има за цел системно да предоставя устойчива подкрепа за разработването на конкретни продукти с цифрови елементи, отговарящи на критериите за свободен софтуер с отворен код и предназначени за търговски дейности, и което гарантира жизнеспособността на тези продукти;

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

16) „вносител“ означава 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;

17) „дистрибутор“ означава 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;

18) „потребител“ означава физическо лице, извършващо действия за цели, които са извън сферата на търговската или стопанската дейност, занаята или професията на това лице;

19) „микропредприятия“, „малки предприятия“ и „средни предприятия“ означава съответно микропредприятия, малки предприятия и средни предприятия съгласно определението в приложението към Препоръка 2003/361/ЕО на Комисията;

20) „период на поддръжка“ означава периодът, през който от производителя се изисква да гарантира, че уязвимостите на продукт с цифрови елементи се отстраняват ефективно и в съответствие със съществените изисквания за киберсигурност, посочени в приложение I, част II;

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

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

23) „предназначение“ означава употребата, за която производителят е предназначил даден продукт с цифрови елементи, включително специфичният контекст и условия на употреба, посочени в информацията, предоставена от производителя в инструкциите за употреба, рекламните или търговските материали и декларации, както и в техническата документация;

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

25) „разумно предвидима неправилна употреба“ означава употреба на продукт с цифрови елементи по начин, който не е в съответствие с неговото предназначение, но който е възможно да е резултат от разумно предвидимо човешко поведение или от взаимодействие с други системи;

26) „нотифициращ орган“ означава националният орган, отговарящ за въвеждането и провеждането на необходимите процедури за оценяване, определяне и нотифициране на органи за оценяване на съответствието и за тяхното наблюдение;

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

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

29) „нотифициран орган“ означава орган за оценяване на съответствието, определен съгласно член 43 и друго приложимо законодателство на Съюза за хармонизация;

30) „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 за киберсигурност, определени в приложение I, част I, или която води до промяна на предназначението, за което е оценен продуктът с цифрови елементи;

31) „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 за киберсигурност, определени в приложение I, и с друго приложимо законодателство на Съюза за хармонизация, в което се предвижда нейното нанасяне;

32) „законодателство на Съюза за хармонизация“ означава законодателството на Съюза, посочено в приложение I към Регламент (ЕС) 2019/1020, и всяко друго законодателство на Съюза, с което се хармонизират условията за предлагане на пазара на продукти, по отношение на които се прилага посоченият регламент;

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

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

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

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

37) „киберриск“ означава възможността за загуби или смущения в резултат на инцидент и се изразява като комбинация от мащаба на загубата или смущението и вероятността за настъпване на инцидента;

38) „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;

39) „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;

40) „уязвимост“ означава слабост, податливост или недостатък на продукт с цифрови елементи, които могат да бъдат използвани при киберзаплаха;

41) „уязвимост, която може да бъде използвана“ означава уязвимост, която има потенциала да бъде ефективно използвана от противник при практически оперативни условия;

42) „активно използвана уязвимост“ означава уязвимост, за която има надеждни доказателства, че злонамерен участник я е използвал в система без разрешението на собственика на системата;

43) „инцидент“ означава инцидент съгласно определението в член 6, точка 6 от Директива (ЕС) 2022/2555;

44) „инцидент, който оказва въздействие върху сигурността на продукта с цифрови елементи“ означава инцидент, който оказва отрицателно въздействие или може да окаже отрицателно въздействие върху способността на продукт с цифрови елементи да защитава наличността, автентичността, целостта или поверителността на данни или функции;

45) „ситуация, близка до инцидент“ означава ситуация, близка до инцидент, съгласно определението в член 6, точка 5 от Директива (ЕС) 2022/2555;

46) „киберзаплаха“ означава киберзаплаха съгласно определението в член 2, точка 8 от Регламент (ЕС) 2019/881;

47) „лични данни“ означава лични данни съгласно определението в член 4, точка 1 от Регламент (ЕС) 2016/679;

48) „свободен софтуер с отворен код“ означава софтуер, чийто изходен код е свободно споделян и който се предоставя чрез свободен лиценз с отворен код, предоставящ всички права, които го правят свободно достъпен, използваем, модифицируем и преразпределяем;

49) „изземване“ означава изземване съгласно определението в член 3, точка 22 от Регламент (ЕС) 2019/1020;

50) „изтегляне“ означава изтегляне съгласно определението в член 3, точка 23 от Регламент (ЕС) 2019/1020;

51) „определен за координатор ЕРИКС“ означава определен за координатор ЕРИКС съгласно член 12, параграф 1 от Директива (ЕС) 2022/2555.

Член 4

Свободно движение

1. Държавите членки не възпрепятстват по отношение на въпросите, 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, демонстрации или други подобни събития държавите членки не възпрепятстват представянето или използването на продукт с цифрови елементи, който не отговаря на изискванията на настоящия регламент, включително негови прототипи, при условие, че продуктът се представя с видим знак, който ясно показва, че продуктът не съответства на настоящия регламент и няма да се предоставя на пазара, докато не бъде приведен в съответствие с настоящия регламент.

3. Държавите членки не възпрепятстват предоставянето на пазара 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 изпитване, и с видим знак, който ясно показва, че той не съответства на настоящия регламент и няма да се предоставя на пазара за цели, различни от изпитване.

4. Параграф 3 не се прилага за предпазните устройства, посочени в законодателството на Съюза за хармонизация, различно от настоящия регламент.

Член 5

Обществени поръчки или използване на продукти с цифрови елементи

1. Настоящият регламент не възпрепятства държавите членки да установяват за продуктите с цифрови елементи допълнителни изисквания за киберсигурност при възлагането на обществени поръчки или използването на тези продукти за конкретни цели, включително когато тези продукти се предоставят чрез обществени поръчки за целите на националната сигурност или отбрана или се използват за целите на националната сигурност или отбрана, при условие че такива изисквания са в съответствие със задълженията на държавите членки, установени в правото на Съюза, и са необходими и пропорционални за постигането на посочените цели.

2. Без да се засягат директиви 2014/24/ЕС и 2014/25/ЕС, когато се възлагат обществени поръчки за продукти с цифрови елементи, които попадат в обхвата на настоящия регламент, държавите членки гарантират, че в процеса на възлагане на обществени поръчки се взема предвид съответствието със съществените изисквания за киберсигурност, определени в приложение I към настоящия регламент, включително способността на производителите да се справят ефективно с уязвимости.

Член 6

Изисквания за продукти с цифрови елементи

Продукти с цифрови елементи се предоставят на пазара само ако:

а) при правилно инсталиране, извършване на техническа поддръжка и използване по предназначение или при разумно предвидими условия, и когато е приложимо, при инсталиране на необходимите актуализации за сигурност, отговарят на съществените изисквания за киберсигурност, определени в приложение I, част I; и

б) въведените от производителя процеси отговарят на съществените изисквания за киберсигурност, определени в приложение I, част II.

Член 7

Важни продукти с цифрови елементи

1. Продуктите с цифрови елементи, които имат основната функционална възможност на дадена продуктова категория, определена в приложение III, се считат за важни продукти с цифрови елементи и подлежат на процедурите за оценяване на съответствието, посочени в член 32, параграфи 2 и 3. Интегрирането на продукт с цифрови елементи, който има основната функционална възможност на дадена продуктова категория, определена в приложение III, само по себе си не води до това продуктът, в който е интегриран, да подлежи на процедурите за оценяване на съответствието, посочени в член 32, параграфи 2 и 3.

2. Категориите продукти с цифрови елементи, посочени в параграф 1 от настоящия член, разделени на класове I и II съгласно определеното в приложение III, отговарят на поне един от следните критерии:

а) продуктът с цифрови елементи изпълнява предимно функции от критично значение за киберсигурността на други продукти, мрежи или услуги, включително осигуряване на удостоверяване на автентичност и достъп, предотвратяване и установяване на проникване, сигурност на крайните точки или защита на мрежата;

б) продуктът с цифрови елементи изпълнява функция, която носи значителен риск от неблагоприятни последици поради своята интензивност и способност за нарушаване, контрол или причиняване на вреди на голям брой други продукти или на здравето, сигурността или безопасността на своите ползватели чрез пряко манипулиране, като например функция на централна система, включително управление на мрежата, контрол на конфигурацията, виртуализация или обработка на лични данни.

3. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 61 за изменение на приложение III чрез включване в списъка на нова категория в рамките на всеки клас от категориите продукти с цифрови елементи и уточняване на нейното определение, преместване на категория продукти от един клас в друг или оттегляне на съществуваща категория от този списък. Когато оценява необходимостта от изменение на списъка, съдържащ се в приложение III, Комисията взема предвид свързаните с киберсигурността функционални възможности или функцията и нивото на киберриска, пораждан от продуктите с цифрови елементи, както е установено в критериите, посочени в параграф 2 от настоящия член.

В делегираните актове, посочени в първа алинея от настоящия параграф, се предвижда, когато е подходящо, минимален преходен период от 12 месеца, по-специално когато нова категория важни продукти с цифрови елементи се добавя към клас I или II или се премества от клас I в клас II, както е посочено в приложение III, преди да започнат да се прилагат необходимите процедури за оценяване на съответствието, както са посочени в член 32, параграфи 2 и 3, освен ако поради наложителни причини за спешност е обоснован по-кратък преходен период.

4. До ... [12 месеца от датата на влизане в сила на настоящия регламент] Комисията приема акт за изпълнение, с който се определя техническото описание на категориите продукти с цифрови елементи от класове I и II, определени в приложение III, и техническото описание на категориите продукти с цифрови елементи, определени в приложение IV. Този акт за изпълнение се приема в съответствие с процедурата по разглеждане, посочена в член 62, параграф 2.

Член 8

Критични продукти с цифрови елементи

1. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 61 за допълване на настоящия регламент, за да определи за кои продукти с цифрови елементи, които имат основната функционална възможност на дадена продуктова категория, определена в приложение IV към настоящия регламент, има изискване да получат европейски сертификат за киберсигурност поне с ниво на увереност „съществено“ съгласно европейска схема за сертифициране на киберсигурност, приета съгласно Регламент (ЕС) 2019/881, за да се докаже съответствието със съществените изисквания за киберсигурност, определени в приложение I към настоящия регламент, или части от тях, при условие че съгласно Регламент (ЕС) 2019/881 е приета европейска схема за сертифициране на киберсигурността, обхващаща тези категории продукти с цифрови елементи, която е на разположение на производителите. В тези делегирани актове се определя изискваното ниво на увереност, което е пропорционално на нивото на киберриска, свързан с продуктите с цифрови елементи, и се взема предвид предназначението им, включително критичната зависимост от тях на съществените субекти, както са посочени в член 3, параграф 1 от Директива (ЕС) 2022/2555.

Преди приемането на такива делегирани актове Комисията извършва оценка на потенциалното въздействие на предвидените мерки върху пазара и провежда консултации със съответните заинтересовани страни, включително Европейската група за сертифициране на киберсигурността, създадена съгласно Регламент (ЕС) 2019/881. При оценката се вземат предвид готовността и равнището на капацитет на държавите членки за прилагането на съответната европейска схема за сертифициране на киберсигурността. Когато не са приети делегирани актове, както е посочено в първа алинея от настоящия параграф, продуктите с цифрови елементи, които имат основната функционална възможност на дадена продуктова категория, определена в приложение IV, подлежат на процедурите за оценяване на съответствието, посочени в член 32, параграф 3.

В делегираните актове, посочени в първа алинея, се предвижда минимален преходен период от шест месеца, освен ако поради наложителни причини за спешност е обоснован по-кратък преходен период.

2. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 61 за изменение на приложение IV чрез добавяне или оттегляне на категории критични продукти с цифрови елементи. При определянето на тези категории критични продукти с цифрови елементи и на изискваното ниво на увереност в съответствие с параграф 1 от настоящия член Комисията взема предвид критериите, посочени в член 7, параграф 2, и гарантира, че категориите продукти с цифрови елементи отговарят на поне един от следните критерии:

а) налице е критична зависимост на съществените субекти, както са посочени в член 3 от Директива (ЕС) 2022/2555, от категорията продукти с цифрови елементи;

б) инцидентите и използваните уязвимости във връзка с категорията продукти с цифрови елементи биха могли да предизвикат сериозни смущения на критичните вериги на доставки в рамките на вътрешния пазар.

Преди да приеме такива делегирани актове, Комисията извършва оценка на вида, посочен в параграф 1.

В делегираните актове, посочени в първа алинея, се предвижда минимален преходен период от шест месеца, освен ако поради наложителни причини за спешност е обоснован по-кратък преходен период.

Член 9

Консултации със заинтересованите страни

1. При изготвянето на мерки за прилагането на настоящия регламент Комисията се консултира със съответните заинтересовани страни и взема предвид становищата на тези заинтересовани страни, като например съответните органи на държавите членки, предприятия от частния сектор, включително микропредприятия и малки и средни предприятия, общността, разработваща софтуер с отворен код, асоциациите на потребителите, академичните среди и съответните агенции и органи на Съюза, както и експертните групи, създадени на равнището на Съюза. По-специално, когато е целесъобразно, Комисията се консултира и търси становищата на тези заинтересовани страни по структуриран начин, когато:

   а) изготвя насоките, посочени в член 26;

   б) изготвя техническите описания на категориите продукти, определени в приложение III, в съответствие с член 7, параграф 4, извършва оценка на необходимостта от потенциални актуализации на списъка на категориите продукти в съответствие с член 7, параграф 3 и член 8, параграф 2 или извършва оценка на потенциалното въздействие върху пазара, посочена в член 8, параграф 1, без да се засяга член 61;

   в) извършва подготвителна работа за оценката и прегледа на настоящия регламент.

2. Комисията организира редовни консултации и информационни сесии поне веднъж годишно, за да получи мненията на заинтересованите страни, посочени в параграф 1, относно прилагането на настоящия регламент.

Член 10

Повишаване на уменията в киберустойчива цифрова среда

За целите на настоящия регламент и за да се отговори на нуждите на специалистите в подкрепа на прилагането на настоящия регламент, държавите членки, когато е целесъобразно, с подкрепата на Комисията, Европейския център за експертни познания в областта на киберсигурността и ENISA, при пълно зачитане на компетентността на държавите членки в областта на образованието, насърчават мерки и стратегии, насочени към:

а) развиване на умения в областта на киберсигурността и създаване на организационни и технологични инструменти, за да се гарантира достатъчна наличност на квалифицирани специалисти в подкрепа на дейностите на органите за надзор на пазара и органите за оценяване на съответствието;

б) засилване на сътрудничеството между частния сектор, икономическите оператори, включително чрез преквалификация или повишаване на квалификацията на служителите на производителите, потребителите, доставчиците на обучение, както и на публичните администрации, като се разширяват възможностите за достъп на младите хора до работни места в сектора на киберсигурността.

Член 11

Обща безопасност на продуктите

Чрез дерогация от член 2, параграф 1, трета алинея, буква б) от Регламент (ЕС) 2023/988, глава III, раздел 1, глави V и VII и глави IX—XI от посочения регламент се прилагат за продукти с цифрови елементи по отношение на аспектите и рисковете или категориите рискове, които не са обхванати от настоящия регламент, когато тези продукти не са предмет на специфични изисквания, установени в друго законодателство на Съюза за хармонизация, както е определено в член 3, точка 27 от Регламент (ЕС) 2023/988.

Член 12

Високорискови системи с ИИ

1. Без да се засягат изискванията, свързани с точността и надеждността, определени в член 15 на Регламент (ЕС) 2024/1689, продуктите с цифрови елементи, които попадат в обхвата на настоящия регламент и са класифицирани като високорискови системи с ИИ съгласно член 6 от посочения регламент, се счита, че съответстват на изискванията за киберсигурност, определени в член 15 от посочения регламент, ако:

   а) тези продукти отговарят на съществените изисквания за киберсигурност, определени в приложение I, част I;

б) въведените от производителя процеси отговарят на съществените изисквания за киберсигурност, определени в приложение I, част II; и

в) постигането на нивото на защита на киберсигурността, изисквано съгласно член 15 от Регламент (ЕС) 2024/1689 е доказано в ЕС декларацията за съответствие, издадена съгласно настоящия регламент.

2. По отношение на продуктите с цифрови елементи и изискванията за киберсигурност, посочени в параграф 1 от настоящия член, се прилага съответната процедура за оценяване на съответствието, предвидена в член 43 от Регламент (ЕС) 2024/1689. За целите на това оценяване нотифицираните органи, които са компетентни да проверяват съответствието на високорисковите системи с ИИ съгласно Регламент (ЕС) 2024/1689, са компетентни също така да проверяват съответствието на високорисковите системи с ИИ, които попадат 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 39 от настоящия регламент, е било оценено в контекста на процедурата за нотифициране съгласно Регламент (ЕС) 2024/1689.

3. Чрез дерогация от параграф 2 от настоящия член, важни продукти с цифрови елементи, изброени в приложение III към настоящия регламент, които подлежат на процедурите за оценяване на съответствието, посочени в член 32, параграф 2, букви а) и б) и член 32, параграф 3 от настоящия регламент, и критични продукти с цифрови елементи, посочени в приложение IV към настоящия регламент, за които се изисква да бъде получен европейски сертификат за киберсигурност съгласно член 8, параграф 1 от настоящия регламент, или, при липсата на такъв, които подлежат на процедурите за оценяване на съответствието, посочени в член 32, параграф 3 от настоящия регламент, и които също така са класифицирани като високорискови системи с ИИ съгласно член 6 от Регламент (ЕС) 2024/1689 и за които се прилага процедурата за оценяване на съответствието, основана на вътрешен контрол, посочена в приложение VI към Регламент (ЕС) 2024/1689, подлежат на процедурите за оценяване на съответствието, предвидени в настоящия регламент, доколкото това се отнася до съществените изисквания за киберсигурност, определени в настоящия регламент.

4. Производителите на продукти с цифрови елементи, посочени в параграф 1 от настоящия член, могат да участват в регулаторните лаборатории в областта на ИИ, посочени в член 57 от Регламент (ЕС) 2024/1689.

Глава II

Задължения на икономическите оператори и разпоредби относно свободния софтуер с отворен код

Член 13

Задължения на производителите

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

2. За целите на изпълнението на 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 и свеждане до минимум на последиците от такива инциденти, включително по отношение на здравето и безопасността на ползвателите.

3. Оценката на киберриска се документира и актуализира по целесъобразност по време на период на поддръжка, който се определя в съответствие с параграф 8 от настоящия член. Тази оценка на киберриска включва най-малко анализ на киберрисковете въз основа на предназначението и разумно предвидимата употреба, както и на условията за употреба на продукта с цифрови елементи, например оперативната среда или активите, които трябва да бъдат защитени, като се взема предвид продължителността, през която се очаква продуктът да бъде в употреба. В оценката на киберриска се посочва дали и по какъв начин изискванията за сигурност, определени в приложение I, част I, точка 2, са приложими за съответния продукт с цифрови елементи и как тези изисквания се прилагат въз основа на оценката на киберриска. В нея също така се посочва как производителят трябва да прилага приложение I, част I, точка 1 и изискванията за отстраняване на уязвимости, определени в приложение I, част II.

4. При пускането на пазара на продукт с цифрови елементи производителят включва оценката на киберриска, посочена в параграф 3 от настоящия член, в техническата документация, изисквана съгласно член 31 и приложение VII. По отношение на продуктите с цифрови елементи, както са посочени в член 12, които са предмет и на други правни актове на Съюза, оценката на киберриска може да бъде част от оценката на риска, изисквана от тези съответни правни актове на Съюза. Когато някои съществени изисквания за киберсигурност не са приложими към продукта с цифрови елементи, производителят включва ясна обосновка за това в тази техническа документация.

5. За целите на спазването на параграф 1 производителите полагат дължимата грижа, когато интегрират компоненти, доставени от трети страни, така че тези компоненти не застрашават киберсигурността на продукта с цифрови елементи, включително когато интегрират компоненти на свободен софтуер с отворен код, които не са били предоставени на пазара в процеса на търговска дейност.

6. 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 произвежда или поддържа компонента, и разглеждат и отстраняват уязвимостта в съответствие с изискванията за отстраняване на уязвимости, посочени в приложение I, част II. Когато производителите са разработили изменение на софтуера или хардуера за справяне с уязвимостта в този компонент, те споделят съответния код или документация с лицето или субекта, който произвежда или поддържа компонента, по целесъобразност в машинночетим формат.

7. Производителите систематично документират — по начин, който е пропорционален на естеството и киберрисковете, съответните аспекти на киберсигурността, отнасящи се до продуктите с цифрови елементи, включително уязвимостите, за които са узнали, и всяка информация от значение, предоставена от трети страни, и когато е приложимо, актуализират оценката на киберриска на продуктите.

8. При пускането на даден продукт с цифрови елементи на пазара и за периода на поддръжка производителите гарантират, че уязвимостите на този продукт, включително неговите компоненти, се отстраняват ефективно и в съответствие със съществените изисквания за киберсигурност, определени в приложение I, част II.

Производителите определят периода на поддръжка, така че той да отразява продължителността, през която се очаква продуктът да бъде в употреба, като вземат предвид по-специално разумните очаквания на ползвателите, естеството на продукта, включително неговото предназначение, както и съответното право на Съюза, определящо жизнения цикъл на продуктите с цифрови елементи. При определянето на периода на поддръжка производителите могат също така да вземат предвид периодите на поддръжка на продукти с цифрови елементи, които предлагат сходна функционалност, пуснати на пазара от други производители, наличието на оперативната среда, периодите на поддръжка на интегрираните компоненти, които предоставят основни функции и са с произход от трети държави, както и съответните насоки, предоставени от специализираната група за административно сътрудничество (ADCO група), създадена съгласно член 52, параграф 15, и от Комисията. Въпросите, които трябва да се вземат предвид, за да се определи периода на поддръжка се разглеждат по начин, който гарантира пропорционалност.

Без да се засяга втора алинея, периодът на поддръжка е най-малко пет години. Ако се очаква продуктът с цифрови елементи да се използва по-малко от пет години, периодът на поддръжка съответства на очакваното време за използване.

Като взема предвид препоръките на ADCO групата, посочени в член 52, параграф 16, Комисията може да приема делегирани актове в съответствие с член 61, за да допълва настоящия регламент като определя минималния период на поддръжка за конкретни категории продукти, когато данните от надзора на пазара сочат, че периодите на поддръжка са неподходящи.

Производителите включват в техническата документация информацията, която е била взета предвид за определяне на периода на поддръжка на продукт с цифрови елементи, както е посочено в приложение VII.

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

9. Производителите гарантират, че всяка актуализация за сигурност, посочена в приложение I, част II, точка 8, която е била предоставена на ползвателите по време на периода на поддръжка, остава на разположение след издаването ѝ в продължение на най-малко 10 години или за остатъка от периода на поддръжка, в зависимост от това кой период е по-дълъг.

10. Когато производител е пуснал на пазара последващи съществено изменени версии на софтуерен продукт, този производител може да гарантира съответствие със съществената изискване за киберсигурност, определено в приложение I, част II, точка 2, само за версията, която производителят последно е пуснал на пазара, при условие че ползвателите на версиите, които преди това са били пуснати на пазара, имат безплатен достъп до последната версия, пусната на пазара, и не се налага да правят допълнителни разходи за коригиране на хардуерната и софтуерната среда, в която използват първоначалната версия на този продукт.

11. Производителите могат да поддържат публични софтуерни архиви, подобряващи достъпа на ползвателите до предишни версии. В тези случаи ползвателите се информират ясно и по леснодостъпен начин за рисковете, свързани с използването на неподдържан софтуер.

12. Преди да пуснат даден продукт с цифрови елементи на пазара, производителите изготвят техническата документация, посочена в член 31.

Те извършват или възлагат извършването на избраните процедури за оценяване на съответствието, както са посочени в член 32.

Когато чрез тази процедура за оценяване на съответствието е доказано съответствието на продукта с цифрови елементи със съществените изисквания за киберсигурност, определени в приложение I, част I, и на въведените от производителя процеси със съществените изисквания за киберсигурност, определени в приложение I, част II, производителите изготвят ЕС декларацията за съответствие съгласно член 28 и поставят маркировката „CE“ съгласно член 30.

13. Производителите съхраняват техническата документация и ЕС декларацията за съответствие на разположение на органите за надзор на пазара в продължение най-малко на 10 години след пускането на пазара на продукта с цифрови елементи или за периода на поддръжка, в зависимост от това кой период е по-дълъг.

14. Производителите гарантират, че съществуват процедури, чрез които продуктите с цифрови елементи, които са обект на серийно производство, остават в съответствие с настоящия регламент. Производителите вземат 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, както са посочени в член 27, чрез позоваване на които се декларира съответствието на продукта с цифрови елементи или чрез прилагане на които се проверява неговото съответствие.

15. Производителите гарантират, че върху техните продукти с цифрови елементи е нанесен типът, партидният или серийният номер или друг елемент, който позволява тяхната идентификация, или когато това не е възможно, че тази информация е представена върху тяхната опаковка или в документ, който придружава продукта с цифрови елементи.

16. Производителите посочват името, регистрираното търговско наименование или регистрираната търговска марка на производителя, както и пощенския адрес, адреса на електронна поща или други цифрови координати за връзка, а също и — когато е приложимо, уебсайта, на които може да се осъществи връзка с производителя, върху продукта с цифрови елементи, върху неговата опаковка или в документ, който придружава продукта с цифрови елементи. Тази информация се включва и в информацията и указанията за ползвателя, предвидени в приложение II. Данните за връзка са на език, който е лесноразбираем за ползвателите и органите за надзор на пазара.

17. За целите на настоящия регламент производителите определят единно звено за контакт, което да дава възможност на ползвателите да комуникират пряко и бързо с тях, включително за да се улесни докладването относно уязвимости на продукта с цифрови елементи.

Производителите гарантират, че единното звено за контакт е лесно разпознаваемо от ползвателите. Те включват и единното звено за контакт в информацията и указанията за ползвателя, посочени в приложение II.

Единното звено за контакт позволява на ползвателите да избират предпочитаните от тях средства за комуникация и не ограничава тези средства до автоматизирани инструменти.

18. Производителите гарантират, че продуктите с цифрови елементи се придружават от информацията и инструкциите за ползвателя, посочени в приложение II, на хартиен или електронен носител. Тази информация и инструкции се предоставят на език, който е лесноразбираем за ползвателите и органите за надзор на пазара. Те трябва да са ясни, разбираеми, смислени и четливи. Те позволяват сигурно инсталиране, експлоатация и използване на продуктите с цифрови елементи. Производителите съхраняват информацията и инструкциите за ползвателя, посочени в приложение II, на разположение на ползвателите и органите за надзор на пазара в продължение най-малко на 10 години след пускането на пазара на продукта с цифрови елементи или за периода на поддръжка, в зависимост от това кой период е по-дълъг. Когато тази информация и инструкции се предоставят онлайн, производителите гарантират, че те са достъпни, лесни за ползване и достъпни онлайн в продължение най-малко на 10 години след пускането на пазара на продукта с цифрови елементи или за периода на поддръжка, в зависимост от това кой период е по-дълъг.

19. Производителите гарантират, че крайната дата на периода на поддръжка, посочен в параграф 8, включително най-малко месецът и годината, е ясно и разбираемо посочена в момента на покупката по леснодостъпен начин и когато е приложимо, върху продукта с цифрови елементи, неговата опаковка или чрез цифрови средства.

Когато това е технически осъществимо с оглед на естеството на продукта с цифрови елементи, производителите показват нотификация до ползвателите, с която ги информират, че техният продукт с цифрови елементи е достигнал края на своя период на поддръжка.

20. Производителите предоставят копие от ЕС декларацията за съответствие или опростена ЕС декларация за съответствие заедно с продукта с цифрови елементи. Когато се представя опростена ЕС декларация за съответствие, тя съдържа точния интернет адрес, на който може да бъде намерен пълният текст на декларацията за съответствие с изискванията на ЕС.

21. От пускането на пазара и за периода на поддръжка 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 за киберсигурност, 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.

22. При мотивирано искане от страна на орган за надзор на пазара производителите предоставят на този орган, на лесноразбираем за този орган 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 за киберсигурност, определени в приложение I. Производителите 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.

23. Производител, който прекратява дейността си и в резултат на това не е в състояние да спази настоящия регламент, информира, преди прекратяването на дейностите да влезе в сила, съответните органи за надзор на пазара, както и, с всички налични средства и доколкото е възможно, ползвателите на съответните продукти с цифрови елементи, пуснати на пазара, за предстоящото прекратяване на дейностите.

24. Чрез актове за изпълнение, при които се вземат предвид европейските или международните стандарти и най-добри практики, Комисията може да определи формата и елементите на описа на софтуерните компоненти, посочен в приложение I, част II, точка 1. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 62, параграф 2.

25. За да се оцени зависимостта на държавите членки и на Съюза като цяло от софтуерни компоненти, по-специално от компоненти, квалифицирани като свободен софтуер с отворен код, ADCO групата може да реши да извърши оценка на зависимостта в целия Съюз за конкретни категории продукти с цифрови елементи. За тази цел органите за надзор на пазара могат да поискат от производителите на такива категории продукти с цифрови елементи да предоставят съответните описи на софтуерните компоненти, както е посочено в приложение I, част II, точка 1. Въз основа на тази информация органите за надзор на пазара могат да предоставят на ADCO групата анонимизирана и обобщена информация за софтуерните зависимости. ADCO групата представя доклад относно резултатите от оценката на зависимостта на групата за сътрудничество, създадена съгласно член 14 от Директива (ЕС) 2022/2555.

Член 14

Задължения на производителите за отчет

1. Производителят нотифицира едновременно определения за координатор ЕРИКС, в съответствие с параграф 7 от настоящия член, и ENISA, за всяка активно използвана уязвимост, съдържаща се в продукта с цифрови елементи, за която е узнал. Производителят нотифицира тази активно използвана уязвимост чрез единната платформа за докладване, създадена съгласно член 16.

2. За целите на нотификацията, посочена в параграф 1, производителят представя:

   а) нотификация за ранно предупреждение за активно използвана уязвимост, без ненужно забавяне и при всички случаи в рамките на 24 часа, след като производителят е узнал за нея, като се посочват, когато е приложимо, държавите членки, за които производителят знае, че на тяхна територия е предоставен продуктът му с цифрови елементи;

б) освен ако съответната информация вече не е била предоставена — нотификация за уязвимост, без ненужно забавяне и при всички случаи в рамките на 72 часа, след като производителят е узнал за активно използваната уязвимост, в която се предоставя обща информация, каквато е налична, относно съответния продукт с цифрови елементи, общия характер на използването и на съответната уязвимост, както и предприетите коригиращи или смекчаващи мерки и коригиращите или смекчаващите мерки, които ползвателите могат да предприемат, и в която също така се посочва, когато е приложимо, доколко чувствителна е според производителя нотифицираната информация;

в) освен ако съответната информация вече не е била предоставена, окончателен доклад, не по-късно от 14 дни, след като коригираща или смекчаваща мярка стане налична, включващ най-малко следното:

i) описание на уязвимостта, включително нейната сериозност и въздействие;

ii) когато е налична, информация относно всеки злонамерен участник, който е използвал или използва уязвимостта;

iii) подробности относно актуализацията за сигурност или други корективни мерки, които са били предоставени за отстраняване на уязвимостта.

3. Производителят нотифицира едновременно на ЕРИКС, който е определен за координатор в съответствие с параграф 7 от настоящия член, и на ENISA, всеки сериозен инцидент, за който е узнал, който оказва въздействие върху сигурността на продукта с цифрови елементи. Производителят нотифицира този инцидент чрез единната платформа за докладване, създадена съгласно член 16.

4. За целите на нотификацията, посочена в параграф 3, производителят представя:

а) нотификация за ранно предупреждение за сериозен инцидент, който оказва въздействие върху сигурността на продукта с цифрови елементи, без ненужно забавяне и при всички случаи в рамките на 24 часа, след като производителят е узнал за него, включително най-малко дали има съмнение, че инцидентът е причинен от незаконни или злонамерени действия, като в нотификацията се посочват, когато е приложимо, държавите членки, за които производителят знае, че на тяхна територия е предоставен продуктът му с цифрови елементи;

б) освен ако съответната информация вече не е била предоставена – нотификация за инцидент, без ненужно забавяне и при всички случаи в рамките на 72 часа, след като производителят е узнал за инцидента, в която се предоставя обща информация, ако е налична, относно естеството на инцидента, първоначална оценка на инцидента, както и предприетите коригиращи или смекчаващи мерки и коригиращите или смекчаващите мерки, които ползвателите могат да предприемат, и в която също така се посочва, когато е приложимо, доколко чувствителна е според производителя нотифицираната информация;

в) освен ако съответната информация вече не е била предоставена, окончателен доклад, в рамките на един месец след подаването на нотификацията за инцидента съгласно буква б), включващ най-малко следното:

i) подробно описание на инцидента, включително неговата тежест и въздействие;

ii) вида на заплахата или първопричината, която вероятно е породила инцидента;

iii) приложените и текущите смекчаващи мерки.

5. За целите на параграф 3 инцидент, който оказва въздействие върху сигурността на продукта с цифрови елементи, се счита за сериозен, когато:

а) оказва отрицателно въздействие или може да окаже отрицателно въздействие върху способността на продукт с цифрови елементи да защитава наличността, автентичността, целостта или поверителността на чувствителни или важни данни или функции; или

б) е довел или е в състояние да доведе до въвеждането или изпълнението на злонамерен код в продукт с цифрови елементи или в мрежовите и информационните системи на ползвател на продукта с цифрови елементи.

6. Когато е необходимо, определеният за координатор ЕРИКС, първоначално получаващ нотификацията, може да поиска от производителите да предоставят междинен доклад за съответните актуализации на ситуацията с активно използваната уязвимост или сериозния инцидент, който оказва въздействие върху сигурността на продукта с цифрови елементи.

7. Нотификациите, посочени в параграфи 1 и 3 от настоящия член, се подават чрез единната платформа за докладване, посочена в член 16, като се използва една от крайните точки за електронно нотифициране, посочени в член 16, параграф 1. Нотификацията се подава, като се използва крайната точка за електронно нотифициране на определения за координатор ЕРИКС на държавата членка, в която се намира основното място на установяване на производителите в Съюза, и едновременно с това е достъпно за ENISA.

За целите на настоящия регламент се счита, че основното място на установяване в Съюза на даден производител е в държавата членка, в която преимуществено се вземат решенията, свързани с киберсигурността на неговите продукти с цифрови елементи. Ако такава държава членка не може да бъде определена, за основно място на установяване се счита държавата членка, в която съответният производител има място на установяване с най-големия брой служители в Съюза.

Когато даден производител няма основно място на установяване в Съюза, той подава нотификациите, посочени в параграфи 1 и 3, като използва крайната точка за електронно нотифициране на определения за координатор ЕРИКС в държавата членка, определена съгласно следния ред и въз основа на информацията, с която разполага производителят:

а) държавата членка, в която е установен упълномощеният представител, действащ от името на производителя за най-голям брой продукти с цифрови елементи на този производител;

б) държавата членка, в която е установен вносителят, който пуска на пазара най-голям брой продукти с цифрови елементи на този производител;

в) държавата членка, в която е установен дистрибуторът, който предоставя на пазара най-голям брой продукти с цифрови елементи на този производител;

г) държавата членка, в която се намират най-много ползватели на продукти с цифрови елементи на този производител.

Във връзка с трета алинея, буква г) производителят може да подава нотификации, свързани с всяка последваща активно използвана уязвимост или сериозен инцидент, който оказва въздействие върху сигурността на продукта с цифрови елементи, на същия определен за координатор ЕРИКС, на който е докладвал за първи път.

8. След като узнае за активно използвана уязвимост или сериозен инцидент, който оказва въздействие върху сигурността на продукт с цифрови елементи, производителят информира засегнатите ползватели на продукта с цифрови елементи и, когато е подходящо, всички ползватели за тази уязвимост или инцидент, и, когато е необходимо, за всички мерки за намаляване на риска и корективни мерки, които ползвателите могат да приложат, за да намалят въздействието на уязвимостта или инцидента, когато е подходящо в структуриран, машинночетим формат, който е лесен за автоматично обработване. Ако производителят не информира своевременно ползвателите на продукта с цифрови елементи, нотифицираните определени за координатори ЕРИКС могат да предоставят тази информация на ползвателите, когато това се счита за пропорционално и необходимо за предотвратяване или смекчаване на въздействието на уязвимостта или инцидента.

9. До … [12 месеца, считано от датата на влизане в сила на настоящия регламент] Комисията приема делегирани актове в съответствие с член 61 за допълване на настоящия регламент, като определя реда и условията за прилагане на основанията, свързани с киберсигурността, за забавяне на разпространението на нотификациите, посочени в член 16, параграф 2. При изготвянето на проектите на делегираните актове Комисията си сътрудничи с мрежата на ЕРИКС, създадена съгласно член 15 от Директива (ЕС) 2022/2555, и с ENISA.

10. Чрез приемане на актове за изпълнение Комисията може да определи допълнително формата и процедурите на нотификациите, посочени в настоящия член, както и в членове 15 и 16. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 62, параграф 2. При изготвянето на тези проекти на актове за изпълнение Комисията си сътрудничи с мрежата на ЕРИКС и ENISA.

Член 15

Доброволно докладване

1. Производителите, както и други физически или юридически лица, могат доброволно да нотифицират на определения за координатор ЕРИКС, или на ENISA всяка уязвимост, съдържаща се в продукт с цифрови елементи, както и киберзаплахите, които биха могли да засегнат рисковия профил на продукт с цифрови елементи.

2. Производителите, както и други физически или юридически лица, могат доброволно да нотифицират на определения за координатор ЕРИКС или на ENISA всеки инцидент, който оказва въздействие върху сигурността на продукта с цифрови елементи, както и ситуации, близки до инциденти, които е можело да доведат до такъв инцидент.

3. Определеният за координатор ЕРИКС или ENISA обработва нотификациите, посочени в параграфи 1 и 2 от настоящия член, в съответствие с процедурата, предвидена в член 16.

   Определеният за координатор ЕРИКС може да обработва с предимство задължителните нотификации пред доброволните нотификации.

4. Когато физическо или юридическо лице, различно от производителя, нотифицира в съответствие с параграфи 1 или 2 активно използвана уязвимост или сериозен инцидент, който оказва въздействие върху сигурността на продукт с цифрови елементи, определеният за координатор ЕРИКС информира без ненужно забавяне производителя.

5. Определеният за координатор ЕРИКС, и ENISA гарантират поверителността и подходящата защита на информацията, предоставяна от нотифициращото физическо или юридическо лице. Без да се засягат предотвратяването, разследването, разкриването и наказателното преследване на престъпления, доброволното докладване не води до налагането на никакви допълнителни задължения на нотифициращото физическо или юридическо лице, на които то не би подлежало, ако не подаде нотификацията.

Член 16

Създаване на единна платформа за докладване

1. За целите на нотификациите, посочени в член 14, параграфи 1 и 3 и член 15, параграфи 1 и 2, и за да се опростят задълженията на производителите за докладване, ENISA създава единна платформа за докладване. Ежедневните операции на тази единна платформа за докладване се управляват и поддържат от ENISA. Архитектурата на единната платформа за докладване позволява на държавите членки и ENISA да въвеждат свои собствени крайни точки за електронно нотифициране.

2. След получаване на нотификация определеният за координатор ЕРИКС, който първоначално получава нотификацията, незабавно разпространява нотификацията чрез единната платформа за докладване до определените за координатори ЕРИКС, на чиято територия производителят е посочил, че е предоставен продуктът с цифрови елементи.

При изключителни обстоятелства, по-специално по искане на производителя и с оглед на степента на чувствителност на нотифицираната информация, посочена от производителя съгласно член 14, параграф 2, буква а) от настоящия регламент, разпространението на нотификацията може да бъде забавено поради основателни причини, свързани с киберсигурността, за период от време, който е строго необходим, включително когато уязвимостта е предмет на координирана процедура за оповестяване на уязвимости, както е посочено в член 12, параграф 1 от Директива (ЕС) 2022/2555. Ако ЕРИКС реши да не публикува нотификация, той незабавно информира ENISA за решението и предоставя както обосновка за непубликуването на нотификацията, така и указание кога ще разпространи нотификацията в съответствие с процедурата за разпространение, предвидена в настоящия параграф. ENISA може да подпомага ЕРИКС при прилагането на основания, свързани с киберсигурността, във връзка със забавяне на разпространението на нотификацията.

При особено изключителни обстоятелства, когато производителят посочва в нотификацията по член 14, параграф 2, буква б):

а) че уязвимостта, за която е подадена нотификация, е била използвана активно от злонамерен участник и според наличната информация, тя не е била използвана в друга държава членка, освен тази на определения за координатор ЕРИКС, който производителят е уведомил за уязвимостта;

б) че всяко незабавно по-нататъшно разпространение на съобщената уязвимост вероятно ще доведе до предоставяне на информация, чието разкриване би било в противоречие с основните интереси на тази държава членка; или

в) че уязвимостта, за която е подадена нотификация, представлява непосредствен висок киберриск, произтичащ от по-нататъшното разпространение;

на ENISA се предоставя едновременно само информацията, че производителят е направил нотификация, общата информация за продукта, информацията за общия характер на използването и информацията, че са приведени основания, свързани със сигурността, докато пълната нотификация не се разпространи до съответните ЕРИКС и ENISA. Когато въз основа на тази информация ENISA счита, че съществува системен риск, засягащ сигурността на вътрешния пазар, тя препоръчва на получаващия ЕРИКС да разпространи пълната нотификация до другите определени за координатори ЕРИКС и до самата ENISA.

3. След получаване на нотификация за активно използвана уязвимост в продукт с цифрови елементи или за сериозен инцидент, който оказва въздействие върху сигурността на продукт с цифрови елементи, определените за координатори ЕРИКС предоставят на органите за надзор на пазара на съответните си държави членки нотифицираната информация, необходима на органите за надзор на пазара, за да изпълнят задълженията си по настоящия регламент.

4. ENISA предприема подходящи и пропорционални технически, оперативни и организационни мерки за управление на рисковете за сигурността на единната платформа за докладване и на информацията, подадена или разпространявана чрез единната платформа за докладване. Тя нотифицира без ненужно забавяне на мрежата на ЕРИКС и Комисията инциденти, свързани със сигурността, които засягат единната платформа за докладване.

5. ENISA, в сътрудничество с мрежата на ЕРИКС, предоставя и прилага спецификации относно техническите, оперативните и организационните мерки във връзка със създаването, поддръжката и сигурното функциониране на единната платформа за докладване, посочена в параграф 1, включително най-малко договореностите за сигурност, свързани със създаването, функционирането и поддръжката на единната платформа за докладване, както и крайните точки за електронно нотифициране, създадени от определените за координатори ЕРИКС на национално равнище и от ENISA на равнището на Съюза, включително процедурни аспекти, за да се гарантира, че когато нотифицираната уязвимост не съдържа коригиращи или смекчаващи мерки, информацията за тази уязвимост се споделя в съответствие със строги протоколи за сигурност и въз основа на принципа „необходимост да се знае“.

6. Когато определен за координатор ЕРИКС е бил уведомен за активно използвана уязвимост като част от координирана процедура за оповестяване на уязвимости, както е посочено в член 12, параграф 1 от Директива (ЕС) 2022/2555, определеният за координатор ЕРИКС, който първоначално получава нотификацията, може да отложи разпространението на съответната нотификация чрез единната платформа за докладване поради основателни причини, свързани с киберсигурността, за срок, който не надвишава строго необходимото, и докато не бъде дадено съгласие за разкриване от участващите страни в координираното разкриване на уязвимости. Това изискване не възпрепятства производителите доброволно да нотифицират такава уязвимост в съответствие с процедурата, предвидена в настоящия член.

Член 17

Други разпоредби, свързани с докладването

1. ENISA може да предоставя на Европейската мрежа за връзка на организациите при киберкризи (EU-CyCLONe), създадена съгласно член 16 от Директива (ЕС) 2022/2555, информацията, нотифицирана съгласно член 14, параграфи 1 и 3 и член 15, параграфи 1 и 2 от настоящия регламент, ако тази информация е от значение за координираното управление на мащабни киберинциденти и кризи на оперативно равнище. За да определи дали съответната информация е от такова значение, ENISA може да взема предвид технически анализи, извършени от мрежата на ЕРИКС, ако има такива.

2. Когато е необходима обществена осведоменост за предотвратяване или смекчаване на сериозен инцидент, който оказва въздействие върху сигурността на продукта с цифрови елементи, или за справяне с текущ инцидент, или когато разкриването на инцидента е в обществен интерес по друг начин, определеният за координатор ЕРИКС на съответната държава членка може, след консултация със засегнатия производител и когато е целесъобразно, в сътрудничество с ENISA, да информира обществеността за инцидента или да изиска от производителя да направи това.

3. Въз основа на нотификациите, получени по член 14, параграфи 1 и 3 и член 15, параграфи 1 и 2 от настоящия регламент, на всеки 24 месеца ENISA изготвя технически доклад за нововъзникващите тенденции по отношение на киберрисковете в продуктите с цифрови елементи и го представя на групата за сътрудничество за МИС, създадена съгласно член 14 от Директива (ЕС) 2022/2555. Първият такъв доклад се представя в срок от 24 месеца от датата на прилагане на задълженията, предвидени в член 14, параграфи 1 и 3 от настоящия регламент. ENISA включва съответната информация от техническите си доклади в своя доклад за състоянието на киберсигурността в Съюза съгласно член 18 от Директива (ЕС) 2022/2555.

4. Самото действие на нотифициране в съответствие с член 14, параграфи 1 и 3 и член 15, параграфи 1 и 2 не възлага на нотифициращото физическо или юридическо лице по-голяма отговорност.

5. След като бъде налична актуализация за сигурност или друга форма на коригираща или смекчаваща мярка, ENISA, със съгласието на производителя на съответния продукт с цифрови елементи, добавя публично известната уязвимост, нотифицирана съгласно член 14, параграф 1 или член 15, параграф 1 от настоящия регламент, към европейската база данни за уязвимости, създадена съгласно член 12, параграф 2 от Директива (ЕС) 2022/2555.

6. Определените за координатори ЕРИКС предоставят на производителите подкрепа във връзка със задълженията за докладване съгласно член 14, по-специално на производителите, които се определят като микропредприятия или малки или средни предприятия.

Член 18

Упълномощени представители

1. Производителят може, чрез писмено пълномощно, да назначава упълномощен представител.

2. Задълженията, установени в член 13, параграфи 1—11 и параграф 12, първа алинея, и параграф 14, не се включват в пълномощното на упълномощения представител.

3. Упълномощеният представител изпълнява задачите, определени в даденото от производителя пълномощно. Упълномощеният представител предоставя при поискване екземпляр от пълномощното на органите за надзор на пазара. Пълномощното 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 28, и техническата документация, посочена в член 31, в продължение на най-малко 10 години след пускането на пазара на продукта с цифрови елементи или за периода на поддръжка, в зависимост от това кой период е по-дълъг;

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 пълномощното на упълномощения представител.

Член 19

Задължения на вносителите

1. Вносителите пускат на пазара само продукти с цифрови елементи, съответстващи на съществените изисквания за киберсигурност, определени в приложение I, част I, и при които въведените от производителя процеси съответстват на съществените изисквания за киберсигурност, определени в приложение I, част II.

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

   а) съответната процедура за оценяване на съответствието, както е посочена в член 32, е била проведена от производителя;

   б) производителят е изготвил техническата документация;

   в) върху продукта с цифрови елементи е нанесена маркировката „CE“, посочена в член 30, и той е придружен от ЕС декларацията за съответствие, посочена в член 13, параграф 20, и от информацията и инструкциите за потребителя, посочени в приложение II, на език, лесно разбираем за ползвателите и органите за надзор на пазара;

   г) производителят е спазил изискванията, определени в член 13, параграфи 15, 16 и 19.

   За целите на настоящия параграф вносителите са в състояние да предоставят необходимите документи, доказващи изпълнението на изискванията, посочени в настоящия член.

3. Когато вносител счита или има основание да счита, че продукт с цифрови елементи или процесите, въведени от производителя, не са в съответствие с настоящия регламент, вносителят не пуска продукта на пазара, докато продуктът или процесите, въведени от производителя, не бъдат приведени в съответствие с настоящия регламент. Освен това, когато продуктът с цифрови елементи представлява значителен киберриск, вносителят информира за това производителя и органите за надзор на пазара.

Когато вносител има основания да счита, че даден продукт с цифрови елементи може да представлява значителен киберриск с оглед на нетехнически рискови фактори, вносителят информира за това органите за надзор на пазара. При получаване на такава информация органите за надзор на пазара следват процедурите, посочени в член 54, параграф 2.

4. Вносителите посочват своето име, регистрирано търговско наименование или регистрирана търговска марка, пощенския адрес, адреса на електронна поща или друг цифров контакт, а също и — когато е приложимо, уебсайта, на който може да се осъществи връзка с тях, върху продукта с цифрови елементи или 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, които знаят или имат основание да смятат, че продукт с цифрови елементи, който са пуснали на пазара, не е в съответствие с настоящия регламент, незабавно предприемат необходимите коригиращи мерки, за да гарантират, че продуктът с цифрови елементи е приведен в съответствие с настоящия регламент, или за изтегляне или изземване на продукта, ако е подходящо.

Когато узнаят за 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 на пазара продукта с цифрови елементи, като предоставят подробни данни, по-специално за несъответствието с изискванията и за всякакви предприети корективни мерки.

6. В продължение на най-малко десет години след пускането на пазара на продукта с цифрови елементи или за периода на поддръжка, в зависимост от това кой период е по-дълъг, 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.

7. 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 за киберсигурност, посочени в приложение I, част I, както и на въведените от производителя процеси със съществените изисквания за киберсигурност, посочени в приложение I, част II, 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 пуснали на пазара.

8. 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 20

Задължения на дистрибуторите

1. Когато предоставят продукт с цифрови елементи на пазара, дистрибуторите действат с дължимата грижа по отношение на изискванията, предвидени в 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 в член 13, параграфи 15, 16, 18, 19 и 20 и член 19, параграф 4, и дали са предоставили всички необходими документи на дистрибутора.

3. Когато дистрибутор счита или има основание да счита, въз основа на информация, с която разполага, че продукт с цифрови елементи или процесите, въведени от производителя, не са в съответствие със съществените изисквания за киберсигурност, 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 с настоящия регламент. Освен това, когато продуктът с цифрови елементи представлява значителен киберриск, дистрибуторът информира за това производителя и органите за надзор на пазара без неоправдано забавяне.

4. Дистрибуторите, които знаят или имат основание да смятат, въз основа на информация, с която разполагат, че продукт с цифрови елементи, който са предоставили на пазара, или процесите, въведени от неговия производител, не са в съответствие с настоящия регламент, 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 подходящо.

Когато узнаят за 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 неспазването на изискванията и за всякакви предприети коригиращи мерки.

5. При мотивирано искане от страна на орган за надзор на пазара дистрибуторите 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 с настоящия регламент 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 предоставили на пазара.

6. Когато дистрибуторът на продукт с цифрови елементи узнае, въз основа на информация, с която разполага, 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, без ненужно забавяне, 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 21

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 за него се прилагат членове 13 и 14, когато този вносител или дистрибутор пуска на пазара продукт с цифрови елементи под своето име или търговска марка или извършва съществено изменение на продукт с цифрови елементи, който вече е пуснат на пазара.

Член 22

Други случаи, в които се прилагат задълженията на производителите

1. Физическо или юридическо лице, различно от производителя, вносителя или дистрибутора, което извършва съществено изменение на продукт с цифрови елементи и предоставя този продукт на пазара, се счита за производител за целите на настоящия регламент.

2. Задълженията по членове 13 и 14 се прилагат по отношение на лицето, посочено в параграф 1 от настоящия член, за частта от продукта с цифрови елементи, която е засегната от съществената промяна, или, ако съществената промяна оказва въздействие върху киберсигурността на продукта с цифрови елементи като цяло, за целия продукт.

Член 23

Идентификация на икономическите оператори

1. По искане на органите за надзор на пазара, икономическите оператори им предоставят следната информация:

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

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

2. Икономическите оператори трябва да бъдат в състояние да представят информацията, посочена в параграф 1, в продължение на 10 години, след като продуктът с цифрови елементи им е бил доставен, и в продължение на 10 години, след като те са доставили продукта с цифрови елементи.

Член 24

Задължения на попечителите на софтуер с отворен код

1. Попечителите на софтуер с отворен код въвеждат и документират по проверим начин политика за киберсигурност за насърчаване на разработването на сигурен продукт с цифрови елементи, както и ефективно справяне с уязвимостите от страна на разработчиците на този продукт. Тази политика също така насърчава доброволното докладване на уязвимости, предвидено в член 15, от разработчиците на този продукт и взема предвид специфичното естество на попечителя на софтуер с отворен код и правните и организационните договорености, които се прилагат за него. Посочената политика включва по-специално аспекти, свързани с документирането, преодоляването и отстраняването на уязвимости, и насърчава споделянето на информация относно открити уязвимости в рамките на общността, работеща с отворен код.

2. Попечителите на софтуер с отворен код сътрудничат на органите за надзор на пазара, по тяхно искане, с цел смекчаване на киберрисковете, породени от продукт с цифрови елементи, отговарящи на критериите за свободен софтуер с отворен код.

   При мотивирано искане от страна на орган за надзор на пазара попечителите на софтуер с отворен код предоставят на този орган на език, лесно разбираем за този орган, документацията, посочена в параграф 1, на хартиен или електронен носител.

3. Задълженията по член 14, параграф 1 се прилагат за попечителите на софтуер с отворен код, доколкото те участват в разработването на продуктите с цифрови елементи. Задълженията по член 14, параграфи 3 и 8 се прилагат за попечителите на софтуер с отворен код, доколкото сериозни инциденти, които оказват въздействие върху сигурността на продуктите с цифрови елементи, засягат мрежовите и информационните системи, предоставени от попечителите на софтуер с отворен код за разработването на такива продукти.

Член 25

Удостоверяване на сигурността на свободния софтуер с отворен код

За да се улесни задължението за дължима грижа, посочено в член 13, параграф 5, по-специално по отношение на производителите, които интегрират компоненти на свободен софтуер с отворен код в своите продукти с цифрови елементи, на Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 61 за допълване на настоящия регламент чрез създаване на доброволни програми за удостоверяване на сигурността, позволяващи на разработчиците или ползвателите на продукти с цифрови елементи, квалифицирани като свободен софтуер с отворен код, както и на други трети страни, да оценяват съответствието на такива продукти с всички или някои съществени изисквания за киберсигурност или други задължения, установени в настоящия регламент.

Член 26

Насоки

1. С цел да се улесни изпълнението и да се гарантира неговата последователност, Комисията публикува насоки за подпомагане на икономическите оператори при прилагането на настоящия регламент със специален акцент върху улесняването на спазването на изискванията от страна на микропредприятията и малките и средните предприятия.

2. Когато възнамерява да предостави насоки, както е посочено в параграф 1, Комисията разглежда най-малко следните аспекти:

   а) обхвата на настоящия регламент, със специален акцент върху решенията за обработване на данни от разстояние и свободния софтуер с отворен код;

   б) прилагането на периоди на поддръжка във връзка с определени категории продукти с цифрови елементи;

   в) насоки за производителите, обхванати от настоящия регламент, спрямо които се прилага и законодателство на Съюза за хармонизация, различно от настоящия регламент, или други свързани правни актове на Съюза;

   г) концепцията за съществено изменение.

   Комисията поддържа също така леснодостъпен списък на делегираните актове и актовете за изпълнение, приети съгласно настоящия регламент.

3. При изготвянето на насоките съгласно настоящия член Комисията се консултира със съответните заинтересовани страни.

Глава III

Съответствие на продукта с цифрови елементи

Член 27

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 за киберсигурност, определени в приложение I, обхванати от тези стандарти или части от тях.

   Комисията, в съответствие с член 10, параграф 1 от Регламент (ЕС) № 1025/2012, отправя искане към една или повече европейски организации за стандартизация да изготвят хармонизирани стандарти за съществените изисквания за киберсигурност, определени в приложение I към настоящия регламент. При изготвянето на исканията за стандартизация за настоящия регламент Комисията се стреми да взема предвид съществуващите европейски и международни стандарти за киберсигурност, които са въведени или са в процес на разработване, за да се опрости разработването на хармонизирани стандарти в съответствие с Регламент (ЕС) № 1025/2012.

2. Комисията може да приема актове за изпълнение за установяване на общи спецификации, обхващащи технически изисквания, които осигуряват начин за спазване на съществените изисквания за киберсигурност, определени в приложение I за продуктите с цифрови елементи, попадащи в обхвата на настоящия регламент.

Тези актове за изпълнение се приемат само когато са изпълнени следните условия:

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

i) искането не е прието;

ii) хармонизираните стандарти, отговарящи на това искане, не са представени в срока, определен в съответствие с член 10, параграф 1 от Регламент (ЕС) № 1025/2012; или

iii) хармонизираните стандарти не са в съответствие с искането; и

б) в *Официален вестник на Европейския съюз* не са публикувани в съответствие с Регламент (ЕС) № 1025/2012 данните за хармонизирани стандарти, обхващащи съответните съществени изисквания за киберсигурност, определени в приложение I, и публикуването на такива данни не се очаква в разумен срок.

Посочените актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 62, параграф 2.

3. Преди да изготви проекта на акт за изпълнение, посочен в параграф 2 от настоящия член, Комисията информира комитета, посочен в член 22 от Регламент (ЕС) № 1025/2012, че счита, че условията по параграф 2 от настоящия член са изпълнени.

4. При изготвянето на проекта на акт за изпълнение, посочен в параграф 2, Комисията взема предвид становищата на съответните органи и надлежно се консултира с всички съответни заинтересовани страни.

5. За продуктите с цифрови елементи и процесите, въведени от производителя, които са в съответствие с общите спецификации, установени с актовете за изпълнение, посочени в параграф 2 от настоящия член, или с части от тях, се приема, че са в съответствие със съществените изисквания за киберсигурност, определени в приложение I, попадащи в обхвата на тези общи спецификации или на части от тях.

6. Когато хармонизиран стандарт е приет от европейска организация за стандартизация и е предложен на Комисията с цел публикуване на данните за него в *Официален вестник на Европейския съюз*, Комисията оценява хармонизирания стандарт в съответствие с Регламент (ЕС) № 1025/2012. Когато в *Официален вестник на Европейския съюз* се публикуват данните за хармонизиран стандарт, Комисията отменя актовете за изпълнение, посочени в параграф 2, или частите от тях, които обхващат същите съществени изисквания за киберсигурност като тези, обхванати от този хармонизиран стандарт.

7. Когато държава членка счита, че дадена обща спецификация не отговаря напълно на съществените изисквания за киберсигурност, определени в приложение I, тя информира Комисията за това, като представя подробно обяснение. Комисията разглежда това подробно обяснение и, ако е уместно, може да измени акта за изпълнение, с който е въведена въпросната обща спецификация.

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

9. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 61 от настоящия регламент за допълване на настоящия регламент чрез определяне на европейските схеми за сертифициране на киберсигурността, приети съгласно Регламент (ЕС) 2019/881, които могат да се използват за доказване на съответствие на продукти с цифрови елементи със съществените изисквания за киберсигурност или с части от тях, както са определени в приложение I към настоящия регламент. Освен това, издаването на Европейски сертификат за киберсигурност по тези схеми, удостоверяващ най-малко „съществено“ ниво на увереност, премахва задължението на производителя да извърши оценяване на съответствието от трета страна за съответните изисквания, както е предвидено в член 32, параграф 2, букви а) и б) и член 32, параграф 3, букви а) и б) от настоящия регламент.

Член 28

ЕС декларация за съответствие

1. ЕС декларацията за съответствие се изготвя от производителите в съответствие с член 13, параграф 12 и в нея се посочва, че изпълнението на приложимите съществени изисквания за киберсигурност, определени в приложение I, е доказано.

2. ЕС декларацията за съответствие се съставя по образеца, установен в приложение V, и съдържа елементите, определени в съответните процедури за оценяване на съответствието, установени в приложение VIII. Тази декларация се актуализира, когато е уместно. Тя се предоставя на езиците, изисквани от държавата членка, на чийто пазар се пуска или предоставя продуктът с цифрови елементи.

Опростената ЕС декларация за съответствие, посочена в член 13, параграф 20, се съставя по образеца, установен в приложение VI. Тя се предоставя на езиците, изисквани от държавата членка, на чийто пазар се пуска или предоставя продуктът с цифрови елементи.

3. Когато приложимите към продукта с цифрови елементи правни 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 правни актове на Съюза. В тази декларация се посочват съответните правни актове на Съюза, включително данните за тяхното публикуване.

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

5. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 61 за допълване на настоящия регламент чрез добавяне на елементи към минималното съдържание на ЕС декларацията за съответствие, посочено в приложение V, за да бъде отчетено технологичното развитие.

Член 29

Основни принципи за маркировката „CE“

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

Член 30

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 подходящо поради естеството на продукта с цифрови елементи, тя се нанася върху опаковката и върху ЕС декларацията за съответствие, посочена в член 28, 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 28, или в уебсайта, придружаващ софтуерния продукт. В последния случай съответният раздел на уебсайта трябва да бъде лесно и пряко достъпен за потребителите.

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 киберриск или употреба, определени в актовете 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), посочена в член 32.

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

5. Държавите членки доразвиват съществуващите механизми, за да гарантират правилното прилагане на режима, уреждащ маркировката „CE“, и предприемат подходящи действия в случай на неправомерно използване на тази маркировка. Когато спрямо продукта с цифрови елементи се прилага друго законодателство на Съюза за хармонизиране, различно от настоящия регламент, което също предвижда нанасянето на маркировката „CE“, маркировката „CE“ показва, че продуктът отговаря и на изискванията, установени в това друго законодателство на Съюза за хармонизация.

6. Комисията може чрез актове за изпълнение да определя технически спецификации за етикети, пиктограми или други знаци, свързани със сигурността на продуктите с цифрови елементи, техните периоди на поддръжка, както и механизми за насърчаване на тяхното използване и за повишаване на обществената осведоменост за сигурността на продуктите с цифрови елементи. При изготвянето на проектите на актове за изпълнение Комисията се консултира със съответните заинтересовани страни и, ако вече е създадена съгласно член 52, параграф 15, с ADCO групата. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 62, параграф 2.

Член 31

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 съществените изисквания за киберсигурност, определени в приложение I. Тя съдържа най-малкото данните, посочени в приложение VII.

2. Техническата документация се изготвя преди пускането на продукта с цифрови елементи на пазара и се актуализира непрекъснато, когато е уместно, поне по време на периода на поддръжка на продукта.

3. По отношение на продуктите с цифрови елементи, посочени в член 12, които са предмет и на други правни актове на Съюза, в които се предвижда техническа документация, се изготвя едно-единствено досие с техническа документация, което съдържа информацията, посочена в приложение VII, и информацията, изисквана съгласно посочените правни 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. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 61 за допълване на настоящия регламент чрез добавяне на елементи, които да бъдат включвани в техническата документация, посочена в приложение VII, за да бъдат отчетени технологичното развитие, както и промените, настъпили в процеса на прилагане на настоящия регламент. За тази цел Комисията се стреми да гарантира, че административната тежест за микропредприятията и малките и средните предприятия е пропорционална.

Член 32

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 за киберсигурност, определени в приложение I. Производителят доказва съответствието със съществените изисквания за киберсигурност, като използва която и да е от следните процедури:

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

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

в) оценка на съответствието въз основа на пълно осигуряване на качеството (въз основа на модул H), посочена в приложение VIII; или

г) когато е налична и приложима, европейска схема за сертифициране на киберсигурността, съгласно посоченото в член 27, параграф 9.

2. Когато при оценяването на съответствието на важен продукт с цифрови елементи, който попада в обхвата на клас I, както е посочено в приложение III, и на процесите, въведени от неговия производител, със съществените изисквания за киберсигурност, определени в приложение I, производителят не е приложил или е приложил само частично хармонизирани стандарти, общи спецификации или европейски схеми за сертифициране на киберсигурността, предоставящи най-малко „съществено“ ниво на увереност, както е посочено в член 27, или когато такива хармонизирани стандарти, общи спецификации или европейски схеми за сертифициране на киберсигурността не съществуват, по отношение на тези съществени изисквания за киберсигурност за съответния продукт с цифрови елементи и за процесите, въведени от производителя, се използва която и да е от следните процедури:

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

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

3. Когато продуктът е важен продукт с цифрови елементи, който попада в обхвата на клас II, както е определен в приложение III, производителят доказва съответствието със съществените изисквания за киберсигурност, определени в приложение I, като използва която и да е от следните процедури:

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

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

в) когато е налична и приложима, европейска схема за сертифициране на киберсигурността съгласно член 27, параграф 9 от настоящия регламент, предоставяща най-малко „съществено“ ниво на увереност съгласно Регламент (ЕС) 2019/881.

4. Съответствието на критичните продукти с цифрови елементи, изброени в приложение IV, на съществените изисквания за киберсигурност, посочени в приложение I, се доказва с една от следните процедури:

а) „европейска схема за сертифициране на киберсигурността“ в съответствие с член 8, параграф 1; или

б) когато условията по член 8, параграф 1 не са изпълнени — която и да е от процедурите, посочени в параграф 3 от настоящия член.

5. Производителите на продукти с цифрови елементи, квалифицирани като свободен софтуер с отворен код, които попадат в категориите, определени в приложение III, трябва да могат да докажат съответствие със съществените изисквания за киберсигурност, определени в приложение I, като използват една от процедурите, посочени в параграф 1 от настоящия член, при условие че техническата документация, посочена в член 31, е предоставена на обществеността в момента на пускането на пазара на тези продукти.

6. Специфичните интереси и потребности на микропредприятията и на малките и средните предприятия, включително стартиращите предприятия, се вземат предвид при определянето на таксите за процедурите за оценяване на съответствието и тези такси се намаляват пропорционално на техните специфични интереси и потребности.

Член 33

Мерки за подкрепа на микропредприятията и малките и средните предприятия, включително новосъздадените предприятия

1. Когато е целесъобразно, държавите членки предприемат следните действия, съобразени с нуждите на микропредприятията и малките предприятия:

   а) организират специфични дейности за повишаване на осведомеността и обучение относно прилагането на настоящия регламент;

б) създават специален канал за комуникация с микропредприятията и малките предприятия и когато е целесъобразно, с местните публични органи, за предоставяне на съвети и отговаряне на запитвания относно прилагането на настоящия регламент;

в) оказват подкрепа за дейностите по изпитване и оценяване на съответствието, включително, когато е целесъобразно, с подкрепата на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността.

2. Когато е целесъобразно, държавите членки могат да създават регулаторни лаборатории за киберустойчивост. Тези регулаторни лаборатории осигуряват контролирана среда за изпитване на иновативни продукти с цифрови елементи, за да се улесни тяхното разработване, проектиране, валидиране и изпитване за целите на спазването на настоящия регламент за ограничен период от време преди пускането на пазара. Комисията, и когато е целесъобразно, ENISA, могат да предоставят техническа подкрепа, съвети и инструменти за създаването и функционирането на регулаторни лаборатории. Регулаторните лаборатории се създават под прекия надзор, насоки и подкрепа от органите за надзор на пазара. Държавите членки информират Комисията и другите органи за надзор на пазара за създаването на регулаторна лаборатория чрез ADCO групата. Регулаторните лаборатории не засягат надзорните и коригиращите правомощия на компетентните органи. Държавите членки гарантират открит, справедлив и прозрачен достъп до регулаторните лаборатории, и по-специално улесняват достъпа на микропредприятията и малките предприятия, включително стартиращите предприятия.

3. В съответствие с член 26 Комисията предоставя насоки за микропредприятията и малките и средните предприятия във връзка с прилагането на настоящия регламент.

4. Комисията разгласява предвидената финансова подкрепа в регулаторната рамка на съществуващите програми на Съюза, по-специално с цел облекчаване на финансовата тежест върху микропредприятията и върху малките и средните предприятия.

5. Микропредприятията и малките предприятия могат да предоставят всички елементи на техническата документация, посочени в приложение VII, като използват опростен формат. За тази цел, чрез актове за изпълнение, Комисията определя опростения формуляр за техническа документация за нуждите на микропредприятията и малките предприятия, включително начина, по който трябва да се предоставят елементите, посочени в приложение VII. Когато микропредприятие или малко предприятие избере да предостави определената в приложение VII информация по опростен начин, то използва формуляра, посочен в настоящия параграф. Нотифицираните органи приемат този формуляр за целите на оценяването на съответствието.

Посочените актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 62, параграф 2.

Член 34

Споразумения за взаимно признаване

Като взема предвид равнището на техническо развитие и подхода към оценяването на съответствието, прилаган от трета държава, Съюзът може да сключва споразумения за взаимно признаване с трети държави в съответствие с член 218 от ДФЕС с цел насърчаване и улесняване на международната търговия.

Глава IV

Нотифициране на органите за оценяване на съответствието

Член 35

Нотифициране

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

2. Държавите членки се стремят да гарантират наличието в Съюза до ... [24 месеца от датата на влизане в сила на настоящия регламент] на достатъчен брой нотифицирани органи за извършване на оценки на съответствието, за да се избегнат затруднения и пречки пред навлизането на пазара.

Член 36

Нотифициращи органи

1. Всяка държава членка определя нотифициращ орган, отговорен за въвеждането и провеждането на необходимите процедури за оценяване, определяне и нотифициране на органите за оценяване на съответствието, както и за тяхното наблюдение, включително съответствието с член 41.

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

3. Когато нотифициращият орган делегира или възлага по друг начин провеждането на оценката, нотифицирането или наблюдението, посочени в параграф 1 от настоящия член, на орган, който не е правителствена структура, този орган е правен субект и спазва *mutatis mutandis* изискванията, установени с член 37. Освен това този орган трябва да разполага с механизми за покриване на отговорността, произтичаща от неговата дейност.

4. Нотифициращият орган поема пълна отговорност за задачите, изпълнявани от органа, посочен в параграф 3.

Член 37

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 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 на брой компетентен персонал за правилното изпълнение на своите задачи.

Член 38

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 информацията, посочена в параграф 1, обществено достояние.

Член 39

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 националното право и има юридическа правосубектност.

3. Органът за оценяване на съответствието е трета страна, независима от организацията или от продукта с цифрови елементи, 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 — трета страна, 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, вносител, дистрибутор, 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, вноса, разпространението, продажбата, монтирането, използването или поддръжката на продуктите с цифрови елементи, които оценяват, 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 консултантските 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 VIII 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 познания и достатъчен и подходящ опит за изпълнение на задачите за оценяване на съответствието;

б) описания на процедурите, съгласно които ще се извършва оценяването на съответствието, като се гарантира прозрачността и възможността за възпроизвеждане 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 то осъществява дейност и неговата структура, степента на сложност на съответната технология на продукта и масовия или сериен характер на производството.

Органът за оценяване на съответствието разполага със средствата, необходими за изпълнение по подходящ начин на техническите и административните задачи, свързани с дейностите по оценяване на съответствието, както и с достъп до необходимото оборудване или съоръжения.

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 за киберсигурност, определени в приложение I, на приложимите хармонизирани стандарти и общи спецификации, и на съответните разпоредби 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 тяхната държава членка 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 VIII 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 51, 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, пропорционални и разумни условия, като избягват създаването на ненужна тежест за икономическите оператори, по-специално като вземат предвид интересите на микропредприятията и малките и средните предприятия във връзка с таксите.

Член 40

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 39, доколкото приложимите хармонизирани стандарти обхващат тези изисквания.

Член 41

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 39, и надлежно информира нотифициращия орган.

2. Нотифицираните органи носят пълна отговорност за дейността, извършена от подизпълнители или поделения, независимо от мястото им на установяване.

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 42

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 с цифрови елементи, за които органът заявява компетентност, както и — когато е приложимо, от сертификат за акредитация, издаден от националния орган по акредитация и удостоверяващ, че органът за оценяване на съответствието отговаря на изискванията, предвидени в член 39.

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 39.

Член 43

Процедура по нотифициране

1. Нотифициращите органи нотифицират само органи за оценяване на съответствието, които отговарят на изискванията, установени в член 39.

2. Нотифициращият орган нотифицира Комисията и другите държави членки, като използва информационната 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 с цифрови елементи, както и съответното удостоверение за компетентност.

4. Когато нотифицирането не се основава на сертификат за акредитация, посочен в член 42, 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 39.

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.

   За целите на настоящия регламент само такъв орган се счита за нотифициран орган

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

Член 44

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 правни 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 45

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 39, 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 46

Оспорване на компетентността на нотифицирани органи

1. Комисията разследва всички случаи, в които има съмнения или когато пред нея са изразени съмнения относно компетентността на нотифициран орган да изпълнява 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 47

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 32 и приложение VIII.

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 предприятията, по-специално по отношение на микропредприятията и малките и средните предприятия, сектора, в който те осъществяват дейност, тяхната структура, степента им на сложност и нивото на киберриска, свързан с продуктите с цифрови елементи и съответната технология и масовия или серийния характер на производството.

3. Въпреки това нотифицираните органи спазват степента на взискателност и равнището на защита, необходими за съответствието на продуктите с цифрови елементи с разпоредбите на настоящия регламент.

4. Когато нотифицираният орган прецени, че определен производител не е изпълнил изискванията, установени в приложение I или в съответстващите им хармонизирани стандарти или в общите спецификации, посочени в член 27, 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 с цифрови елементи 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 48

Обжалване на решения на нотифицираните органи

Държавите членки гарантират наличието на процедура за обжалване на решенията на нотифицираните органи.

Член 49

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 с цифрови елементи, съответна информация по проблеми, свързани с отрицателни и при поискване, положителни резултати от оценяване на съответствието.

Член 50

Обмен на опит

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

Член 51

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 52

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 продукти с цифрови елементи, които попадат 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. Органите за надзор на пазара, определени съгласно параграф 2 от настоящия член, отговарят също така за извършването на дейности по надзор на пазара във връзка със задълженията на попечителите на софтуер с отворен код, определени в член 24. Когато орган за надзор на пазара установи, че даден попечител на софтуер с отворен код не спазва задълженията, определени в посочения член, той изисква от попечителя на софтуер с отворен код да гарантира, че са предприети всички подходящи коригиращи действия. Попечителите на софтуер с отворен код гарантират, че са предприети всички подходящи коригиращи действия по отношение на задълженията им съгласно настоящия регламент.

4. Когато е приложимо, органите за надзор на пазара си сътрудничат с националните органи за сертифициране в областта на киберсигурността, определени по силата на член 58 от Регламент (ЕС) 2019/881, и редовно обменят информация. По отношение на надзора на изпълнението на задълженията за докладване по член 14 от настоящия регламент определените органи за надзор на пазара си сътрудничат и редовно обменят информация с определените за координатори ЕРИКС и с ENISA.

5. Органите за надзор на пазара могат да поискат от определения за координатор ЕРИКС или от ENISA да предостави технически съвети по въпроси, свързани с изпълнението и правоприлагането на настоящия регламент. Когато провеждат разследване по член 54, органите за надзор на пазара могат да поискат от определения за координатор ЕРИКС или от ENISA да предостави анализ в подкрепа на оценки на съответствието на продуктите с цифрови елементи.

6. Когато е приложимо, органите за надзор на пазара си сътрудничат с други органи за надзор на пазара, определени въз основа на законодателство на Съюза за хармонизация, различно от настоящия регламент, и редовно обменят информация.

7. 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 10, 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.

8. Държавите членки гарантират, че на определените органи за надзор на пазара се предоставят подходящи финансови и технически ресурси, включително, когато е целесъобразно, средства за автоматизация на обработката, както и човешки ресурси с необходимите умения в областта на киберсигурността за изпълнение на задачите им съгласно настоящия регламент.

9. Комисията насърчава и улеснява обмена на опит между определените органи за надзор на пазара.

10. Органите за надзор на пазара могат да предоставят насоки и съвети на икономическите оператори относно прилагането на настоящия регламент с подкрепата на Комисията и когато е целесъобразно, ЕРИКС и ENISA.

11. Органите за надзор на пазара информират потребителите за това къде да подават жалби, които биха могли да посочат несъответствие с настоящия регламент, в съответствие с член 11 от Регламент (ЕС) 2019/1020, и предоставят на потребителите информация за това къде и как да получат достъп до механизми за улесняване на докладването на уязвимости, инциденти и киберзаплахи, които могат да засегнат продукти с цифрови елементи.

12. Когато е целесъобразно, органите за надзор на пазара улесняват сътрудничеството със съответните заинтересовани страни, включително научни, научноизследователски и потребителски организации.

13. 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.

14. По отношение на продуктите с цифрови елементи, които попадат в обхвата на настоящия регламент, класифицирани като високорискови системи с ИИ по смисъла на член 6 от Регламент (ЕС) 2024/1689, органите за надзор на пазара, определени за целите на Регламент (ЕС) 2024/1689, са органите, които отговарят за дейностите по надзор на пазара, изисквани съгласно настоящия регламент. Органите за надзор на пазара, определени за целите на Регламент (ЕС) 2024/1689, 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 14 от настоящия регламент — с определените за координатори ЕРИКС и с ENISA. Органите за надзор на пазара, определени в съответствие с Регламент (ЕС) 2024/1689, 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.

15. ADCO групата се създава за еднакво прилагане на настоящия регламент в съответствие с член 30, параграф 2 от Регламент (ЕС) 2019/1020. ADCO групата е съставена от представители на определените органи за надзор на пазара и ако е целесъобразно, от представители на единните служби за връзка. ADCO групата разглежда и конкретни въпроси, свързани с дейностите по надзор на пазара във връзка със задълженията, наложени на попечителите на софтуер с отворен код.

16. Органите за надзор на пазара наблюдават как производителите са приложили критериите, посочени в член 13, параграф 8, когато определят периода на поддръжка на своите продукти с цифрови елементи.

ADCO групата публикува в публично достъпна и лесна за ползване форма съответните статистически данни за категориите продукти с цифрови елементи, включително средните периоди на поддръжка, определени от производителя съгласно член 13, параграф 8, и предоставя насоки, които включват ориентировъчни периоди на поддръжка за категориите продукти с цифрови елементи.

Когато данните сочат неподходящи периоди на поддръжка за конкретни категории продукти с цифрови елементи, ADCO групата може да отправи препоръки към органите за надзор на пазара да съсредоточат дейностите си върху такива категории продукти с цифрови елементи.

Член 53

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 за киберсигурност, определени в приложение I, на органите за надзор на пазара се предоставя, при мотивирано искане, достъп на език, който е лесноразбираем за тях, 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 54

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 основание да счита, че даден продукт с цифрови елементи, включително отстраняването на уязвимости, представлява значителен киберриск, той извършва без неоправдано забавяне и когато е целесъобразно, в сътрудничество със съответните ЕРИКС, 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 икономически оператор да предприеме необходимите корективни действия, за да приведе продукта с цифрови елементи в съответствие с тези изисквания или да го изтегли от пазара, или да го изземе в определен от органа за надзор на пазара разумен срок, съобразен с естеството на киберриска.

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

2. При определяне на значимостта на киберриск, посочен в параграф 1 от настоящия член, органите за надзор на пазара вземат предвид и нетехническите рискови фактори, по-специално тези, установени в резултат на координирани оценки на риска за сигурността на критичните вериги на доставки на равнището на Съюза, извършени в съответствие с член 22 от Директива (ЕС) 2022/2555. Когато орган за надзор на пазара има достатъчно основание да счита, че даден продукт с цифрови елементи представлява значителен киберриск с оглед на нетехнически рискови фактори, той информира компетентните органи, определени или създадени съгласно член 8 от Директива (ЕС) 2022/2555, и при необходимост си сътрудничи с тези органи.

3. 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 икономическия оператор.

4. Икономическият оператор гарантира, че са предприети всички подходящи корективни действия по отношение на всички съответни продукти с цифрови елементи, които той предоставя на пазара в целия Съюз.

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

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

6. Информацията, посочена в параграф 5, включва всички налични подробни данни, по-специално данните, необходими за идентифицирането на несъответстващия продукт с цифрови елементи, произхода на този продукт 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 икономически оператор. По-специално органите за надзор на пазара посочват дали несъответствието се дължи на една или няколко от следните причини:

   а) несъответствие на продукта с цифрови елементи или на процесите, въведени от производителя, със съществените изисквания за киберсигурност, определени в приложение I;

   б) недостатъци в хармонизираните стандарти, европейските схеми за сертифициране на киберсигурността или общите спецификации, посочени в член 27.

7. 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 съответния продукт с цифрови елементи, и в случай на несъгласие с нотифицираната национална мярка — за своите възражения.

8. Когато в срок от три месеца от получаването на уведомлението, посочено в параграф 5 от настоящия член, 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 икономически оператор в съответствие с член 18 от Регламент (ЕС) 2019/1020.

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

Член 55

Предпазна процедура на Съюза

1. Когато в срок от три месеца след получаване на уведомлението по член 54, параграф 5 държава членка е повдигнала възражения срещу мярка, предприета от друга държава членка, или когато Комисията счита, че мярката противоречи на правото на Съюза, Комисията без забавяне започва консултации със съответната държава членка и съответния(те) икономически оператор(и) и извършва оценка на националната мярка. Въз основа на резултатите от тази оценка Комисията решава в срок от девет месеца от уведомлението, посочено в член 54, параграф 5, дали националната мярка е оправдана или не 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 я оттегля.

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 11 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, посочена в член 27, Комисията преценява дали да измени или отмени даден делегиран акт, приет съгласно член 27, параграф 9, 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, посочени в член 27, Комисията преценява дали да измени или отмени даден акт за изпълнение, приет съгласно член 27, параграф 2, с който се определят тези общи спецификации.

Член 56

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

1. Когато Комисията има достатъчно основание 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 информира съответните органи за надзор на пазара. Когато органите за надзор на пазара извършват оценка на продукта с цифрови елементи, който може да представлява значителен киберриск по отношение на съответствието си с изискванията, определени в настоящия регламент, се прилагат процедурите, посочени в членове 54 и 55.

2. Когато Комисията има достатъчно основание да счита, че даден продукт с цифрови елементи представлява значителен киберриск с оглед на нетехнически рискови фактори, тя информира съответните органи за надзор на пазара и когато е целесъобразно, компетентните органи, определени или създадени съгласно член 8 от Директива (ЕС) 2022/2555, и при необходимост си сътрудничи с тези органи. Комисията разглежда също така значението на идентифицираните рискове за този продукт с цифрови елементи с оглед на своите задачи по отношение на координираните на равнището на Съюза оценки на риска за сигурността на критичните вериги на доставки, предвидени в член 22 от Директива (ЕС) 2022/2555, и при необходимост се консултира с групата за сътрудничество, създадена съгласно член 14 от Директива (ЕС) 2022/2555, и ENISA.

3. При обстоятелства, които оправдават незабавна намеса за запазване на правилното функциониране на вътрешния пазар, и когато Комисията има достатъчно основания да счита, че продуктът с цифрови елементи, 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 извършва оценка на съответствието и може да поиска от ENISA да предостави анализ в подкрепа на оценката. Комисията надлежно информира съответните органи за надзор на пазара. Съответните икономически оператори си сътрудничат при необходимост с ENISA.

4. Въз основа на оценката, посочена в параграф 3, 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).

5. Въз основа на консултацията, посочена в параграф 4 от настоящия член, Комисията може да приеме актове за изпълнение, за да предвиди корективни или ограничителни мерки на равнището на Съюза, включително изискващи засегнатите продукти с цифрови елементи да бъдат изтеглени от пазара или иззети, в разумен срок, съобразен с естеството на риска. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 62, параграф 2.

6. Комисията незабавно съобщава актовете за изпълнение, посочени в параграф 5, на съответния(те) икономически оператор(и). Държавите членки изпълняват тези актове за изпълнение без забавяне — и уведомяват Комисията за това.

7. Параграфи 3—6 се прилагат за срока на извънредната ситуация, която е оправдала намесата на Комисията, при условие че съответният продукт с цифрови елементи не бъде приведен в съответствие с настоящия регламент.

Член 57

Съответстващи продукти с цифрови елементи, които представляват значителен киберриск

1. Органът за надзор на пазара на държава членка изисква от икономическия оператор да предприеме всички подходящи мерки, когато след извършване на оценката съгласно член 54 установи, че въпреки че даден продукт с цифрови елементи и въведените от производителя процеси са в съответствие с настоящия регламент, той представлява значителен киберриск, както и риск за:

   а) здравето или безопасността на хората;

   б) спазването на задължения съгласно правото на Съюза или националното право, имащо за цел защитата на основните права;

в) наличността, автентичността, целостта или поверителността на услугите, предлагани чрез електронна информационна система от съществените субекти, както са посочени в член 3, параграф 1 от Директива (ЕС) 2022/2555; или

г) други аспекти на защитата на обществения интерес.

Мерките, посочени в първа алинея, може да включват мерки, с които да се гарантира, че съответният продукт с цифрови елементи и въведените от производителя процеси вече не представляват съответните рискове, когато се предоставят на пазара, съответният продукт с цифрови елементи се изтегля от пазара или се изземва, и са съизмерими с естеството на тези рискове.

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

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 посоченото в параграф 4 решение до държавите членки.

6. Когато Комисията има достатъчно основание 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 от настоящия член, тя уведомява и може да поиска от съответния орган или органи за надзор на пазара да извършат оценка и да следват процедурите, посочени в член 54 и параграфи 1, 2 и 3 от настоящия член.

7. При обстоятелства, които оправдават незабавна намеса за запазване на правилното функциониране на вътрешния пазар, и когато Комисията има достатъчно основания да счита, че продуктът с цифрови елементи, 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 извършва оценка на рисковете, свързани с този продукт с цифрови елементи и може да изиска от ENISA да предостави анализ в подкрепа на тази оценка, и информира съответните органи за надзор на пазара за това. Съответните икономически оператори си сътрудничат при необходимост с ENISA.

8. Въз основа на оценката, 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) икономически оператор(и).

9. Въз основа на консултацията, посочена в параграф 8 от настоящия член, Комисията може да приеме актове за изпълнение, за да вземе решение за корективни или ограничителни мерки на равнището на Съюза, включително изискващи засегнатите продукти с цифрови елементи да бъдат изтеглени от пазара или иззети, в разумен срок, съобразен с естеството на риска. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 62, параграф 2.

10. Комисията незабавно съобщава актовете за изпълнение, посочени в параграф 9, на съответния(те) икономически оператор(и). Държавите членки изпълняват тези актове за изпълнение 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 с цифрови елементи продължава да носи рисковете, посочени в параграф 1.

Член 58

Формално 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 „CE“ е нанесена в нарушение на член 29 или 30;

б) маркировката „CE“ 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 59

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 на пазара или предоставени на пазара, по-специално продукти с цифрови елементи, за които често се установява, че представляват киберрискове.

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

3. Органите за надзор на пазара и когато е приложимо, 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 съвместните дейности, извършени като част от предприето от него разследване.

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

Член 60

Мащабни проверки

1. Органите за надзор на пазара провеждат едновременни координирани действия за контрол („мащабни проверки“) на конкретни продукти или категории продукти с цифрови елементи, за да проверят съответствието с настоящия регламент или да открият нарушения на настоящия регламент. Тези мащабни проверки може да включват проверки на продукти с цифрови елементи, придобити под прикрита самоличност.

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

3. Когато при изпълнението на своите задачи, включително въз основа на уведомленията, получени съгласно член 14, параграфи 1 и 3, ENISA определи категории продукти с цифрови елементи, за които може да се организират мащабни проверки, тя представя предложение за такава проверка на координатора, посочен в параграф 2 от настоящия член, което се разглежда 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 52—58, и всички други правомощия, предоставени им от националното право.

5. Органите за надзор на пазара могат да канят 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 61

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 5, втора алинея, член 7, параграф 3, член 8, параграфи 1 и 2, член 13, параграф 8, четвърта алинея, член 14, параграф 9, член 25, член 27, параграф 9, член 28, параграф 5 и член 31, параграф 5 се предоставя на Комисията за срок от пет години, считано от ... [датата на влизане в сила на настоящия регламент]. Комисията изготвя доклад относно делегирането на правомощия не по-късно от девет месеца преди изтичането на петгодишния срок. Делегирането на правомощия се продължава мълчаливо за срокове с еднаква продължителност, освен ако Европейският парламент или Съветът не възразят срещу подобно продължаване не по-късно от три месеца преди изтичането на всеки срок.

3. Делегирането на правомощия, посочено в член 2, параграф 5, втора алинея, член 7, параграф 3, член 8, параграфи 1 и 2, член 13, параграф 8, четвърта алинея, член 14, параграф 9, член 25, член 27, параграф 9, член 28, параграф 5 и член 31, 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 5, втора алинея, член 7, параграф 3, член 8, параграфи 1 и 2, член 13, параграф 8, четвърта алинея, член 14, параграф 9, член 25, член 27, параграф 9, член 28, параграф 5 или член 31, 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. Посоченият срок може да се удължи с два месеца по инициатива на Европейския парламент или на Съвета.

Член 62

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 63

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 (ЕС) 2016/943 на Европейския парламент и на Съвета[36];

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

   в) обществения интерес и националната сигурност;

   г) независимостта на наказателните или административните производства.

[36] 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).

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 64

Санкции

1. Държавите членки установяват система от санкции, приложими при нарушение на настоящия регламент, и вземат всички мерки, необходими за осигуряване на прилагането им. Предвидените санкции трябва да бъдат ефективни, пропорционални и възпиращи. Държавите членки незабавно нотифицират на Комисията тези разпоредби и мерки и я нотифицират незабавно за всяко последващо изменение, което ги засяга.

2. Неспазването на съществените изисквания за киберсигурност, определени в приложение I, и неизпълнението на задълженията, установени в членове 13 и 14, се наказват с 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.

3. Неизпълнението на задълженията, посочени в членове 18—23, член 28, член 30, параграфи 1—4, член 31, параграфи 1—4, член 32, параграфи 1, 2 и 3, член 33, параграф 5, и членове 39, 41, 47, 49 и 53, се наказва с административна глоба 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.

4. Предоставянето на неправилна, непълна или подвеждаща информация в отговор на искане от нотифицираните органи и органите за надзор на пазара се наказва с административна глоба 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.

5. 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) характера, тежестта и продължителността на нарушението и последиците от него;

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

   в) размера, по-специално по отношение на микропредприятията и малките и средните предприятия, включително стартиращите предприятия, и пазарния дял на икономическия оператор, извършил нарушението.

6. Органите за надзор на пазара, които налагат административни глоби, съобщават за това на органите за надзор на пазара на други държави членки чрез информационната и комуникационна система, посочена в член 34 от Регламент (ЕС) 2019/1020.

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

8. 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.

9. В зависимост от обстоятелствата във всеки отделен случай, административните глоби могат да бъдат наложени в допълнение към други корективни или ограничителни мерки, приложени от органите за надзор на пазара за същото нарушение.

10. Чрез дерогация от параграфи 3—9 административните глоби, посочени в тези параграфи, не се прилагат за:

    а) производители, квалифицирани като микропредприятия или малки предприятия, при неспазване на срока, посочен в член 14, параграф 2, буква а) или член 14, параграф 4, буква а);

    б) всяко нарушение на настоящия регламент, извършено от попечители на софтуер с отворен код.

Член 65

Представителни искове

Директива (ЕС) 2020/1828 се прилага по отношение на представителните искове, подадени за нарушения от страна на икономически оператори на разпоредбите на настоящия регламент, които засягат или могат да засегнат колективните интереси на потребителите.

Глава VIII

Преходни и заключителни разпоредби

Член 66

Изменение на Регламент (ЕС) 2019/1020

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

„XX[+]. Регламент (ЕС) 2024/... на Европейския парламент и на Съвета*[++].

---

* Регламент (ЕС) 2024/... на Европейския парламент и на Съвета от ... относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на регламенти (ЕС) № 168/2013 и (ЕС) 2019/1020 и Директива (ЕС) 2020/1828 (Акт за киберустойчивост) (ОВ ..., ELI: ...).“

[+] ОВ: Моля, въведете в текста следващия пореден номер в списъка, съдържащ се в приложение I към Регламент (ЕС) 2019/1020.

[++] ОВ: моля, въведете в текста номера на регламента, съдържащ се в документ PE-CONS 100/23 (2022/0272(COD)), и добавете в бележката под линия номера, датата и данните за публикацията в ОВ на този регламент.

Член 67

Изменение на Директива (ЕС) 2020/1828

В приложение I към Директива (ЕС) 2020/1828 се добавя следната точка:

„ (XX[+]) Регламент (ЕС) 2024/... на Европейския парламент и на Съвета*[++]“.

---

* Регламент (ЕС) 2024/... на Европейския парламент и на Съвета от ... относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на регламенти (ЕС) № 168/2013 и (ЕС) 2019/1020 и Директива (ЕС) 2020/1828 (Акт за киберустойчивост) (ОВ ..., ELI: ...).“

[+] ОВ: Моля, въведете в текста следващия пореден номер в списъка, съдържащ се в приложение I към Директива (ЕС) 2020/1828.

[++] ОВ: моля, въведете в текста номера на регламента, съдържащ се в документ PE-CONS 100/23 (2022/0272(COD)) и добавете в бележката под линия номера, датата и данните за публикацията в ОВ на този регламент.

Член 68

Изменение на Регламент (ЕС) № 168/2013

Приложение II към Регламент (ЕС) № 168/2013 на Европейския парламент и на Съвета[37] се изменя, както следва:

в част B1 в таблицата се добавя следното вписване:

„

XX+	18	Защита на превозното средство срещу кибератаки		x	x	x	x	x	x	x	x	x	x	x	x	x	x

“

[37] Регламент (ЕС) № 168/2013 на Европейския парламент и на Съвета от 15 януари 2013 г. относно одобряването и надзора на пазара на дву-, три- и четириколесни превозни средства (ОВ L 60, 2.3.2013 г., стр. 52).

[+] ОВ: Моля, въведете в текста следващия пореден номер в списъка под заглавие B1 в приложение II към Регламент (ЕС) № 168/2013.

Член 69

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 законодателство на Съюза за хармонизация, различно от настоящия регламент, остават валидни до ... [42 месеца от датата на влизане в сила на настоящия регламент], освен ако срокът им на валидност изтича преди тази дата или ако е предвидено друго в друго подобно законодателство на Съюза за хармонизация, в който случай те остават валидни, както е посочено в това законодателство.

2. Продукти с цифрови елементи, които са пуснати на пазара преди ... [36 месеца от датата на влизане в сила на настоящия регламент], подлежат на изискванията, установени в настоящия регламент, само ако от тази дата посочените продукти са предмет на съществено изменение.

3. Като изключение от параграф 2 от настоящия член, задълженията по член 14 се прилагат за всички продукти с цифрови елементи, които попадат в обхвата на настоящия регламент и които са били пуснати на пазара преди ... [36 от датата на влизане в сила на настоящия регламент].

Член 70

Оценка и преглед

1. В срок до ... [72 месеца от датата на влизане в сила 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.

2. В срок до ... [45 месеца от датата на влизане в сила на настоящия регламент] Комисията, след консултация с ENISA и мрежата на ЕРИКС, представя на Европейския парламент и на Съвета доклад, в който се оценява ефективността на единната платформа за докладване, посочена в член 16, както и въздействието от прилагането на основанията, свързани с киберсигурността, посочени в член 16, параграф 2, от страна на определените за координатори ЕРИКС, върху ефективността на единната платформа за докладване по отношение на навременното разпространение на получените уведомления до други съответни ЕРИКС.

Член 71

Влизане в сила и прилагане

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

2. Настоящият регламент се прилага от ... [36 месеца от датата на влизане в сила на настоящия регламент].

   Член 14 обаче се прилага от ... [21 месеца от датата на влизане в сила на настоящия регламент], а Глава IV (членове 35—51) се прилага от ... [18 месеца от датата на влизане в сила на настоящия регламент].

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

Съставено в ...

За Европейския парламент	*За Съвета*
Председател	*Председател*

ПРИЛОЖЕНИЕ I

СЪЩЕСТВЕНИ ИЗИСКВАНИЯ ЗА КИБЕРСИГУРНОСТ

Част I Изисквания за киберсигурност, свързани със свойствата на продуктите, съдържащи цифрови елементи

(1) Продуктите с цифрови елементи се проектират, разработват и произвеждат по такъв начин, че да гарантират подходящо ниво на киберсигурност въз основа на рисковете;

(2) Въз основа на оценката на киберриска, посочена в член 13, параграф 2, и когато е приложимо, продуктите с цифрови елементи:

а) се предоставят на пазара без уязвимости, които са вече известни и могат да бъдат използвани;

б) се предоставят на пазара с настройки за сигурност по подразбиране, освен ако между производителя и стопанския ползвател е договорено друго във връзка с индивидуализиран продукт с цифрови елементи, включително възможност за възстановяване на продукта до първоначалното му състояние;

в) осигуряват възможност да се отстраняват уязвимостите чрез актуализации за сигурност, включително, когато е приложимо, чрез активирана по подразбиране настройка за инсталиране в подходящи срокове на автоматични актуализации за сигурност, с ясен и лесен за използване механизъм за отказ от това, както и чрез уведомяване на потребителите за наличните актуализации и възможността за временното им отлагане;

г) гарантират защита от непозволен достъп чрез подходящи механизми за контрол, включително, но не само, системи за управление на удостоверяването на автентичност, самоличността и достъпа, и докладват за евентуален непозволен достъп;

д) защитават поверителността на съхранени, предадени или обработени по друг начин данни, лични или други, като например чрез криптиране на съответните данни в покой или при пренос чрез най-съвременните механизми и чрез използване на други технически средства;

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

ж) обработват само данни, лични или други, които са подходящи, свързани със и ограничени до необходимото във връзка с предназначението на продукта с цифрови елементи („свеждане на данните до минимум“);

з) защитават наличието на основни и базисни функции, също така и след инцидент, включително чрез мерки за устойчивост срещу и смекчаване на въздействието на атаки за отказ на услуга;

и) ограничават до минимум отрицателното въздействие на самите продукти или на свързани устройства върху наличието на услуги, предоставяни от други устройства или мрежи;

й) са проектирани, разработени и произведени по такъв начин, че да бъдат ограничени повърхностите, уязвими за атаки, включително външните интерфейси;

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

л) осигуряват информация, свързана със сигурността, посредством възможности за записване и наблюдение на съответната вътрешна дейност, включително достъпа до данни, услуги или функции или тяхната промяна, с механизъм за отказ за ползвателя;

м) предоставят възможност на потребителите сигурно и лесно да премахват по траен начин всички данни и настройки, а когато тези данни могат да бъдат прехвърлени към други продукти или системи, гарантират, че това се извършва по сигурен начин.

Част II Изисквания относно отстраняването на уязвимости

Производителите на продукти с цифрови елементи:

(1) идентифицират и документират уязвимостите и компонентите, съдържащи се в продуктите с цифрови елементи, включително чрез изготвяне на опис на софтуерните компоненти в общоприет и машинночитаем формат, обхващащ най-малко зависимостите на продуктите на най-високо равнище;

(2) във връзка с рисковете за продуктите с цифрови елементи, незабавно предприемат действия и отстраняват уязвимостите, включително чрез осигуряване на актуализации за сигурност, когато това е технически осъществимо, новите актуализации за сигурност се предоставят отделно от актуализациите на функционалните възможности;

(3) изпълняват ефективни и редовни проверки и прегледи на сигурността на продукта с цифрови елементи;

(4) след като бъде предоставена актуализация за сигурност, споделят и публично разкриват информация за коригираните уязвимости, включително описание на уязвимостите, информация, която дава възможност на ползвателите да идентифицират засегнатия продукт с цифрови елементи, въздействието на уязвимостите, тяхната сериозност и ясна и достъпна информация, помагаща на ползвателите да коригират уязвимостите; в надлежно обосновани случаи, когато производителите считат, че рисковете за сигурността поради публикуването превишават ползите за сигурността, те могат да отложат публичното оповестяване на информация относно отстранена уязвимост, докато на потребителите бъде дадена възможност да приложат съответната софтуерна поправка;

(5) въвеждат и прилагат политика относно координирано оповестяване на уязвимости;

(6) предприемат мерки за улесняване на споделянето на информация за потенциалните уязвимости в техния продукт с цифрови елементи, както и в компоненти на трети страни, съдържащи се в този продукт, включително чрез предоставяне на адрес за контакт за докладване на уязвимостите, открити в продукта с цифрови елементи;

(7) предоставят механизми за сигурно разпространение на актуализации за продукти с цифрови елементи, за да се гарантира, че уязвимостите са коригирани или въздействието им е смекчено своевременно и когато е приложимо за актуализациите за сигурност, по автоматичен начин;

(8) гарантират, че когато са налични актуализации на защитата с цел преодоляване на установени проблеми със сигурността, те се разпространяват незабавно и — освен ако между производител и стопански ползвател е договорено друго във връзка с индивидуализиран продукт с цифрови елементи — безплатно, придружени от информационни съобщения, предоставящи на ползвателите необходимата информация, включително относно потенциалните действия, които трябва да бъдат предприети.

ПРИЛОЖЕНИЕ II

ИНФОРМАЦИЯ И УКАЗАНИЯ ЗА ПОЛЗВАТЕЛЯ

Като минимум продуктът с цифрови елементи се придружава от:

1. името, регистрираното търговско наименование или регистрираната търговска марка на производителя, пощенския адрес, адреса на електронна поща или друг цифров начин за контакт, както и уебсайта, на който може да се осъществи контакт с производителя, ако съществува такъв;

2. единния център за контакт, където може да бъде докладвана и получена информация за уязвимости в киберсигурността на продукта с цифрови елементи и където може да бъде намерена политиката на производителя по отношение на координираното оповестяване на уязвимости;

3. наименование, тип и всякаква допълнителна информация, позволяваща уникалната идентификация на продукта с цифрови елементи;

4. предназначението на продукта с цифрови елементи, включително средата на сигурност, осигурена от производителя, както и основните функции на продукта и информация за параметрите на сигурността;

5. известните или предвидимите обстоятелства, свързани с използването на продукта с цифрови елементи в съответствие с предназначението му или в условия на разумно предвидима неправилна употреба, които могат да доведат до значими киберрискове;

6. когато е приложимо, интернет адреса, на който може да бъде намерена ЕС декларацията за съответствие;

7. вида на техническата поддръжка за сигурност, предлагана от производителя, и крайната дата на периода на поддръжка, през който ползвателите могат да очакват да бъдат отстранявани уязвимостите и да получават актуализации за сигурност;

8. подробни инструкции или интернет адрес, препращащ към такива подробни инструкции и информация за:

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

   б) по какъв начин промените в продукта с цифрови елементи могат да засягат сигурността на данните,

   в) това как да се инсталират актуализациите, свързани със сигурността,

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

   д) това как може да се изключи настройката по подразбиране, позволяваща автоматичното инсталиране на актуализации за сигурност, както се изисква в приложение I, част I, точка 2, буква в),

   е) когато продуктът с цифрови елементи е предназначен за интегриране в други продукти с цифрови елементи — информацията, необходима на интегратора, за да спази съществените изисквания за киберсигурност, посочени в приложение I, и изискванията за документацията, съдържащи се в приложение VII;

9. ако производителят реши да предостави на потребителя опис на софтуерните компоненти, информация къде може да бъде получен достъп до въпросния опис на софтуерните компоненти.

ПРИЛОЖЕНИЕ III

ВАЖНИ ПРОДУКТИ С ЦИФРОВИ ЕЛЕМЕНТИ

Клас I

1. Системи за управление на самоличността и софтуер и хардуер за управление на привилегирован достъп, включително четци за автентификация и контрол на достъпа, включително биометрични четци;

2. Отделни и вградени браузъри;

3. Мениджъри на пароли;

4. Софтуер, който търси, премахва или поставя под карантина зловреден софтуер;

5. Продукти с цифрови елементи с функцията виртуална частна мрежа (VPN);

6. Системи за управление на мрежата;

7. Системи за управление на информацията за безопасност и на събитията, свързани със сигурността;

8. Мениджъри за зареждане;

9. Инфраструктура на публичния ключ и софтуер за издаване на електронни сертификати;

10. Физически и виртуални мрежови интерфейси;

11. Операционни системи;

12. Маршрутизатори, модеми, предназначени за връзка с интернет, и комутатори;

13. Микропроцесори с функционални възможности, свързани със сигурността;

14. Микроконтролери с функционални възможности, свързани със сигурността;

15. Интегрални схеми, специфични за приложенията (ASIC), и програмируеми логически матрици (FPGA) с функционални възможности, свързани със сигурността;

16. Виртуални асистенти с общо предназначение за интелигентни домове;

17. Продукти за интелигентни домове с функции за сигурност, включително интелигентни ключалки за врати, камери за сигурност, системи за наблюдение на бебето и алармени системи;

18. Свързани с интернет играчки, обхванати от Директива 2009/48/ЕО на Европейския парламент и на Съвета[1], които имат социални интерактивни характеристики (напр. говорене или заснемане) или които имат функции за проследяване на местоположението;

19. Лични устройства за прикрепване към тялото, предназначени да се носят или поставят върху човешкото тяло с цел наблюдение на здравето (например проследяване) и за които не се прилага нито Регламент (ЕС) 2017/745, нито Регламент (ЕС) 2017/746, или лични устройства за прикрепване към тялото, предназначени за употреба от и за деца.

Клас II

1. Хипервайзори и системи за изпълнение на контейнери, които поддържат виртуализация на операционни системи и подобни среди;

2. Защитни стени, системи за установяване и/или предотвратяване на проникване;

3. Защитени от външна намеса микропроцесори;

4. Защитени от външна намеса микроконтролери.

---

[1] Директива **2009/48**/**ЕО** на Европейския парламент и на Съвета от 18 юни 2009 г. относно безопасността на детските играчки (ОВ L 170, 30.6.2009 г., стр. 1).

ПРИЛОЖЕНИЕ IV

КРИТИЧНИ ПРОДУКТИ С ЦИФРОВИ ЕЛЕМЕНТИ

1. Хардуерни устройства с кутии за сигурност;

2. Шлюзове за интелигентни измервателни уреди в рамките на интелигентни измервателни системи съгласно определението в член 2, точка 23 от Директива (ЕС) 2019/944 на Европейския парламент и на Съвета[1], и други устройства за целите на усъвършенстваната сигурност, включително за сигурна криптообработка;

3. Смарткарти или подобни устройства, включително защитени елементи.

---

[1] Директива (ЕС) 2019/944 на Европейския парламент и на Съвета от 5 юни 2019 г. относно общите правила за вътрешния пазар на електроенергия и за изменение на Директива 2012/27/ЕС (ОВ L 158, 14.6.2019 г., стр. 125).

ПРИЛОЖЕНИЕ V

ЕС ДЕКЛАРАЦИЯ ЗА СЪОТВЕТСТВИЕ

ЕС декларацията за съответствие по член 28 съдържа цялата посочена по-долу информация:

1. наименование, тип и всякаква допълнителна информация за уникалната идентификация на продукта с цифрови елементи;

2. име и адрес на производителя или на упълномощения от него представител;

3. изявление, че единствено доставчикът носи отговорност за издадената ЕС декларация за съответствие;

4. предмет на декларацията (идентификация на продукта с цифрови елементи, позволяваща проследяването му, която при необходимост може да включва снимка);

5. изявление, че описаният по-горе предмет на декларацията е в съответствие с приложимото законодателство на Съюза за хармонизация;

6. позоваване на използваните хармонизирани стандарти или на други общи спецификации или сертифициране за киберсигурност, по отношение на които се декларира съответствие;

7. когато е приложимо, наименование и номер на нотифицирания орган, описание на извършената процедура за оценяване на съответствието и идентификация на издадения сертификат;

8. Допълнителна информация:

Подписано за и от името на:……

(място и дата на издаване):

(име, длъжност) (подпис):

ПРИЛОЖЕНИЕ VI

ОПРОСТЕНА ЕС ДЕКЛАРАЦИЯ ЗА СЪОТВЕТСТВИЕ

Опростената ЕС декларация за съответствие, посочена в член 13, параграф 20, се предоставя в следния вид:

С настоящото [наименование на производителя] декларира, че типът продукт с цифрови елементи [обозначение на типа продукт с цифров елемент] е в съответствие с Регламент (ЕС) .../... на Европейския парламент и на Съвета[1].

Пълният текст на ЕС декларацията за съответствие може да се намери на следния интернет адрес:

---

[1] ОВ: Моля, въведете в текста номера на регламента, съдържащ се в документ PE-CONS №/YY (2022/0272(COD)).

ПРИЛОЖЕНИЕ VII

СЪДЪРЖАНИЕ НА ТЕХНИЧЕСКАТА ДОКУМЕНТАЦИЯ

Техническата документация по член 31 съдържа най-малко следната информация, приложима за съответния продукт с цифрови елементи:

1. Общо описание на продукта с цифрови елементи, включително:

   а) неговото предназначение,

   б) версии на софтуера, които засягат съответствието със съществените изисквания за киберсигурност,

   в) в случаите когато продуктът с цифрови елементи е хардуерен продукт, снимки или илюстрации, показващи външните характеристики, маркировките и вътрешната схема,

   г) информация и указания за ползвателите, както е посочено в приложение II.

2. Описание на проектирането, разработването и производството на продукта с цифрови елементи и на процесите на отстраняване на уязвимостите, включително:

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

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

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

3. Оценка на киберрисковете, срещу които продуктът с цифрови елементи е проектиран, разработен, произведен, доставен и поддържан съгласно член 13, включително по какъв начин са приложими съществените изисквания за киберсигурност, определени в приложение I, част I.

4. Съответната информация, която е била взета предвид за определяне на периода на поддръжка на продукта с цифрови елементи съгласно член 13, параграф 8.

5. Списък на приложените изцяло или частично хармонизирани стандарти, данните за които са публикувани в *Официален вестник на Европейския съюз*, общите спецификации, посочени в член 27 от настоящия Регламент, или европейските схеми за сертифициране на киберсигурността, приети съгласно Регламент (ЕС) 2019/881 съгласно член 27, параграф 8 от настоящия регламент, а в случаите, когато тези хармонизирани стандарти, общи спецификации или схеми за сертифициране на киберсигурността не са били приложени — описания на решенията, приети за изпълнение на съществените изисквания за киберсигурност, определени в приложение I, части I и II, включително списък на приложените други подходящи технически спецификации. При частично приложени хармонизирани стандарти, общи спецификации или европейски схеми за сертифициране на киберсигурността, в техническата документация се посочват частите, които са били приложени.

6. Докладите от изпитванията, извършени с цел проверка на съответствието на продукта с цифрови елементи и на процесите за отстраняване на уязвимостите с приложимите съществени изисквания за киберсигурност, определени в приложение I, части I и II.

7. Копие на ЕС декларацията за съответствие.

8. Когато е приложимо, опис на софтуерните компоненти при обосновано искане от страна на орган за надзор на пазара, при условие че това е необходимо, за да може този орган да проверява съответствието със съществените изисквания за киберсигурност, определени в приложение I.

ПРИЛОЖЕНИЕ VIII

ПРОЦЕДУРИ ЗА ОЦЕНЯВАНЕ НА СЪОТВЕТСТВИЕТО

Част I Процедура за оценяване на съответствието въз основа на вътрешен контрол (въз основа на модул А)

1. Вътрешният контрол е процедурата за оценяване на съответствието, чрез която производителят изпълнява задълженията, установени в точки 2, 3 и 4 от настоящата част, и гарантира и декларира на своя отговорност, че продуктите с цифрови елементи отговарят на всички съществени изисквания за киберсигурност, определени в приложение I, част I, както и че производителят отговаря на съществените изисквания за киберсигурност, определени в приложение I, част II.

2. Производителят изготвя техническата документация, описана в приложение VII.

3. Проектиране, разработване, производство и отстраняване на уязвимостите на продукти с цифрови елементи

   Производителят взема всички необходими мерки за това процесите по проектиране, разработване, производство и отстраняване на уязвимостите и тяхното наблюдение да гарантират съответствието на произвежданите или разработваните продукти с цифрови елементи и на въведените от производителя процеси със съществените изисквания за киберсигурност, определени в приложение I, части I и II.

4. Маркировка за съответствие и декларация за съответствие

4.1. Производителят поставя маркировката „CE“ върху всеки отделен продукт с цифрови елементи, който отговаря на приложимите изисквания, установени в настоящия Регламент.

4.2. Производителят изготвя писмена ЕС декларация за съответствие за всеки продукт с цифрови елементи в съответствие с член 28 и я съхранява заедно с техническата документация на разположение на националните органи в продължение на 10 години след пускането на продукта с цифрови елементи на пазара или през очаквания експлоатационен срок на продукта или периода на поддръжка, в зависимост от това кой период е по-дълъг. В ЕС декларацията за съответствие се посочва продуктът с цифрови елементи, за който е изготвена. Копие от ЕС декларацията за съответствие се предоставя на съответните органи при поискване.

5. Упълномощени представители

Задълженията на производителя по точка 4 могат да бъдат изпълнявани от негов упълномощен представител, от негово име и на негова отговорност, при условие че съответните задължения са конкретно посочени в пълномощното.

Част II ЕС изследване на типа (въз основа на модул B)

1. ЕС изследване на типа е част от процедура за оценяване на съответствието, в която нотифициран орган проверява техническия проект и разработването на продукт с цифрови елементи и процесите за отстраняването на уязвимостите, въведени от производителя, и удостоверява, че продукт с цифрови елементи отговаря на съществените изисквания за киберсигурност, определени в приложение I, част I, както и че производителят отговаря на съществените изисквания за киберсигурност, определени в приложение I, част II.

2. ЕС изследване на типа се извършва чрез оценка на пригодността на техническия проект и на разработването на продукта с цифрови елементи чрез изследване на техническата документация и подкрепящите доказателства по точка 3, с изследване на образци от една или повече основни части на продукта (комбинация от производствен тип и проектен тип).

3. Производителят подава заявление за ЕС изследване на типа само до един нотифициран орган по свой избор.

   Заявлението включва:

   3.1 името и адреса на производителя, а в случаите, в които заявлението е подадено от упълномощения представител — и неговото име и адрес,

3.2 писмена декларация, че същото заявление не е подадено до друг нотифициран орган,

3.3 техническата документация, която позволява да се направи оценка на съответствието на продукта с цифрови елементи с приложимите съществени изисквания за киберсигурност, определени в приложение I, част I, и на процесите на отстраняване на уязвимостите на производителя, посочени в приложение I, част II, и включва подходящ анализ и оценка на рисковете. В техническата документация се посочват приложимите изисквания и се обхващат — доколкото е необходимо за оценката — проектирането, производството и експлоатацията на продукта с цифрови елементи. Техническата документация съдържа, когато е приложимо, като минимум елементите, определени в приложение VII,

3.4 подкрепящите доказателства за пригодност на техническите решения за проекта и разработването и на процесите на отстраняване на уязвимостите. В тези подкрепящи доказателства се посочват всички използвани документи, по-специално в случаите, когато съответните хармонизирани стандарти или технически спецификации не са били приложени изцяло. Когато е необходимо, подкрепящите доказателства включват резултатите от изпитванията, проведени от подходяща лаборатория на производителя или от друга лаборатория от негово име и на негова отговорност.

4. Нотифицираният орган:

4.1. разглежда техническата документация и подкрепящите доказателства, за да направи оценка на съответствието на техническия проект и на разработката на продукта с цифрови елементи със съществените изисквания за киберсигурност, определени в приложение I, част I, както и на въведените от производителя процеси на отстраняване на уязвимостите със съществените изисквания за киберсигурност, определени в приложение I, част II,

4.2. удостоверява, че образците са разработени или произведени в съответствие с техническата документация, и определя елементите, проектирани и разработени в съответствие с приложимите разпоредби на съответните хармонизирани стандарти или технически спецификации, както и елементите, които са проектирани и разработени без прилагане на съответните разпоредби на тези стандарти,

4.3. извършва подходящи изследвания и изпитвания или организира извършването им с цел да се увери, че в случаите, когато производителят е предпочел да приложи решенията от съответните хармонизирани стандарти или технически спецификации по отношение на изискванията, посочени в приложение I, същите са били приложени правилно,

4.4. извършва подходящи изследвания и изпитвания или организира извършването им с цел да се увери, че в случаите, когато решенията от съответните хармонизирани стандарти или технически спецификации по отношение на изискванията, посочени в приложение I, не са приложени, решенията, избрани от производителя, отговарят на съответните съществени изисквания за киберсигурност,

4.5. съгласува с производителя мястото, където да се извършат изследванията и изпитванията.

5. Нотифицираният орган изготвя доклад от оценката, в който описва действията, предприети съгласно точка 4, и получените резултати. Без да се нарушават задълженията му по отношение на нотифициращите органи, нотифицираният орган разгласява изцяло или отчасти съдържанието на доклада само със съгласието на производителя.

6. Когато типът и процесите на отстраняване на уязвимостите отговарят на съществените изисквания за киберсигурност, определени в приложение I, нотифицираният орган издава на производителя сертификат за ЕС изследване на типа. Сертификатът съдържа името и адреса на производителя, заключенията от изследването, условията (ако има такива) за неговата валидност, необходимите данни за идентификация на одобрения тип и на процесите на отстраняване на уязвимостите. Сертификатът може да съдържа едно или повече приложения.

Сертификатът и приложенията към него съдържат цялата необходима информация, за да може да бъде оценено съответствието на произведените или разработените продукти с цифрови елементи с изследвания тип и процеси на отстраняване на уязвимости, и да се даде възможност за контрол по време на експлоатация.

Когато типът и процесите на отстраняване на уязвимости не отговарят на приложимите съществени изисквания за киберсигурност, определени в приложение I, нотифицираният орган отказва издаването на сертификат за ЕС изследване на типа и информира заявителя по надлежния ред, като подробно мотивира отказа си.

7. Нотифицираният орган следи за евентуални промени в общоприетото ниво на технически познания, които показват, че има вероятност одобреният тип и процесите на отстраняване на уязвимости вече да не отговарят на приложимите съществени изисквания за киберсигурност, определени в приложение I към настоящия Регламент, и преценява дали е необходимо по-нататъшно проучване на такива промени. Ако това е така, нотифицираният орган информира производителя по съответния начин.

Производителят информира нотифицирания орган, у когото се намира техническата документация, отнасяща се до сертификата за ЕС изследване на типа, за всички промени на одобрения тип и на процесите на отстраняване на уязвимостите, които могат да повлияят на съответствието със съществените изисквания за киберсигурност, определени в приложение I, или на условията за валидност на сертификата. Такива промени изискват допълнително одобрение под формата на допълнение към оригиналния сертификат за ЕС изследване на типа.

8. Нотифицираният орган извършва периодични одити, за да гарантира, че процесите за отстраняване на уязвимости, посочени в приложение I, част II, се прилагат по подходящ начин.

9. Всеки нотифициран орган информира своите нотифициращи органи за сертификатите за ЕС изследване на типа и за допълненията към тях, които е издал или отнел, и периодично или при поискване предоставя на нотифициращите органи списъка на сертификатите и допълненията към тях, които е отказал, временно прекратил или ограничил по някакъв друг начин.

Всеки нотифициран орган информира останалите нотифицирани органи за сертификатите за ЕС изследване на типа и за допълненията към тях, които е отказал, отнел, временно прекратил или ограничил по някакъв друг начин, а при поискване — и за сертификатите и допълненията към тях, които е издал.

Комисията, държавите членки и останалите нотифицирани органи могат при поискване да получат копие от сертификатите за ЕС изследване на типа и от всички допълнения към тях. При поискване Комисията и държавите членки могат да получат копие от техническата документация и резултатите от проведените от нотифицирания орган изследвания. Нотифицираният орган съхранява копие от сертификата за ЕС изследване на типа, неговите приложения и допълнения, както и техническото досие, включващо документацията, представена от производителя, до изтичане на валидността на сертификата.

10. Производителят съхранява копие от сертификата за ЕС изследване на типа, неговите приложения и допълнения заедно с техническата документация на разположение на националните органи в продължение на 10 години след пускането на продукта с цифрови елементи на пазара или в продължение на периода на поддръжка, в зависимост от това, кой е по-дълъг.

11. Упълномощеният представител на производителя може да подава заявлението по точка 3 и да изпълнява задълженията по точки 7 и 10, при условие че съответните задължения са конкретно посочени в пълномощното.

Част III Съответствие с типа въз основа на вътрешен производствен контрол (въз основа на модул C)

1. Съответствието с типа въз основа на вътрешен производствен контрол е тази част от процедурата за оценяване на съответствието, чрез която производителят изпълнява задълженията, установени в точки 2 и 3 от настоящата част, и гарантира и декларира, че съответните продукти с цифрови елементи са в съответствие с типа, описан в сертификата за ЕС изследване на типа, и отговарят на съществените изисквания за киберсигурност, определени в приложение I, част I и че производителят изпълнява съществените изисквания за киберсигурност, посочени в приложение I, част II.

2. Производство

Производителят взема всички необходими мерки за това производството и неговото наблюдение да осигурят съответствието на произвежданите продукти с цифрови елементи с одобрения тип, описан в сертификата за ЕС изследване на типа, и със съществените изисквания за киберсигурност, определени в приложение I, част I, и да гарантират, че производителят отговаря на съществените изисквания за киберсигурност, определени в приложение I, част II.

3. Маркировка за съответствие и декларация за съответствие

3.1. Производителят поставя маркировката „CE“ върху всеки отделен продукт с цифрови елементи, който е в съответствие с типа, описан в сертификата за ЕС изследване на типа, и което отговаря на приложимите изисквания, установени в нормативния акт.

3.2. Производителят изготвя писмена декларация за съответствие за образец от продукта и я съхранява на разположение на националните органи в продължение на 10 години след пускането на продукта с цифрови елементи на пазара или в продължение на периода на поддръжка, в зависимост от това кой е по-дълъг. Декларацията за съответствие идентифицира образеца от продукта, за който е изготвена. Копие от декларацията за съответствие се предоставя на съответните органи при поискване.

4. Упълномощен представител

Задълженията на производителя по точка 3 могат да бъдат изпълнявани от негов упълномощен представител, от негово име и на негова отговорност, при условие че съответните задължения са конкретно посочени в пълномощното.

Част IV Съответствие въз основа на пълно осигуряване на качеството (въз основа на модул H)

1. Съответствие въз основа на пълно осигуряване на качеството е процедурата за оценяване на съответствието, чрез която производителят изпълнява задълженията, установени в точки 2 и 5 от настоящата част, и гарантира и декларира на своя отговорност, че съответните продукти с цифрови елементи (или продуктови категории) отговарят на съществените изисквания за киберсигурност, определени в приложение I, част I, както и че процесите на отстраняване на уязвимостите, въведени от производителя, отговарят на изискванията, посочени в приложение I, част II.

2. Проектиране, разработване, производство и отстраняване на уязвимостите на продукти с цифрови елементи

Производителят разполага с одобрена система за управление на качеството, както е посочено в точка 3, за проектирането, разработването и крайния контрол и изпитване на съответните продукти с цифрови елементи и за отстраняването на уязвимости, поддържа нейната ефективност през периода на поддръжка и подлежи на надзор, както е посочено в точка 4.

3. Система за управление на качеството

3.1. Производителят подава заявление за оценяване на неговата система за управление на качеството по отношение на съответните продукти с цифрови елементи до нотифициран орган по свой избор.

Заявлението включва:

– името и адреса на производителя, а в случаите, в които заявлението е подадено от упълномощения представител — и неговото име и адрес,

– техническата документация за един образец от всяка категория продукти с цифрови елементи, чието производство или разработване се предвижда. Техническата документация съдържа, когато е приложимо, като минимум елементите, посочени в приложение VII,

– документацията относно системата за управление на качеството и

– писмена декларация, че същото заявление не е подадено до друг нотифициран орган.

3.2. Системата за управление на качеството осигурява съответствието на продуктите с цифрови елементи със съществените изисквания за киберсигурност, определени в приложение I, част I, и съответствието на въведените от производителя процеси на отстраняване на уязвимостите с изискванията, посочени в приложение I, част II.

Всички елементи, изисквания и предписания, приети от производителя, се документират редовно и систематично под формата на писмени политики, процедури и инструкции. Документацията на системата за управление на качеството позволява еднозначно тълкуване на програмите, плановете, наръчниците и записите във връзка с контрола на качеството.

По-конкретно тя включва достатъчно описание на:

– целите във връзка с качеството и организационната структура, отговорностите и правомощията на ръководството по отношение на проектирането, разработването, качеството на продукта и отстраняването на уязвимостите,

– техническите спецификации на проекта и разработването, включително стандарти, които ще бъдат приложени, а когато съответните хармонизирани стандарти и/или технически спецификации няма да бъдат приложени изцяло, средствата, които ще се използват за осигуряване съответствието на продуктите с цифрови елементи със съществените изисквания за киберсигурност, определени в приложение I, част I,

– спецификациите на процедурите, включително стандарти, които ще бъдат приложени, а когато съответните хармонизирани стандарти и/или технически спецификации няма да бъдат приложени изцяло, средствата, които ще се използват за осигуряване съответствието на производителя със съществените изисквания за киберсигурност, определени в приложение I, част II,

– контролът на проектирането и разработката, както и техниките, процесите и системните действия за проверка на проекта и разработката, които ще бъдат използвани при проектирането и разработването на продуктите с цифрови елементи, принадлежащи към обхванатата продуктова категория,

– съответните техники на производство, контрол на качеството и осигуряване на качеството, процесите и системните действия, които ще се използват,

– изследванията и изпитванията, които ще се извършват преди, по време на и след производството, и честотата с която ще се извършват,

– записите по качеството, като доклади от проверки и данни от изпитвания, данни за калибриране и доклади за квалификацията на съответния персонал,

– средствата за наблюдение за постигане на изискваното качество на проекта и на продукта, и за ефективното функциониране на системата за управление на качеството.

3.3. Нотифицираният орган оценява системата за управление на качеството, за да определи дали тя отговаря на изискванията, посочени в точка 3.2.

По отношение на елементите на системата за управление на качеството, които отговарят на съответните спецификации на националния стандарт, който въвежда съответния хармонизиран стандарт или технически спецификации нотифицираният орган приема, че е налице съответствие с посочените по-горе изисквания.

В допълнение към опита в системи за управление на качеството, екипът одитори разполага най-малко с един член с опит в оценяването на съответната продуктова област и технологията на продукта, както и притежава познания за приложимите изисквания, установени в настоящия регламент. Одитът включва посещение за оценка в помещенията на производителя, когато такива помещения съществуват. Екипът одитори извършва преглед на техническата документация по точка 3.1, второ тире с цел да установи способността на производителя да определи приложимите изисквания, установени в настоящия регламент, и да проведе необходимите изследвания, за да осигури съответствието на продукта с цифрови елементи с тези изисквания.

Решението се съобщава на производителя или на неговия упълномощен представител.

Уведомлението съдържа заключенията от одита и мотивирано решение относно извършеното оценяване.

3.4. Производителят се задължава да изпълнява задълженията, произтичащи от одобрената система за управление на качеството, както и да я поддържа в състояние на пригодност и ефикасно функциониране.

3.5. Производителят редовно информира нотифицирания орган, одобрил системата за управление на качеството, за всякакви планирани изменения в нея.

Нотифицираният орган оценява предложените изменения и решава дали изменената система за управление на качеството ще продължи да отговаря на изискванията по точка 3.2, или се налага ново оценяване.

Той уведомява производителя за своето решение. Уведомлението включва заключенията от извършеното изследване и мотивирано решение относно извършеното оценяване.

4. Надзор под отговорността на нотифицирания орган

4.1. Целта на надзора е да се гарантира, че производителят изпълнява правилно задълженията, произтичащи от одобрената система за управление на качеството.

4.2. За целите на оценката производителят предоставя достъп на нотифицирания орган до местата на проектиране, разработване, производство, проверка, изпитване и съхраняване и му предоставя цялата налична информация, по-специално:

– документацията на системата за управление на качеството,

– записите по качеството, посочени в проектната част на системата по качеството, като резултати от анализи, изчисления и изпитвания,

– записите по качеството, посочени в производствената част на системата по качеството, като доклади от проверки, данни от изпитвания, данни от калибриране и доклади за квалификацията на съответния персонал.

4.3. Нотифицираният орган извършва периодични одити, за да се увери, че производителят поддържа и прилага системата за управление на качеството, и предоставя на производителя доклад от одита.

5. Маркировка за съответствие и декларация за съответствие

5.1. Производителят поставя маркировката „CE“, и на отговорността на нотифицирания орган, посочен в точка 3.1, идентификационния му номер, върху всеки отделен продукт с цифрови елементи, който отговаря на изискванията, посочени в приложение I, част I към настоящия регламент.

5.2. Производителят изготвя писмена декларация за съответствие за образец от всеки продукт и я съхранява на разположение на националните органи в продължение на 10 години след пускането на продукта с цифрови елементи на пазара или в продължение на периода на поддръжка, в зависимост от това кой е по-дълъг. Декларацията за съответствие идентифицира образеца от продукта, за който е изготвена.

Копие от декларацията за съответствие се предоставя на съответните органи при поискване.

6. В продължение на най-малко 10 години след пускането на продукта с цифрови елементи на пазара или в продължение на периода на поддръжка, в зависимост от това кой е по-дълъг, в зависимост от това кой период е по-дълъг, производителят съхранява на разположение на националните органи:

6.1 техническата документация по точка 3.1;

6.2 документацията относно системата за управление на качеството по точка 3.1;

6.3 одобрените изменения по точка 3.5;

6.4 решенията и докладите на нотифицирания орган по точки 3.5 и 4.3.

7. Всеки нотифициран орган информира своите нотифициращи органи за одобренията на системи за управление на качеството, които е издал или отнел, и периодично или при поискване им предоставя списък с одобренията на системи за управление на качеството, които е отказал, временно прекратил или ограничил по някакъв друг начин.

Всеки нотифициран орган информира останалите нотифицирани органи за одобренията на системи за управление на качеството, които е отказал, временно прекратил или отнел, и при поискване, за одобренията на системи за управление на качеството, които е издал.

8. Упълномощен представител

Задълженията на производителя, определени в точки 3.1, 3.5, 5 и 6, могат да бъдат изпълнявани от негов упълномощен представител, от негово име и на негова отговорност, при условие че съответните задължения са конкретно посочени в пълномощното.

По отношение на настоящия акт беше направено изявление, което може да бъде намерено в [ОВ: моля, попълнете: ОВ C XXX, XX.XX.2024 г., стр. XX] и на следния линк: [ОВ: моля, вмъкнете линка към изявлението].