C/2026/6013

17.11.2026 г.

# СЪОБЩЕНИЕ НА КОМИСИЯТА

## Насоки на Комисията относно прилагането на Регламент (ЕС) 2024/2847 (Акт за киберустойчивост)

(C/2026/6013)

### Съдържание

*Страница*

1. ВЪВЕДЕНИЕ ... 3
   - 1.1. Актът за киберустойчивост ... 3
   - 1.2. Цел на насоките ... 3
2. ПРИЛОЖНО ПОЛЕ ... 4
   - 2.1. Пускане на пазара ... 4
   - 2.2. Софтуер като продукт с цифрови елементи ... 5
   - 2.3. Компютърен код ... 6
   - 2.4. Комбинация от хардуер и софтуер, формиращи продукт с цифрови елементи ... 7
   - 2.5. Връзка на данни ... 8
   - 2.6. Сложни системи ... 8
   - 2.7. Продукти с цифрови елементи, проектирани преди датата, от която се прилага АК ... 9
3. СВОБОДЕН СОФТУЕР С ОТВОРЕН КОД ... 11
   - 3.1. Определяне дали даден свободен софтуер с отворен код е под нечия отговорност ... 12
   - 3.2. Определяне дали свободен софтуер с отворен код е пуснат на пазара на ЕС ... 13
     - 3.2.1. Начисляване на цена ... 13
     - 3.2.2. .Извличане на печалба от други услуги или изискване да се обработват лични данни ... 13
     - 3.2.3. Услуги за поддръжка ... 14
     - 3.2.4. Дарения ... 15
     - 3.2.5. Финансиране на свободен софтуер с отворен код ... 15
     - 3.2.6. Образувания с нестопанска цел, създадени за постигане на нестопански цели ... 16
     - 3.2.7. Интегриране от други производители ... 16
   - 3.3. Задължения на попечителите на софтуер с отворен код ... 16
     - 3.3.1. Устойчива подкрепа и гарантиране на жизнеспособността на FOSS ... 17
   - 3.4. Сътрудници и употреба надолу по веригата ... 18
   - 3.5. Илюстративни сценарии ... 19
4. СЪЩЕСТВЕНИ ИЗМЕНЕНИЯ И РЕЗЕРВНИ ЧАСТИ ... 21
   - 4.1. Физически ремонти ... 22
   - 4.2. Резервни части ... 23
   - 4.3. Софтуерни актуализации като съществени изменения ... 24

4.4. Последици от съществено изменение ..... 27
4.4.1. Съществени изменения, които се извършват от лице, различно от първоначалния производител .. 28
4.4.2. Съществени изменения, извършени от първоначалния производител ..... 29
5. ПЕРИОД НА ПОДДРЪЖКА ..... 29
5.1. Съществени изменения и период на поддръжка ..... 31
6. ВАЖНИ И КРИТИЧНИ ПРОДУКТИ С ЦИФРОВИ ЕЛЕМЕНТИ ..... 32
6.1. Основна функционална възможност ..... 33
6.2. Оценяване на съответствието за важни и критични продукти с цифрови елементи ..... 36
6.3. Последствия за презумпцията за съответствие ..... 38
7. ОЦЕНКА НА КИБЕРРИСКА И ИНТЕГРИРАНЕ НА ПРОДУКТИ С ЦИФРОВИ ЕЛЕМЕНТИ И КОМПОНЕНТИ ..... 41
7.1, Оценка и третиране на киберрисковете ..... 41
7.2. Проектиране, разработване и производство на продукти с цифрови елементи по такъв начин, че да гарантират подходящо ниво на киберсигурност въз основа на рисковете ..... 42
7.3. Оценка на риска и дължима грижа във връзка с външни зависимости и интегрирани компоненти ..... 42
7.4. Повторно използване на оценки на риска и документация за съответствие за семейства продукти с цифрови елементи ..... 44
8. ОБРАБОТВАНЕ НА ДАННИ ОТ РАЗСТОЯНИЕ ..... 44
8.1. Какво се счита за решение за обработване на данни от разстояние по отношение на даден продукт с цифрови елементи? ..... 45
8.1.1. Понятието „от разстояние“ ..... 46
8.1.2. Липсата на такова обработване би ли попречила на продукта с цифрови елементи да изпълнява една от своите функции? ..... 46
8.1.3. Проектиран и разработен ли е софтуерът от производителя или под негова отговорност? ..... 47
8.2. Практически и технически последици от решенията за обработване на данни от разстояние и разчитането на решения на трети страни ..... 49
8.3. Случаи на употреба за решения за обработване на данни от разстояние ..... 50
8.3.1. Приложение за мобилно банкиране ..... 51
8.3.2. Интелигентен термостат ..... 52
8.3.3. Електронен четец ..... 53
8.3.4. Промишлен робот ..... 53
8.3.5. Клетъчна мрежа ..... 53
9. ДОПЪЛНИТЕЛНИ ЕЛЕМЕНТИ ..... 54
9.1. Задължения за докладване ..... 54
9.2. Отстраняване на уязвимости ..... 56
9.2.1. Докладване нагоре по веригата и споделяне на корекции за сигурност ..... 56
9.2.2. Уязвимости, които са вече известни и могат да бъдат използвани ..... 57
9.2.3. Ефективни и редовни проверки и прегледи ..... 58
9.3. Взаимодействие с други законодателни актове ..... 59
9.3.1. Регламент (ЕС) 2019/2144 и Регламент (ЕС) № 168/2013 ..... 59
9.3.2. Валидност на сертификатите за ЕС изследване на типа (член 69, параграф 1) ..... 59

# 1. **ВЪВЕДЕНИЕ**

## 1.1. **Актът за киберустойчивост**

1. Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета от 23 октомври 2024 г. 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) ([1]) влезе в сила на 10 декември 2024 г. Целите на регламента са укрепване на подхода на ЕС към киберсигурността, справяне с киберустойчивостта на равнището на ЕС и подобряване на функционирането на вътрешния пазар чрез установяване на единна правна рамка за съществените изисквания за киберсигурност при пускането на продукти с цифрови елементи на пазара на ЕС, както и по време на жизнения цикъл на даден продукт с цифрови елементи.

2. Актът за киберустойчивост (АК) се основава на новата законодателна рамка (НЗР) на ЕС, установена в Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. за определяне на изискванията за акредитация и надзор на пазара във връзка с предлагането на пазара на продукти и за отмяна на Регламент (ЕИО) № 339/93 и 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 ([2]).

3. Надзорът на пазара и правоприлагането се извършват от националните органи за надзор на пазара. Продуктите с цифрови елементи, които попадат в приложното поле на АК, са обхванати от 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. Комисията и Агенцията на Европейския съюз за киберсигурност (ENISA) подпомагат икономическите оператори и държавите членки при прилагането на АК.

## 1.2. **Цел на насоките**

4. Съгласно член 26, параграф 1 от АК от Комисията се изисква да публикува насоки за подпомагане на икономическите оператори при прилагането на регламента със специален акцент върху улесняването на спазването на изискванията от страна на микропредприятията и малките и средните предприятия (МСП). В член 26, параграф 2 са определени минималните аспекти, които следва да бъдат разгледани в насоките. Те включват: i) обхвата на АК (по-специално решенията за обработване на данни от разстояние и свободния софтуер с отворен код); ii) понятието „периоди на поддръжка“; iii) взаимодействието между АК и други законодателни актове на ЕС; и iv) концепцията за „съществено изменение“.

5. На 3 декември 2025 г. Комисията публикува поредица от често задавани въпроси (ЧЗВ), които имат за цел да се подпомогнат икономическите оператори при подготовката за прилагането на АК ([3]).

6. Настоящите насоки са предназначени за подпомагане на икономическите оператори при спазването на АК и на дейностите на органите за надзор на пазара, нотифициращите органи и нотифицираните органи с оглед осигуряване на хармонизирано прилагане на АК в целия Съюз. Настоящите насоки нямат за цел да обхванат цялото приложно поле на АК, а по-скоро да предоставят разяснения относно обосновката на някои ключови разпоредби и начина, по който те могат да бъдат приложени на практика. Настоящите насоки се отнасят за АК и не са приложими за други законодателни актове на ЕС.

([1]) ОВ L 2024/2847, 20.11.2024 г., ELI:. http://data.europa.eu/eli/reg/2024/2847/oj.

([2]) В работната програма на Комисията за 2026 г. се предвижда представянето на „Европейски акт за продуктите“ за актуализиране на НЗР и правилата за надзора на пазара и за стандартизацията: https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:52025DC0870.

([3]) ЧЗВ могат да бъдат изтеглени чрез уебсайта на Комисията за прилагане на АК от специалната уебстраница с ЧЗВ.

7. При изготвянето на настоящите насоки бяха проведени обстойни консултации със заинтересованите страни, включително с участието на Експертната група по киберсигурност на продукти с цифрови елементи ([4]) и чрез обществена консултация, проведена между 3 март и 13 април 2026 г. ([5]).

8. Настоящите насоки не са задължителни за икономическите оператори или другите участници, за които се прилага АК. Авторитетно тълкуване на АК може да бъде дадено само от Съда на Европейския съюз. Въпреки това настоящите насоки представляват тълкуването на АК от страна на Комисията с оглед подпомагане на спазването на изискванията и допринасяне за ефективното прилагане на регламента. Освен това насоките включват редица примери за илюстриране на прилагането на конкретни разпоредби. Тези примери обаче нямат за цел да заместят индивидуалната оценка, която винаги ще е необходима, за да се отчетат особеностите на всеки отделен случай.

9. В съответствие с член 26 от АК Комисията може да издава евентуални допълнителни насоки, включително насоки за производителите, които са обхванати от АК и спрямо които се прилага законодателство на Съюза за хармонизация, различно от АК, или други свързани правни актове на Съюза. Тези насоки могат например да разглеждат въпроси относно взаимодействието между АК и Регламент (ЕС) 2024/1689 за установяване на хармонизирани правила относно изкуствения интелект (Акт за изкуствения интелект) и Регламент (ЕС) 2022/2554 относно оперативната устойчивост на цифровите технологии във финансовия сектор (DORA).

## 2. **ПРИЛОЖНО ПОЛЕ**

### 2.1. **Пускане на пазара**

10. АК се прилага за продукти с цифрови елементи, които се предоставят на пазара на ЕС. Понятието „предоставяне на пазара“ е дефинирано в член 3, параграф 22 от АК като „доставянето на продукт с цифрови елементи за разпространение или използване на пазара на Съюза в процеса на търговска дейност, срещу заплащане или безвъзмездно“. В съответствие с член 3, параграф 21 даден продукт с цифрови елементи се счита за пуснат на пазара при предоставянето му за първи път на пазара на Съюза.

11. В последното издание на „Синьото ръководство“ за прилагане на правилата на ЕС относно продуктите, публикувано през 2022 г. („Синьото ръководство“) ([6]), се предоставят насоки за по-лесно разбиране на правилата на ЕС относно продуктите и за по-еднаквото и съгласувано прилагане на тези правила в рамките на приложимите за различните сектори правни рамки в съответствие с новата законодателна рамка (НЗР), като например АК. В Синьото ръководство се посочва, че понятията „пускане на пазара“ и „предоставяне на пазара“ трябва да се разбират като отнасящи се „за всеки отделен продукт, а не за вид продукти, без оглед на това дали продуктът е произведен като самостоятелно изделие, или в серия“ (раздел 2.3).

12. По отношение на по-традиционни продукти с цифрови елементи, обхванати от НЗР, като например хардуер под формата на машини или радиосъоръжения, понятието „пускане на пазара“ е добре установено и Синьото ръководство предоставя допълнителни насоки за изясняване на момента, в който тези продукти се считат за пуснати на пазара. С обобщените примери, изброени в раздел 2.12 от Синьото ръководство, се предоставят допълнителни примери за понятието „пускане на пазара“.

13. Като се има предвид обаче естеството на нематериалните продукти с цифрови елементи, като например самостоятелните софтуерни продукти, са необходими допълнителни насоки за момента, в който тези продукти с цифрови елементи се считат за пуснати на пазара. След като етапът на производство на софтуера приключи и продуктът с цифрови елементи бъде предложен на потенциални ползватели на пазара на ЕС, може да се счита, че неговият производител е произвел множество копия на един и същ софтуерен продукт с цифрови елементи и ги е доставил за разпространение или използване. За разлика от материалните продукти с цифрови елементи,

([4]) Експертна група по киберсигурност на продукти с цифрови елементи в регистъра на експертните групи на Комисията и други сходни структури.

([5]) Обществена консултация относно проект на насоки на Комисията относно Акта за киберустойчивост.

([6]) Известие на Комисията — „Синьото ръководство“ за прилагане на правилата на ЕС относно продуктите — 2022 г. (2022/C 247/01) (ОВ C 247, 29.6.2022 г., стр. 1).

самостоятелният софтуер не подлежи на физическо производство или ограничения по отношение на наличностите: с всяко предоставяне на софтуера за изтегляне или разпространение се създава ново идентично копие за ползвателя. Докато тази версия на софтуера не бъде изменена по начин, който се отразява на съответствието с АК, пускането на пазара на ЕС следва да се счита за извършено в момента на първото предлагане за разпространение или използване. Поради това възможността за последващо изтегляне или разпространение на тази версия на софтуерния продукт с цифрови елементи трябва да се счита за случай, в който този софтуерен продукт с цифрови елементи се предоставя на пазара ([7]).

14. Поради това даден самостоятелен софтуерен продукт с цифрови елементи следва да се счита за пуснат на пазара, когато етапът на производството му е приключил и този софтуер е доставен за първи път за разпространение или използване на пазара на ЕС в процеса на търговска дейност. Следва да се счита, че производителят е пуснал на пазара множество копия на един и същ софтуерен продукт с цифрови елементи едновременно. Следователно, докато множеството копия на един и същ софтуер остават отделни продукти с цифрови елементи, те се считат за пуснати на пазара едновременно, независимо от момента на прехвърляне на правото на собственост или използване на всяко отделно копие на друго физическо или юридическо лице. В същото време, когато производителят предоставя различни варианти на даден софтуер, които се различават по включените компоненти, конфигурации или активирани функционалности (напр. компилации за различни операционни системи или пакети с различни набори от функции), тези варианти не могат да се считат за множество копия на един и същ софтуерен продукт с цифрови елементи. Поради това те следва да се третират като отделни продукти с цифрови елементи за целите на пускането на пазара.

*Пример 1: на 1 януари 2028 г. дружество А за първи път доставя за разпространение чрез своя уебсайт версия 1.0.0 на своя софтуер X. В същия ден клиент 1 закупува копие на версия 1.0.0 на софтуер X. На 15 януари 2028 г. клиент 2 закупува копие на версия 1.0.0 на софтуер X. И двете копия на версия 1.0.0 на софтуер X са пуснати на пазара на 1 януари 2028 г.*

15. Предвид итеративния характер на разработването на софтуер следва допълнително да се поясни, че последващите модификации на даден софтуерен продукт с цифрови елементи се считат за новопуснати на пазара, когато тези модификации се квалифицират като „съществено изменение“ на софтуерен продукт с цифрови елементи, който вече е пуснат на пазара, както е посочено в съображение 41 от АК. За модификациите, които не се квалифицират като съществени изменения, не се изисква производителят да извършва нова процедура за оценяване на съответствието и следователно с тях не се променя датата на пускане на този софтуер на пазара. За повече насоки относно понятието „съществено изменение“ вж. раздел 4. *Съществени изменения*.

*Пример 2: на 1 януари 2028 г. дружество А за първи път доставя за разпространение чрез своя уебсайт версия 1.0.0 на софтуер X. В същия ден клиент 1 закупува копие на версия 1.0.0 на софтуер X. На 15 януари 2028 г. дружество А издава актуализирана версия 1.0.1 на софтуер X, която не представлява съществено изменение. На 30 януари 2028 г. клиент 2 закупува копие от версия 1.0.1 на софтуер X. И двете копия на версия 1.0.0 и 1.0.1 на софтуер X се считат за пуснати на пазара на 1 януари 2028 г.*

16. Насоките, изложени в точки 13, 14 и 15, се прилагат изключително доколкото продуктът с цифрови елементи е самостоятелен софтуер. Случаят не е такъв, когато например софтуерът се комбинира с хардуер, както е посочено в раздел *2.4 Комбинация от хардуер и софтуер, формиращи продукт*.

### 2.2. **Софтуер като продукт с цифрови елементи**

17. Съгласно определението в член 3, параграф 1 от АК „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“. Тези продукти с цифрови елементи попадат в обхвата на АК, когато тяхното предназначение или разумно предвидима употреба включва пряка или непряка логическа или физическа връзка на данни с устройство или мрежа.

([7]) В съответствие с член 13, параграф 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.

18. Следователно АК може да обхваща редица продукти с цифрови елементи, включително: i) самостоятелен софтуер, като например приложения и компютърни програми, независимо дали се разпространяват физически или по електронен път; ii) хардуер с вграден софтуер (напр. устройства, свързани към интернет на предметите, преносими компютри, таблети); iii) самостоятелен хардуер (напр. интегрални схеми, дънни платки); и (iv) всяка комбинация от хардуер и софтуер, доставени отделно, но предназначени да работят заедно.

19. Следователно самостоятелният софтуер попада в обхвата на АК, когато се пуска на пазара като продукт с цифрови елементи. Удачно е да се прави разграничение между софтуерни продукти с цифрови елементи, които са предмет на АК, и предоставяне на услуги от разстояние, които не попадат в обхвата на АК.

20. За да попада в обхвата на АК, даден софтуерен продукт с цифрови елементи трябва да бъде предоставен на ползвател и получен от него и да работи в електронната информационна система на ползвателя или като част от нея. Софтуерът, който се изтегля, инсталира или по друг начин се доставя на ползвател и който се изпълнява в електронната информационна система на ползвателя, отговаря на тези критерии, включително ако е под формата на разширение за уеб браузър или приложение, разработено чрез уеб технологии, но доставено за локално изпълнение.

21. За разлика от него софтуерът, който се изпълнява от разстояние и до който ползвателят само получава достъп, не представлява продукт с цифрови елементи единствено на това основание. Това разграничение е направено в съображения 11 и 12 от АК, като се пояснява, че обработването или съхранението от разстояние попада в обхвата на АК само доколкото то е необходимо, за да може даден продукт с цифрови елементи да изпълнява своите функции (т.е. чрез понятието „обработване на данни от разстояние“ съгласно определението, дадено в член 3, параграф 2), а не сам по себе си като продукт с цифрови елементи. Това обикновено важи за уеб приложенията, включително прогресивни уеб приложения, когато до тях се осъществява достъп единствено чрез уеб браузър. Това се отнася и за уебсайтовете: въпреки че уебсайтовете могат, в ограничена степен, технически да работят и да се изпълняват на устройството на ползвателя, от съображение 12 от АК следва, че сами по себе си уебсайтовете не следва да се считат за продукти с цифрови елементи и попадат в обхвата на АК само когато поддържат функционалността на продукт с цифрови елементи, т.е. доколкото биват класифицирани като обработване на данни от разстояние (както е обяснено по-подробно в раздел *8* и по-специално *8.1.2 Липсата на такова обработване би ли попречила на продукта с цифрови елементи да изпълнява една от своите функции?*).

*Пример 3: мобилно приложение, което даден ползвател изтегля от магазин за приложения и инсталира на своя смартфон, се доставя на ползвателя и се изпълнява на устройството му и следователно е продукт с цифрови елементи. То може да попада в обхвата на АК, когато се пуска на пазара в процеса на търговска дейност.*

*Пример 4: настолно приложение, създадено чрез уебтехнологии, но в пакет за локално инсталиране, се доставя на ползвателя и се изпълнява на устройството му и следователно е продукт с цифрови елементи. То може да попада в обхвата на АК, когато се пуска на пазара в процеса на търговска дейност.*

*Пример 5: уеб приложение, до което ползвателят има достъп единствено чрез уеб браузър, не представлява продукт с цифрови елементи. Освен ако не поддържа функционалността на продукт с цифрови елементи, то не попада в обхвата на АК. За разлика от него приложение, доставено на ползвателя като локално инсталиран клиент, който се изпълнява на устройството на ползвателя, се счита за продукт с цифрови елементи. То може да попада в обхвата на АК, когато се пуска на пазара в процеса на търговска дейност.*

*Ако изпълнението на една или повече функции на този клиент зависи от обработване на данни от разстояние, което отговаря на определението за обработване на данни от разстояние, тази обработка на данни от разстояние също е част от продукта с цифрови елементи.*

*Пример 6: уебсайт, който единствено представя информация на своите посетители и не поддържа функционалността на продукт с цифрови елементи, сам по себе си не представлява продукт с цифрови елементи. Следователно той не попада в обхвата на АК.*

### 2.3. **Компютърен код**

22. Също така е удачно да се изясни дали изходният код може да представлява софтуерен продукт с цифрови елементи. Съгласно определението, установено в АК, „софтуер“ означава „частта от електронна информационна система, която се състои от компютърен код“ (член 3, параграф 4). Компютърният код може да бъде под формата на i) машинен код, който е набор от изпълнявани директно от процесора на компютъра инструкции в двоичен формат; или ii) изходен код, т.е. набор от инструкции и команди на програмен език, които трябва да бъдат компилирани или интерпретирани, за да бъдат изпълнени от компютър. Определението за софтуер, установено в АК, обхваща и двата елемента.

23. Отделен въпрос е дали дадена доставка на компютърен код е еквивалентна на пускането на продукт с цифрови елементи на пазара на ЕС, което изисква доставка в процеса на търговска дейност. Това често може да не е така по отношение на изходния код. Например физическо или юридическо лице, което споделя свободен и отворен компютърен код в публично достъпни хранилища, обикновено не се счита за лице, което пуска този код на пазара на ЕС за целите на АК (както е разгледано по-подробно в раздел *3 Свободен софтуер с отворен* код). Незавършен код, споделен по време на етапа на проектиране и разработване на продукт с цифрови елементи (напр. с цел изпитване или преглед), също не се счита за пуснат на пазара за целите на АК, тъй като етапът на производството му не е завършен. По същия начин примерен или демо код, предоставен като част от уроци или материали за обучение, също не се счита за пуснат на пазара за целите на АК ([8]).

24. От друга страна, когато производителят предоставя на своите клиенти компютърен код като продукт с цифрови елементи, този код се счита за пуснат на пазара, независимо дали е машинен код, или изходен код ([9]).

*Пример 7: дружество А лицензира изходен код на дружество Б за персонализирана вътрешна платформа и предоставя този изходен код в текстов файл. Дори ако за този изходен код се изисква допълнителна адаптация и компилиране от страна на дружество Б, преди да бъде използван, дружество А пуска този изходен код на пазара и следователно той е предмет на АК. Дружество А не носи отговорност за съответствието с АК на последващите адаптации и компилиране на този код от страна на дружество Б.*

### 2.4. **Комбинация от хардуер и софтуер, формиращи продукт с цифрови елементи**

25. Определянето на софтуер като част от продукт с цифрови елементи следва да се извършва не въз основа на начина и момента на доставка на този софтуер на ползвателя, а като се вземе предвид дали, с оглед на предназначението и разумно предвидимата употреба на продукта, софтуерът е необходим за изпълнението на предвидените функции на продукта с цифрови елементи. Когато хардуерен продукт с цифрови елементи е проектиран да работи заедно със специфичен софтуер, който се предоставя от същия производител, за да изпълнява функциите си, хардуерът и този софтуер заедно съставляват продукта с цифрови елементи. Софтуерът, който е необходим за функционирането, конфигурирането, контрола или използването на продукт с цифрови елементи в съответствие с предназначението му, следователно е част от продукта с цифрови елементи, дори ако е получен чрез отделен канал (напр. магазин за приложения, връзка за изтегляне или друг цифров канал, след като хардуерният продукт с цифрови елементи е бил пуснат на пазара). Следователно пускането му на пазара се случва в момента на пускане на екземплярите на хардуерния продукт с цифрови елементи на пазара.

*Пример 8: тръжов принтер се пуска на пазара като хардуерен продукт с цифрови елементи, а софтуерните драйвери, необходими за изпращане на задачи за печат, конфигуриране на устройството и управление на работата му, се предоставят за изтегляне от уебсайта на производителя. Въпреки че принтерът и драйверите се доставят чрез различни канали, те заедно съставляват един продукт с цифрови елементи, тъй като принтерът не може да изпълнява предназначението си без драйверите.*

*Пример 9: на пазара се пуска носимо устройство за следене на физическата форма, измерващо сърдечната честота и активността на ползвателя, като за показването на измерванията и хронологията и за конфигурирането на устройството е необходимо предоставяно от производителя приложение за смартфон. Въпреки че приложението се изтегля отделно чрез магазин за приложения, носимото устройство и приложението заедно съставляват един продукт с цифрови елементи, тъй като те са проектирани и предназначени да работят заедно с цел осигуряване на функционалната възможност на продукта с цифрови елементи.*

([8]) Следва също да се припомни, че съгласно член 4, параграф 3 производителите могат да предоставят на пазара незавършен софтуер, който не спазва регламента, 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.

([9]) От друга страна, следва да се отбележи, че за целите на законодателството относно отговорността за продуктите, самият компютърен код не представлява продукт и следователно производителите, които пускат такъв код на пазара, не могат да бъдат държани отговорни съгласно Директива (ЕС) 2024/2853 (Директивата относно отговорността за продуктите). В съображение 13 от тази директива се посочва, че „информацията обаче не следва да се счита за продукт и поради това правилата за отговорността за вреди, причинени от дефекти на продукти, не следва да се прилагат за съдържанието на цифрови файлове, като например медийни файлове или електронни книги, или изходния код на софтуера“. Това не изключва възможността производителите да носят отговорност съгласно националното деликтно право.

### 2.5. **Връзка на данни**

26. В член 2, параграф 1 се посочва, че АК „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“. Следователно обхватът на АК не се основава на самото наличие на електроника, а на способността на продукта с цифрови елементи да обменя цифрова информация.

27. Въпреки че понятията „логическа връзка“ и „физическа връзка“ са дефинирани в член 3, в АК не се дава определение за „връзка на данни“ или „цифрови данни“. Поради това е удачно да се изложи тълкуване на понятието „връзка на данни“ с цел изясняване на границите на обхвата на АК. Тези граници са от особена важност за отличаването на продукти с цифрови елементи, които само използват електрически сигнали, от тези, които участват в цифрова комуникация и следователно са изложени на киберрискове.

28. На най-основно ниво връзката на данни включва предаване на информация в двоична форма, т.е. като поредица от нули и единици. Самото включване/изключване на изход (т.е. 0/1) не представлява връзка на данни, ако съответното състояние не е предназначено да представлява данни или не се прочита от цифров вход. За да съществува връзка на данни, двоичните състояния трябва да бъдат преднамерено кодирани като информация от източник и трябва да могат да бъдат декодирани като информация в местоназначението. С други думи, трябва да има предавател, който целенасочено генерира цифрови символи съгласно определена схема, и приемник, способен да интерпретира тези символи като данни. Когато електрически или електронни сигнали се използват единствено за задействане или захранване на функция, без да предават цифрово кодирана информация, не съществува връзка на данни за целите на АК и следователно продуктът с цифрови елементи не попада в обхвата на член 2, параграф 1.

### 2.6. **Сложни системи**

29. Продуктите с цифрови елементи в обхвата на АК могат да се състоят не само от отделни устройства или софтуерни компоненти, но и от сложни системи, включително системи от множество хардуерни и софтуерни елементи, които работят заедно с цел изпълнение на определена функция. Когато такава система бъде пусната на пазара като един продукт с цифрови елементи, тя представлява продукт с цифрови елементи по смисъла на АК.

30. Такива сложни системи често се характеризират с дълги цикли на проектиране и разработване, с договори, които може да са били подписани преди датата, от която се прилага АК, с удължен експлоатационен срок и с висока степен на техническа и организационна сложност. Пускането на такива системи на пазара след датата, от която се прилага АК, може да зависи от компоненти, пуснати на пазара преди датата, от която се прилага АК, от утвърдени архитектури или широко използвани стандарти за оперативна съвместимост, включително стандарти, посочени в друго законодателство на ЕС или негови специфични за отделните сектори рамки. В резултат на това някои технически характеристики на тези системи могат да бъдат трудни или непропорционални за изменение, без това да засегне тяхното предназначение, безопасност, надеждност или оперативна съвместимост със съществуващата инфраструктура.

31. Сами по себе си тези характеристики не съставляват основание за изключване на сложните системи от обхвата на АК. С тях по-скоро се илюстрира прилагането на основания на риска подход съгласно АК, чрез който съответствието може да бъде доказано по различни начини в зависимост от характеристиките и ограниченията на продукта с цифрови елементи, както е предвидено в член 13, параграф 3 от АК. Тези характеристики са част от неговото предназначение и оперативен контекст и следователно са от значение при оценяването на съответствието със съществените изисквания за киберсигурност („съществените изисквания“). По-конкретно, в съображение 55 изрично се посочва, че някои съществени изисквания може да не са напълно съвместими с естеството на даден продукт с цифрови елементи. Например такъв може да е случаят, когато съответствието би засегнало задължителните изисквания за оперативна съвместимост или правилното функциониране на системата.

32. Съответно производителите са задължени да разглеждат киберрисковете въз основа на оценката на киберриска, посочена в член 13, параграф 2. Както е обяснено и в съображение 55, в някои случаи специфични съществени изисквания не са приложими или не могат да бъдат изпълнени чрез прилагане на най-съвременни мерки за

сигурност — например поради предназначението на системата, което изисква продуктът с цифрови елементи да взаимодейства със съществуващи зависимости или да следва определени изисквания за оперативна съвместимост. В такива случаи производителите следва да идентифицират и документират тези специфични ограничения, да оценят свързаните с тях рискове и да приложат подходящи алтернативни или компенсаторни мерки за намаляване на риска, така че да не бъде застрашена сигурността на продукта с цифрови елементи. За тези цели посочената в член 31 техническа документация и посочените в приложение II информация и инструкции за ползвателя, са от решаващо значение за прозрачното описване на идентифицираните ограничения, свързаните киберрискове и приложените мерки за намаляване на риска. В съответствие със задължението за поддържане на оценката на риска актуализирана по време на периода на поддръжка, производителите следва също периодично да преоценяват дали тези ограничения продължават да съществуват. Когато такива ограничения могат да бъдат премахнати или намалени с течение на времето, производителите следва съответно да актуализират продукта с цифрови елементи, така че той да може да гарантира подходящо ниво на киберсигурност ([10]).

*Пример 10: производител пуска на пазара продукт с цифрови елементи, който комуникира с външни системи чрез мрежов протокол. Като част от прилагането на съществените изисквания, въз основа на оценката на киберриска производителят определя, че е необходимо използването на сигурен комуникационен протокол с цел осигуряване на поверителността и целостта на данните, обменяни от продукта с цифрови елементи.*

*Въпреки това неговото предназначение включва оперативна съвместимост със съществуващи системи, които поддържат само по-стар или по-малко сигурен протокол. В такива случаи производителят може да приложи посочения протокол, когато това е необходимо за постигане на оперативна съвместимост, при условие че свързаните киберрискове са идентифицирани и ограничени чрез други средства.*

*Когато е технически осъществимо продуктът с цифрови елементи да поддържа както сигурния протокол, така и по-малко сигурния протокол, от производителя се очаква да приложи сигурния протокол и да активира използването му по подразбиране. По-малко сигурният протокол би бил разрешен само когато е необходим за осигуряване на оперативна съвместимост.*

*Пример 11: производител на система за индустриална автоматизация закупува някои микроконтролери преди датата, от която се прилага АК. Производителят извършва оценка на киберриска за своята система за индустриална автоматизация, която ще бъде пусната на пазара след датата, от която се прилага АК. Въз основа на тази оценка на киберриска производителят не идентифицира специфични киберрискове, свързани с използването на един от тези микроконтролери. Производителят го интегрира в своята система за индустриална автоматизация и гарантира, че продуктът с цифрови елементи като цяло (системата за индустриална автоматизация) отговаря на съществените изисквания.*

### 2.7. **Продукти с цифрови елементи, проектирани преди датата, от която се прилага АК**

33. В някои случаи производител ще пусне на пазара, след 11 декември 2027 г. — датата, от която се прилага АК, единици от продукт с цифрови елементи, произведен в съответствие с тип или модел, проектиран и разработен преди датата, от която се прилага АК. В такива случаи съответствието с настоящия регламент не изисква непременно повторно проектиране на тези единици от продукта с цифрови елементи. Производителят е задължен да извърши оценка на киберриска в съответствие с член 13, параграф 2 от АК, за да определи, въз основа на предназначението и разумно предвидимата употреба на продукта с цифрови елементи, кои от съществените изисквания, посочени в приложение I, част I, са приложими за този продукт с цифрови елементи и как тези изисквания се прилагат.

34. Когато според резултата от тази оценка на риска продуктът с цифрови елементи вече включва подходящи и ефективни мерки за сигурност за справяне със съответните рискове, производителят може да се позове на тях, за да докаже съответствието с АК. АК сам по себе си не налага задължение за въвеждане на нови функции за сигурност или за повторно проектиране на продукта с цифрови елементи, когато това не е необходимо за справяне с идентифицираните рискове.

([10]) Следва да се отбележи, че изложените в настоящия параграф съображения може да са приложими, по целесъобразност, за всички продукти с цифрови елементи в обхвата на АК, а не само за сложни системи.

35. Въпреки това производителят остава обвързан със задълженията, предвидени в АК. Те включват гарантиране, преди продуктът с цифрови елементи да бъде пуснат на пазара, че е извършена приложимата процедура за оценяване на съответствието, че е съставена ЕС декларацията за съответствие и че е поставена маркировката „CE“. Съответствието с тези изисквания е независимо от това дали дизайнът на продукта с цифрови елементи е изисквал изменение в резултат на оценката на риска. По отношение на продукти с цифрови елементи, проектирани преди датата, от която се прилага АК, но пуснати на пазара след нея, когато не е възможно производителят да докаже как е взета предвид оценката на риска по време на етапа на проектиране и разработване на продукта с цифрови елементи, задължението по член 13, параграф 2 следва да се разбира като изискване към производителя да извърши оценка на киберриска и въз основа на нея да докаже, че продуктът с цифрови елементи включва подходящи мерки за сигурност 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.

36. Съответно продуктите с цифрови елементи, проектирани преди датата, от която се прилага АК, могат да бъдат пуснати на пазара в съответствие с АК без повторно проектиране, при условие че производителят може да докаже, чрез оценката на киберриска и техническата документация, че продуктът с цифрови елементи осигурява подходящо ниво на киберсигурност с оглед на неговото предназначение и разумно предвидима употреба и отговаря на съществените изисквания за киберсигурност.

37. Освен това е полезно да се изясни прилагането на задълженията за оценяване на съответствието за производители на продукти с цифрови елементи, които се пускат на пазара след датата, от която се прилага АК, но са произведени в съответствие с тип или модел, проектиран и разработен преди тази дата. В съответствие с член 13, параграф 12 производителят е задължен да докаже чрез съответната процедура за оценяване на съответствието, че неговият продукт с цифрови елементи е в съответствие с приложимите съществени изисквания, и да включи доказателства за това в техническата документация на продукта (приложение VII, точка 6).

38. Прилагането на тези изисквания обаче трябва да се тълкува с оглед на оценката на киберриска и киберрисковия профил на продукта с цифрови елементи. По-конкретно, по отношение на продукти с цифрови елементи, проектирани преди датата, от която се прилага АК (но пуснати на пазара след тази дата), и подлежащи на процедурите за оценяване на съответствието, посочени в член 32, параграф 1, когато с оценката на риска се доказва, че продуктът с цифрови елементи вече включва подходящи и ефективни мерки за сигурност за справяне със свързаните с този продукт рискове, задължението за предоставяне на доказателства като част от процедурата за оценяване на съответствието не следва да се разбира като изискване към производителя да предостави резултати от изпитвания, обхващащи първоначалните етапи на проектиране и разработване на такива продукти с цифрови елементи. Това не би било необходимо, тъй като няма да допринесе за повишаване на сигурността на самия продукт с цифрови елементи. Когато въпреки това може да са необходими изпитвания, от производителите не се очаква да предоставят доказателства за изпитвания на всички варианти на продукта — те могат да групират такива изпитвания по семейства продукти с цифрови елементи, както е разгледано по-подробно в раздел *7.4 Повторно използване на оценки на риска и документация за съответствие за семейства продукти с цифрови елементи*.

39. Въпреки това производителят следва да предостави доказателства за съответствието с процесите на отстраняване на уязвимостите, предвидени в приложение I, част II, да актуализира оценката на риска в съответствие с член 13, параграф 3 и да изпълнява всички други установени в АК задължения, включително чрез предоставяне на ползвателите на информация и инструкции в съответствие с член 13, параграф 18.

*Пример 12: производител пуска на пазара микроконтролер, който е проектиран и разработен преди датата, от която се прилага АК. Микроконтролерът е предназначен за интегриране в редица електронни продукти с цифрови елементи, включително продукти с цифрови елементи с функционалности за свързаност.*

*Преди да пусне нови единици от микроконтролера на пазара след датата, от която се прилага АК, производителят извършва оценка на киберриска в съответствие с член 13, параграф 2. Въз основа на предназначението и разумно предвидимата употреба на микроконтролера производителят идентифицира съответните киберрискове, като например непозволен достъп, манипулиране на софтуер или данни, или неправилна употреба на налични интерфейси.*

*Оценката на риска показва, че микроконтролерът, както е проектиран първоначално, вече включва подходящи и ефективни мерки за сигурност за справяне с идентифицираните рискове. Поради това производителят стига до заключението, че продуктът с цифрови елементи отговаря на съответните съществени изисквания, определени в приложение I, част I, и че не е необходимо повторно проектиране или въвеждане на допълнителни функции за сигурност.*

*Когато не е възможно да се докаже как е взета предвид оценката на киберриска по време на етапа на първоначалното проектиране и разработване, производителят документира текуща оценка на киберриска и обяснява как се намаляват идентифицираните рискове чрез съществуващия дизайн и мерки. От производителя не се изисква да създава повторно документация за предишен дизайн или изпитвания, тъй като това не би допринесло за подобряване на киберсигурността на продукта с цифрови елементи. Когато няколко варианта на микроконтролера се основават на един и същ дизайн и споделят един и същ киберрисков профил, производителят може също да се позове на представителни доказателства за съответното семейство продукти.*

*Производителят също така гарантира съответствие с изискванията относно отстраняването на уязвимости, предвидени в приложение I, част II, включително чрез поддържане на процеси за справяне и отстраняване на уязвимостите и чрез прегледи на оценката на киберриска в съответствие с член 13, параграф 3.*

*При тези обстоятелства микроконтролерът, проектиран преди датата, от която се прилага АК, може да бъде пуснат на пазара без повторно проектиране, при условие че производителят може да докаже, чрез оценката на киберриска и техническата документация, че е осигурено подходящо ниво на киберсигурност с оглед на предназначението и разумно предвидимата употреба на продукта и на неговото съответствие със съществените изисквания за киберсигурност.*

## 3. **СВОБОДЕН СОФТУЕР С ОТВОРЕН КОД**

40. Както е припомнено в раздел *2.1 Пускане на пазара*, АК се прилага за продукти с цифрови елементи, които се предоставят за първи път на пазара на ЕС в процеса на търговска дейност (т.е. се „пускат на пазара“), както и за всеки следващ случай, който се счита за предоставяне на същия продукт с цифрови елементи на пазара. В Синьото ръководство (раздел 2.2) се пояснява, че „търговска дейност“ трябва да се разбира като предоставяне на стоки срещу заплащане или безплатно в контекста на дейности със стопанска цел и може да бъде оценена само според конкретния случай, като се вземат предвид редовността на доставките, характеристиките на продукта, намеренията на доставчика и др.

41. Доставянето в процеса на търговска дейност се характеризира с редица обстоятелства, подробно документирани в Синьото ръководство и припомнени в съображение 15 от АК. Те могат да включват директно начисляване на цена, както и „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“ (съображение 15) ([11]).

42. АК обаче отчита особеностите на различните начини на разработване и публикуване на „свободен софтуер с отворен код“ (FOSS) и предлага насоки за подпомагане на процеса по установяване дали даден FOSS е продукт с цифрови елементи, пуснат на пазара (т.е. в процеса на търговска дейност) по смисъла на АК. Както е обяснено в съображение 18, „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 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“.

([11]) Следва също да се припомни, че въпреки честото извличане на печалба от продуктите с цифрови елементи (също) чрез обработване на лични данни, защитата на личните данни е основно право и следователно личните данни не могат да се считат за стока, както е посочено в съображение 24 от Директива (ЕС) 2019/770 на Европейския парламент и на Съвета от 20 май 2019 г. за някои аспекти на договорите за предоставяне на цифрово съдържание и цифрови услуги (ОВ L 136, 22.5.2019 г., стр. 1, ELI: http://data.europa.eu/eli/dir/2019/770/oj).

43. Поради това е удачно i) да се поясни какво представлява FOSS; ii) да се определи кога се счита, че за него носи отговорност физическо или юридическо лице; и iii) да се предоставят примери, с които да се подпомогнат заинтересованите страни в процеса на разбиране кога разпространението на FOSS представлява пускане на пазара. Когато FOSS не е пуснат на пазара, той е извън обхвата на АК, освен ако субектът, който го публикува, не е юридическо лице, което отговаря на определението за „попечител на софтуер с отворен код“ (наричан по-долу „попечителят“), установено в член 3, параграф 14. В този случай той има единствено задълженията, предвидени в член 24.

44. Съгласно определението в член 3, параграф 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“. Въпреки че в настоящите насоки не се посочват конкретни свободни лицензи с отворен код, които са съвместими с определението, установено в член 3, параграф 48, от формулировката на тази разпоредба следва, че само софтуер, който кумулативно изпълнява следните две условия, може да бъде квалифициран като FOSS за целите на АК: i) софтуерът трябва да се предоставя чрез свободен лиценз с отворен код, предоставящ пълния набор от права съгласно член 3, параграф 48; и ii) неговият изходен код трябва да бъде свободно споделян.

45. С изискването лицензът да прави софтуера „свободно достъпен, използваем, модифицируем и преразпределяем“ се отразява традиционното разбиране за FOSS, а именно, че ползвателите трябва да имат достъп до изходния код и да могат да го използват без неоправдани ограничения, да го модифицират и да разпространяват повторно оригинални или модифицирани версии. Достъпът до изходния код следователно е необходимо предварително условие за упражняването на останалите права: без достъп до изходния код не е практически възможно софтуерът да бъде модифициран или използван повторно по подходящ начин.

46. Член 3, параграф 48 обаче не се ограничава единствено до позоваване на лицензионните условия, тъй като с него изрично се изисква изходният код да „е свободно споделян“. Понятието „свободно споделян“ означава, че изходният код трябва да бъде публично достъпен (както „нагоре по веригата“, така и „надолу по веригата“), а не предоставян само при определени ограничения или условия. Съответно разпространяван чрез свободен лиценз с отворен код софтуер с изходен код, който е споделян (или може да бъде споделян) само с клиенти, които извършват плащане, или с ограничена група ползватели, не трябва да се счита за FOSS по смисъла на член 3, параграф 48. Поради това за целите на АК единствено софтуер с изходен код, който е публично достъпен и предоставян чрез свободен лиценз с отворен код, предоставящ пълния набор от права съгласно член 3, параграф 48, следва да се счита за FOSS.

### 3.1. **Определяне дали даден свободен софтуер с отворен код е под нечия отговорност**

47. С АК се установяват ключови отговорности на икономическите оператори, които доставят продукти с цифрови елементи на пазара на ЕС. Съгласно даденото в него определение „производител“ означава физическо или юридическо лице, което доставя продукт с цифрови елементи под своето име или търговска марка в процеса на търговска дейност (като по този начин го пуска на пазара). По същия начин „вносител“ означава физическо или юридическо лице, установено в Съюза, което доставя продукта с цифрови елементи, създаден от физическо или юридическо лице, установено извън Съюза, в процеса на търговска дейност (като по този начин го пуска на пазара). Задълженията на попечителите се прилагат за юридическото лице, което доставя предназначен за търговски дейности FOSS ([12]), но не го пуска на пазара по смисъла на АК.

48. Поради това, за да се определи дали физическо или юридическо лице пуска FOSS на пазара на ЕС, първо трябва да се изясни дали това физическо или юридическо лице действително доставя FOSS. За правилното установяване на приложимите задължения съгласно АК е от съществено значение да се определи дали физическото или юридическото лице действително доставя FOSS. Всъщност, както е припомнено в съображение 18, АК не се прилага за физически или юридически лица, които допринасят с изходен код за продукти с цифрови елементи, отговарящи на критериите за FOSS, които не са под тяхна отговорност.

([12]) Това е необходимо, но не и достатъчно условие за едно юридическо лице да бъде квалифицирано като попечител на софтуер с отворен код, тъй като в определението по член 3, параграф 14 се съдържат допълнителни условия за квалифицирането на дадено юридическо лице като попечител.

49. Предвид особеностите на процеса на разработване на FOSS, който често включва множество сътрудници, децентрализирани модели на сътрудничество и разделение между приноса и вземането на решения, е удачно да се поясни, че се счита, че FOSS е „под отговорността“ на физическите или юридическите лица, които го публикуват и упражняват основен контрол върху решенията за разработването, издаването на версии и разпространението на FOSS (често наричани „структури по поддръжката“). Лицата, които допринасят с изходен код, но не контролират решенията за издаване на версии, пътни карти или управление, се считат за „сътрудници“; в такива случаи FOSS не е под тяхна отговорност, въпреки че са допринесли за него чрез код. Самото съществуване на технически разрешения, като например право за внасяне на промени, не е достатъчно, за да се установи, че FOSS е под отговорността на съответното лице; отговорността се носи от лицата, които публикуват и контролират FOSS.

*Пример 13: индивидуален разработчик или служител на дадено дружество изпраща заявка за сливане, съдържаща софтуерна корекция за сигурност или нова функционалност по проект за FOSS. Структурите по поддръжката на проекта преглеждат, приемат и сливат кода в основното хранилище, като впоследствие го включват в нова версия. В този сценарий лицето, което е изпратило заявката за сливане, е „сътрудник“ и не е обект на АК. Въпреки че това лице е допринесло с изходен код, то не упражнява основен контрол върху решенията за разработването, издаването на версии и разпространението.*

### 3.2. **Определяне дали свободен софтуер с отворен код е пуснат на пазара на ЕС**

50. След като се установи, че даден FOSS е под отговорността на физическо или юридическо лице, трябва да се установи дали това лице го доставя в процеса на търговска дейност, което представлява пускане на пазара.

#### 3.2.1. *Начисляване на цена*

51. Когато физическото или юридическото лице, което доставя FOSS, начислява цена за самия софтуер (напр. чрез начисляване на цена за предварително компилирани файлове в двоичен формат), това лице пуска на пазара продукт с цифрови елементи. Следователно лицето, което пуска FOSS на пазара, е производител съгласно АК.

52. Често производителите на FOSS безплатно доставят версии на този софтуер (често наричани „общностни“ версии), чиято кодова база е (почти) идентична с тази на платената версия. Тези продукти с цифрови елементи обаче са различни продукти: от платената версия се извлича печалба по някакъв начин (напр. чрез начисляване на цена или чрез други средства, както е изложено в настоящия раздел), и следователно тя се счита за пусната на пазара, като с това се задейства прилагането на задълженията на производителя. От безплатно предоставяната версия (общностната версия) не се извлича печалба и следователно тя не се счита за пусната на пазара за целите на АК. Това е така и в случаите, когато платената версия е „разширена“ търговска версия, която надгражда кодовата база на безплатната версия или включва тази версия в по-широкообхватен продукт с цифрови елементи (напр. при модела „отворено ядро“).

53. Ако субектът доставчик на общностната версия е юридическо лице, това юридическо лице също е обект на приложимите за попечителите задължения по отношение на безплатно доставяната от него версия (общностната версия). Ако субектът е физическо лице, безплатно доставяната от него версия (общностната версия) не попада в обхвата на АК.

#### 3.2.2. *Извличане на печалба от други услуги или изискване да се обработват лични данни*

54. Физическо или юридическо лице, което публикува FOSS, може също да го пуска на пазара (т.е. да го доставя в процеса на търговска дейност), когато предоставя софтуера, чрез който извлича печалба от други продукти с цифрови елементи или услуги, или когато изисква 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.

*Пример 14: физическо или юридическо лице публикува безплатно приложение за пазаруване с отворен код. Приложението е достъпно безплатно и позволява на ползвателите да закупуват стоки или услуги чрез него. Чрез приложението лицето, което го е публикувало, може да извлича печалба от други продукти с цифрови елементи и услуги, предлагани чрез него (напр. чрез реклами или комисионни или абонаментни такси). Поради това приложението се счита за пуснато на пазара в процеса на търговска дейност.*

*Пример 15: физическо или юридическо лице публикува свободна VPN с отворен код. Приложението е достъпно безплатно, но чрез него ползвателите могат да заплащат за достъп до допълнителни сървъри или специални IP адреси. Чрез приложението това лице може да извлича печалба от други предлагани чрез него услуги и поради това се счита за пуснато на пазара в процеса на търговска дейност.*

*Пример 16: физическо или юридическо лице публикува свободно приложение с отворен код, предназначено за следене на физическата форма. Приложението е достъпно безплатно, но използването му е обвързано с обработване на лични данни на ползвателите за цели като реклamно таргетиране или анализи, които не са свързани със сигурността, съвместимостта или оперативната съвместимост на софтуера. Поради това изискване за обработване на личните данни като условие за използване на приложението, то се счита за пуснато на пазара в процеса на търговска дейност.*

3.2.3. *Услуги за поддръжка*

55. Самият факт, че физическо или юридическо лице, което публикува FOSS, предлага и свързани с него платени услуги за поддръжка, не означава сам по себе си, че продуктът с цифрови елементи се доставя в процеса на търговска дейност. Услугите за поддръжка могат да включват дейности като консултации, обучение или професионални услуги, свързани с използването, документацията, конфигурирането и внедряването на софтуера от страна на клиента.

56. Решаващият фактор е дали достъпът до самия FOSS (т.е. предоставянето на продукта с цифрови елементи), включително неговата поддръжка, се предоставя срещу възнаграждение или единствено се предлагат професионални услуги, свързани със свободно достъпен продукт с цифрови елементи, както е посочено в съображение 18 от АК („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“). Ако FOSS може да бъде свободно изтеглен и инсталиран и ползвателите могат по избор да закупят професионални услуги отделно, този FOSS не се счита за пуснат на пазара.

57. За разлика от това, в някои случаи достъпът до конкретна версия на продукта с цифрови елементи, включително определени ползи като техническа помощ или оптимизация на работните характеристики, е обвързан с възнаграждение. В такива случаи това предоставяне представлява предоставяне на продукт с цифрови елементи, от което се извлича печалба в процеса на търговска дейност и поради това той се счита за пуснат на пазара. Това включва случаите, в които платено издание или корпоративна версия се предоставят съгласно търговско споразумение, независимо дали функционално еквивалентен софтуер е свободно достъпен чрез лиценз с отворен код.

*Пример 17: физическо или юридическо лице публикува свободна операционна система с отворен код, предлагайки платена версия на тази операционна система, която включва услуги за поддръжка като техническа помощ или оптимизация на работните характеристики. Платената версия на операционната система се счита за пусната на пазара в процеса на търговска дейност.*

*Пример 18: физическо или юридическо лице публикува свободен инструмент за командeн ред с отворен код. Инструментът е свободно достъпен и всеки може да го изтегли и инсталира. Това физическо или юридическо лице отделно предлага професионални услуги като незадължителни консултантски услуги за обучение и подкрепа на ползвателите и подкрепа при инсталирането и използването на инструмента. Този FOSS не се счита за пуснат на пазара по смисъла на АК.*

58. По-специално, в случай на физически лица, които публикуват FOSS, предлагането на директно обвързана с достъпа до продукта с цифрови елементи техническа помощ не се квалифицира като търговска дейност, ако начислената цена служи само за възстановяване на действителните разходи, както е посочено в съображение 15 от АК. Действителните разходи включват например различни разходи, свързани с проектирането, разработването и поддръжката на този софтуер, включително разумните разходи за издръжка на лицето. Поради това физическо лице, което публикува FOSS и предлага техническа помощ, за да покрие разходите си и да получи справедливо възнаграждение, не трябва да се счита само на това основание за пускащо този софтуер на пазара на ЕС.

59. Физическо или юридическо лице, което предлага техническа помощ, свързана с FOSS, който не е под негова отговорност, не се счита за пускащо този софтуер на пазара, освен ако това лице не извършва съществено изменение на FOSS в съответствие с член 22 като част от доставянето на такава помощ.

*Пример 19: доставчик на услуги не публикува FOSS, но помага на клиент да го инсталира на локалния сървър на клиента. Това действие се осъществява без извършване на съществено изменение на този FOSS. Поради това доставчикът на услуги не се счита за лице, което пуска FOSS на пазара.*

3.2.4. *Дарения*

60. Физически или юридически лица, които публикуват проекти за FOSS, обикновено включват начини ползвателите на този софтуер доброволно да даряват средства с цел да благодарят на издателя(ите) на проекта и да осигурят продължаване на активната поддръжка на проекта.

61. Както е посочено в съображение 15 от АК, „приемането на дарения без намерение за извличане на печалба не следва да се счита за търговска дейност“. Самият факт на включване на връзка към платформа за дарения или подобни инструменти за събиране на дарения не следва да се разглежда като намерение за извличане на печалба, дори когато събраната чрез дарения сума надвишава разходите, свързани с проектирането, разработването и предоставянето на продукт с цифрови елементи. Това включва разумно възнаграждение за сътрудниците, наети от юридическото лице, и/или разумни разходи за издръжка на физическото лице. По своята същност даренията варират във времето и поради това следва да се проявява известна гъвкавост при преценката дали FOSS, от който се извлича печалба единствено чрез дарения, се счита за пуснат на пазара. Поради това е малко вероятно FOSS, поддържан единствено чрез дарения, да се счита за пуснат на пазара по смисъла на АК.

*Пример 20: физическо или юридическо лице публикува FOSS в публично онлайн хранилище, позволявайки на всеки да го изтегля, използва, модифицира и преразпределя чрез свободен лиценз с отворен код. Издателят кани ползвателите да направят доброволни дарения чрез платформа за дарения, за да подкрепят продължаващото развитие и поддръжка на проекта. Достъпът до софтуера, неговия изходен код и неговите актуализации не е обвързан с извършването на дарение. Този FOSS не се счита за доставен в процеса на търговска дейност и не се счита за пуснат на пазара по смисъла на АК.*

62. Въпреки това съществуват случаи, когато поддържан чрез дарения FOSS може да се счита за пуснат на пазара. Такъв е случаят, когато въз основа на цялостна оценка на обстоятелствата даренията фактически са еквивалентни на начисляването на цена за достъп до продукта с цифрови елементи или до определени негови функции. По-конкретно такъв може да е случаят, когато достъпът до FOSS, до основни функции или до актуализации практически е обвързан с извършването на дарение или когато даренията са свързани с договорни ползи или изключителни предимства, които надхвърлят предимствата за общността.

*Пример 21: физическо или юридическо лице публикува софтуерен продукт с цифрови елементи чрез свободен лиценз с отворен код, но предоставя версии за изтегляне и актуализации за сигурност единствено на ползвателите, които правят дарение. Ползвателите, които не направят дарение, нямат достъп до текущата версия на софтуера.*

*В този случай даренията фактически са условие за достъп до продукта с цифрови елементи и следователно са еквивалентни на начисляването на цена. Поради това този FOSS се счита за пуснат на пазара по смисъла на АК.*

*Пример 22: физическо или юридическо лице предоставя изходния код на FOSS като публично достъпен, но предоставя предварително компилирани файлове в двоичен формат, редовни актуализации и гарантирани корекции за сигурност само на дарителите. В този случай даренията са свързани с достъпа до основни аспекти на продукта с цифрови елементи и представляват възнаграждение за доставянето на този продукт. Поради това този FOSS се счита за пуснат на пазара в процеса на търговска дейност.*

3.2.5. *Финансиране на свободен софтуер с отворен код*

63. Фактът, че трета страна е заплатила, спонсорирала или по друг начин е финансирала разработването на FOSS, сам по себе си не позволява да се определи дали този FOSS е пуснат на пазара. Честа практика в екосистемата на FOSS е индивидуални разработчици, фондации или общности да получават финансиране от дружества, публични органи или други спонсори, за да работят по конкретни функции, да коригират грешки или да поддържат критични компоненти. Това финансиране може да се извършва под много форми, включително безвъзмездни средства, награди за откриване на уязвимости, спонсорства, поръчки за услуги или платена работа по разработката.

64. Както вече беше припомнено, в съображение 18 от АК се пояснява, че 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.

65. Следователно, когато FOSS е свободно споделян и се предоставя на всички лица като свободно достъпен, използваем, модифицируем и преразпределяем, фактът, че търговско дружество може да е платило за този проект, не следва да допринася за определянето на това дали софтуерът е пуснат на пазара. Всъщност, ако не се извлича печалба от този FOSS по друг начин, той не следва да се счита за пуснат на пазара. Когато дружеството, което е финансирало разработването на FOSS (както и всяко друго дружество), го интегрира в своя продукт с цифрови елементи, това дружество трябва да положи дължимата грижа в съответствие с член 13, параграф 5 от АК.

*Пример 23: индивидуален разработчик публикува проект за FOSS и го поддържа активно. Производител А иска индивидуалният разработчик да добави конкретна функция към този FOSS и финансира тази разработка. Разработчикът добавя функцията към кодовата база на FOSS, като я споделя свободно и я предоставя на всички лица като свободно достъпна, използваема, модифицируема и преразпределяема. Не се счита, че индивидуалният разработчик е пуснал този FOSS на пазара. Ако производителят интегрира FOSS в своя продукт с цифрови елементи, той трябва да положи дължимата грижа в съответствие с член 13, параграф 5.*

3.2.6. *Образувания с нестопанска цел, създадени за постигане на нестопански цели*

66. Когато юридическо лице, което публикува FOSS, е организация с нестопанска цел, „създадена по начин, който гарантира, че всички печалби след разходите се използват за постигането на нестопански цели“ (съображение 18 от АК), публикуваният от него FOSS не се счита за пуснат на пазара. Когато това юридическо лице отговаря на определението за „попечител“, то е обект на съответните задължения (член 24 от АК).

*Пример 24: юридическо лице публикува уеб браузър с отворен код, от който се извлича печалба директно чрез партньорства с търсачки, но всичките му приходи след покриване на разходите се използват за нестопански цели. Уеб браузърът не се счита за пуснат на пазара по смисъла на АК. Юридическото лице, което го публикува, е обект на приложимите за попечителите задължения.*

3.2.7. *Интегриране от други производители*

67. В някои случаи FOSS се публикува от ясно идентифицируемо физическо или юридическо лице, но този FOSS е „предназначен за интегриране от други производители в техните собствени продукти с цифрови елементи“. В такива случаи този FOSS не се счита за пуснат на пазара на ЕС, освен ако лицето, което го публикува (т.е. първоначалният производител), не извлича печалба от него в съответствие с предходните раздели от настоящите насоки.

68. Когато този FOSS не е пуснат на пазара, юридическото лице, което го публикува, би било обект на приложимите за попечителите задължения, ако предоставя устойчива подкрепа в съответствие с определението за „попечител“.

*Пример 25: юридическо лице публикува библиотека FOSS за изграждане на потребителски интерфейси. То не извлича печалба от доставянето на тази библиотека, но я интегрира в един от своите продукти с цифрови елементи (който от своя страна е пуснат на пазара). Библиотеката не се счита за пусната на пазара по смисъла на АК, но е предназначена за интегриране в продукти с цифрови елементи. Юридическото лице, което я публикува, е неин попечител.*

*Пример 26: юридическо лице пуска операционна система на пазара и също така публикува библиотеки FOSS, които да служат като референтни реализации за ползвателите на тази операционна система. Юридическото лице не извлича печалба от библиотеките FOSS, които са предназначени за интегриране в други продукти с цифрови елементи. Юридическото лице, което ги публикува, е попечител на тези библиотеки FOSS.*

3.3. **Задължения на попечителите на софтуер с отворен код**

69. С АК се въвежда новата правна категория „попечител на софтуер с отворен код“ с оглед на „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 [АК]“ (съображение 19 от АК).

70. В някои случаи FOSS се публикува, но не се предоставя на пазара по смисъла на АК от юридическо лице, което „има за цел системно да предоставя устойчива подкрепа за разработването на [FOSS] […], предназначени за търговски дейности, и което гарантира жизнеспособността на тези продукти“ (член 3, параграф 14 от АК). В такива случаи това юридическо лице е обект на приложимите за попечителите задължения.

71. Попечителят се определя като „юридическо лице, различно от производител“, тъй като производителят по дефиниция е физическото или юридическото лице, което пуска (предлага) на пазара продукти с цифрови елементи на пазара под своето име или търговска марка. Дадено юридическо лице може да бъде попечител единствено на продукти с цифрови елементи, отговарящи на критериите за FOSS, които са публикувани, но не са предоставени на пазара по смисъла на АК. Следователно концепцията за попечител се прилага за конкретни случаи на FOSS, 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“ (съображение 19 от АК ([13])), но не са предоставени на пазара по смисъла на АК, и за които юридическото лице, публикуващо този FOSS, системно предоставя подкрепа.

72. Фактът, че дадено юридическо лице е попечител на конкретен FOSS, не означава, че то непременно е попечител и на друг FOSS, който публикува. По същия начин фактът, че дадено юридическо лице е производител на конкретен FOSS, не означава, че то не може да бъде попечител на друг FOSS. Това включва предоставянето на „общностни“ версии на същия FOSS, както е описано в раздел *3.2.1 Начисляване на цена*.

73. Следователно дадено юридическо лице може едновременно да бъде попечител на конкретен FOSS (когато попечителят системно предоставя устойчива подкрепа и гарантира жизнеспособността на софтуера) и производител на друг конкретен FOSS (когато го пуска на пазара). С други думи, от един правен субект може да се изисква да изпълнява различни роли за различни проекти за FOSS.

74. За всеки конкретен FOSS, който публикува, юридическото лице ще трябва да установи дали този FOSS се счита за пуснат на пазара по смисъла на АК. Ако е така, правният субект се явява производител на софтуера. Ако FOSS не се счита за пуснат на пазара, юридическото лице може да бъде негов попечител, ако софтуерът е предназначен за търговски дейности и ако юридическото лице го поддържа в съответствие с определението за попечител ([14]).

#### 3.3.1. *Устойчива подкрепа и гарантиране на жизнеспособността на FOSS*

75. В съображение 19 се разяснява, че предоставянето на устойчива подкрепа за разработването на продукт с цифрови елементи може да включва (без да се ограничава до): i) хостинг и управление на платформи за сътрудничество при разработването на софтуер; ii) хостинг на изходен код или софтуер; iii) администриране или управление на продукти с цифрови елементи, квалифицирани като FOSS; и iv) направляване на разработването на такива продукти с цифрови елементи.

76. Такъв може да бъде случаят, когато правният субект разработва FOSS за интегриране в собствените си продукти с цифрови елементи и след това го публикува, без да го пуска на пазара. Това също се разглежда в раздел *3.2.7 Интегриране от други производители*. В този случай юридическото лице не е производител на софтуера, но може да бъде негов попечител. Освен това, както е обяснено и в предходните раздели, юридическо лице, което публикува свободна (или общностна) версия и извлича печалба от версия на същия FOSS, се счита за попечител на свободната (или общностната) версия и за производител на версията, от която извлича печалба.

77. По същия начин правен субект, който извлича печалба от FOSS, но е образувание с нестопанска цел, чиито приходи след приспадане на разходите се използват за постигане на нестопански цели (и следователно неговият FOSS не е пуснат на пазара по смисъла на АК, както е посочено в раздел *3.2.6 Образувания с нестопанска цел*), е попечител на FOSS, който публикува.

78. Освен това някои фондации предлагат платформи за сътрудничество с различни форми на управление, чрез които производителите могат да допринасят редовно за разработването на FOSS и/или които се финансират редовно от производителите. Такива фондации трябва да се считат за попечители във връзка с конкретни FOSS, които са предназначени за търговски дейности и за които фондацията предлага устойчива подкрепа. Въпреки това, както е обяснено в раздел *3.3 Задължения на попечителите на софтуер с отворен код*, такава фондация може да не бъде обект на задължения съгласно АК за други конкретни FOSS, които хоства, в случаите, когато не предоставя системно подкрепа за конкретен FOSS, не гарантира неговата жизнеспособност и/или този конкретен софтуер не е предназначен за търговски дейности.

([13]) Това понятие се съдържа и във формулировката „предназначени за търговски дейности“, включена в определението за „попечител на софтуер с отворен код“, дадено в член 3, параграф 14 от АК.

([14]) Правният субект може също така да не е обект на задължения съгласно АК в случаите, когато: i) конкретен FOSS не е пуснат на пазара по смисъла на АК; и ii) правният субект не отговаря на определението за попечител във връзка с този конкретен FOSS.

79. Видът „устойчива подкрепа“, която фондациите и подобни организации предоставят на конкретни проекти за FOSS, може да варира в значителна степен. Например някои юридически лица предоставят само нетехническа подкрепа, като например управление на брандинга на проекта, определяне на правила за управление, организиране на събития на общността или събиране на дарения. Други субекти предоставят също основната ИТ инфраструктура, необходима за изпълнението на проекта, като например хостване на хранилища за изходен код, предоставяне на системи за контрол на версиите или генериране на ключове за подписване. Трети образувания разширяват обхвата на предоставяната от тях подкрепа, като активно допринасят с инженерни ресурси за проекта — например чрез наемане на разработчици, координиране на работата по разработката, преглед или сливане на кодове, управление на версиите или обработване на докладите за уязвимостите и корекциите за сигурност. Въпреки че всички правни субекти, които се квалифицират като попечители по смисъла на АК, трябва да спазват задълженията по член 24, параграфи 1 и 2, степента, в която предвидените в член 14, параграфи 1, 3 и 8 задължения се прилагат за тези правни субекти, варира в зависимост от вида на предоставяната от тях подкрепа в съответствие с член 24, параграф 3.

80. Например попечител, който предоставя само нетехническа подкрепа, по дефиниция не участва в разработването на продукта с цифрови елементи и следователно не е длъжен да докладва за активно използвани уязвимости. Този попечител също така не предоставя мрежови и информационни системи за разработването на такива продукти с цифрови елементи и следователно не е длъжен да докладва за сериозни инциденти на ENISA и ЕРИКС или на засегнатите ползватели. Въпреки това, когато попечителят е узнал за активно използвана уязвимост (напр. чрез доклад от външни източници като изследователи по сигурността), той следва да сподели информацията със структурите по поддръжката на продукта с цифрови елементи в съответствие със своята политика за киберсигурност. Структурите по поддръжката на продуктите с цифрови елементи и/или попечителите също следва да обмислят доброволно докладване на уязвимостта в съответствие с член 15.

81. От друга страна, когато попечителят предоставя основната ИТ инфраструктура за определени продукти с цифрови елементи, той е длъжен да нотифицира ENISA и ЕРИКС в съответствие с член 14, параграф 3 за всички сериозни инциденти, свързани с тази инфраструктура, които оказват въздействие върху сигурността на продуктите с цифрови елементи. Той също така е длъжен, когато е целесъобразно, да информира всички ползватели (напр. чрез общо съобщение). Както е посочено в предходната точка, въпреки че от попечителя не се изисква да докладва за активно използвани уязвимости, за които е узнал, той следва да насърчава правилното отстраняване на уязвимостите и да обмисли доброволно докладване в съответствие с член 15.

82. И накрая, когато попечителят предоставя и инженерни ресурси за конкретни продукти с цифрови елементи, той е длъжен: i) да нотифицира активно използваните уязвимости, за които е узнал, в съответствие с член 14, параграф 1; и ii) да информира всички ползватели, когато е целесъобразно. Доколкото попечителят има и преки отношения със засегнатите ползватели, той също е длъжен да ги информира в съответствие с член 14, параграф 8.

83. Когато даден субект преустанови системното предоставяне на устойчива подкрепа за конкретен FOSS, той може вече да не отговаря на определението за попечител и следователно може вече да не е обект на съответните задължения. В такива случаи този субект се насърчава ясно да съобщи промяната в статута си за този конкретен FOSS.

84. В определени ситуации даден субект, който е бил попечител на конкретен проект, може да вземе решение за пряко извличане на печалба от този проект, в резултат на което този продукт с цифрови елементи се пуска на пазара и се задействат задълженията на производителя съгласно АК. При такива обстоятелства този субект се квалифицира като производител на продукта с цифрови елементи от датата, на която го пуска на пазара (но не и по отношение на по-ранни версии, за които е действал като попечител).

### 3.4. **Сътрудници и употреба надолу по веригата**

85. Както вече беше споменато в раздел *3.1 Определяне дали даден свободен софтуер с отворен код е под нечия отговорност*, в АК се пояснява, че той 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“ (съображение 18).

86. Производителите на продукти с цифрови елементи, които интегрират компоненти на FOSS в свои собствени продукти с цифрови елементи, също не носят отговорност за индивидуалното съответствие на тези компоненти с АК дори когато производителите допринасят с изходен код за тяхната поддръжка.

87. По същия начин самият факт, че производителите интегрират компоненти на FOSS в свои собствени продукти с цифрови елементи (от които извличат печалба), не засяга състоянието на този компонент на FOSS съгласно АК. Структурите по поддръжката на компоненти на FOSS, които не са пуснати на пазара, нямат задължения по отношение на други субекти, които могат да интегрират такива компоненти в своите продукти с цифрови елементи. Прилагането на АК за даден компонент на FOSS зависи единствено от това дали физическото или юридическото лице, което го публикува, го пуска на пазара.

88. Въпреки това производителите на продукти с цифрови елементи, които интегрират компоненти на FOSS, са длъжни да спазват АК за своите собствени продукти с цифрови елементи. Те също така имат задължение за полагане на дължимата грижа по отношение на интегрираните от тях компоненти на FOSS в съответствие с член 13, параграф 5. Освен това те са задължени да докладват за установените уязвимости в интегрираните компоненти и да споделят корекции за сигурност в съответствие с член 13, параграф 6. За повече насоки по тази тема вж. раздел *9.2.1 Докладване нагоре по веригата и споделяне на корекции за сигурност*.

### 3.5. **Илюстративни сценарии**

89. Изброените по-долу примери са напълно хипотетични и имат за цел единствено да илюстрират различни случаи, разяснени в разделите по-горе.

*Пример 27: индивидуален разработчик А е разработил FOSS. Разработчик А публикува този FOSS под своето име или търговска марка, но не начислява цена за използването му. Софтуерът е свободно споделян и се предоставя на всички като свободно достъпен, използваем, модифицируем и преразпределяем. Разработчик А също така включва връзка към платформа за събиране на доброволни дарения.*

*Дружества Б, В и Г интегрират този FOSS в свои собствени продукти с цифрови елементи. За да подкрепят текущата поддръжка, дружества Б, В и Г правят доброволни дарения в полза на разработчик А. Чрез тези дарения разработчик А поддържа проекта активно.*

*Този FOSS не е пуснат на пазара по смисъла на АК. Разработчик А няма задължения съгласно АК. Дружества Б, В и Г трябва да полагат дължимата грижа в съответствие с член 13, параграф 5, когато интегрират този FOSS в свои собствени продукти с цифрови елементи.*

*Пример 28: фондация с нестопанска цел Е публикува компонент на FOSS за интегриране в други продукти с цифрови елементи за търговски цели. Фондация Е се ангажира да предоставя устойчива подкрепа за този FOSS с цел гарантиране на неговата жизнеспособност и въвеждане. Дружества А, Б и В интегрират този FOSS в свои собствени продукти с цифрови елементи. Дружества А и Б доброволно допринасят чрез част от времето на своите разработчици за развитието и поддръжката на проекти за FOSS в рамките на фондация Е, включително за този FOSS.*

*Тъй като фондация Е е организация с нестопанска цел, създадена по начин, който гарантира, че всички приходи след приспадане на разходите се използват за постигане на нестопански цели, FOSS не се счита за пуснат на пазара по смисъла на АК. Фондация Е е попечителят на FOSS и е обект на съответните задължения, предвидени в член 24. Дружества А, Б и В трябва да полагат дължимата грижа в съответствие с член 13, параграф 5, когато интегрират този FOSS в свои собствени продукти с цифрови елементи.*

*Пример 29: дружество А е разработило компонент на FOSS за интегриране в свои собствени продукти с цифрови елементи. То също така публикува този FOSS отделно под своето име или търговска марка и активно го поддържа. То обаче не изисква заплащане за използването му и не извлича печалба от него по друг начин. Дружества Б, В и Г интегрират този FOSS в свои собствени продукти с цифрови елементи и доброволно допринасят с част от времето на своите разработчици за неговата поддръжка.*

*Този FOSS не се счита за пуснат на пазара по смисъла на АК. Дружество А не е негов производител, а е негов попечител. Дружества Б, В и Г трябва да полагат дължимата грижа в съответствие с член 13, параграф 5, когато интегрират този FOSS в свои собствени продукти с цифрови елементи.*

*Пример 30: дружество А публикува FOSS под своето име или търговска марка и го предлага като платена версия, която включва определени предимства като техническа помощ или оптимизация на работните характеристики. Разработчици от дружества Б, В и Г допринасят за поддръжката на FOSS, но той остава под контрола на дружество А.*

*Дружество А се счита за производител на този FOSS ([15]). Дружества Б, В и Г не са обект на задължения съгласно АК за този конкретен FOSS. Ако интегрират този FOSS в свои собствени продукти с цифрови елементи, те трябва да положат дължимата грижа в съответствие с член 13, параграф 5.*

*Пример 31: дружество А публикува FOSS под своето име или търговска марка и предоставя текуща поддръжка с оглед гарантиране на неговата дългосрочна жизнеспособност с цел интегриране на този софтуер в продукти с цифрови елементи на други дружества. Дружество А не изисква заплащане за използването му, не обработва лични данни, които събира чрез продукта с цифрови елементи, и не продава услуги за поддръжка, свързани с публикуването на FOSS.*

*Дружество Б допринася чрез код и време на разработчици за поддръжката на FOSS, но не го разпространява за търговски цели. Дружество Б предлага услуги за техническа поддръжка независимо от разпространението на FOSS. Дружество А се счита за попечител на този FOSS, а дружество Б няма задължения съгласно АК във връзка с този FOSS.*

*Пример 32: компонент на FOSS се публикува от организация с нестопанска цел, създадена по начин, който гарантира, че всички печалби след разходите се използват за постигането на нестопански цели. Субектът предоставя устойчива подкрепа, за да гарантира дългосрочната жизнеспособност на проекта. Поддръжката се осигурява чрез публично финансиране, като например безвъзмездни средства за изследвания. Допълнителни разработки, включително нови функции, се финансират чрез дарения и конкретни проекти, изпълнявани в партньорство с производители, които интегрират този FOSS в своите продукти с цифрови елементи. Тези функции се включват в кодовата база на FOSS.*

*Организацията с нестопанска цел, която публикува FOSS, се счита за попечител на този компонент на FOSS. Производител, който е допринесъл за разработването на определени функции, не се счита за производител на този компонент на FOSS. Когато производителят интегрира този компонент на FOSS в свой собствен продукт с цифрови елементи, той трябва да положи дължимата грижа в съответствие с член 13, параграф 5.*

*Пример 33: организация с нестопанска цел, създадена по начин, който гарантира, че всички печалби след разходите се използват за постигането на нестопански цели, публикува комплект за разработване на FOSS (SDK) и осигурява неговата текуща поддръжка. SDK е свободно споделян и се предоставя на всички като свободно достъпен, използваем, модифицируем и преразпределяем. Финансирането се осигурява чрез членски вноски, изплащани на организацията с нестопанска цел, а наети от организациите членки разработчици допринасят за разработването на SDK чрез код и други ресурси. Производителите използват SDK като компонент за създаване на други продукти с цифрови елементи.*

*Организацията с нестопанска цел, която публикува този SDK, е негов попечител. Членовете на фондацията не носят отговорност за съответствието на SDK с АК. Когато производителите използват SDK за създаване на свои собствени продукти с цифрови елементи, те трябва да положат дължимата грижа в съответствие с член 13, параграф 5.*

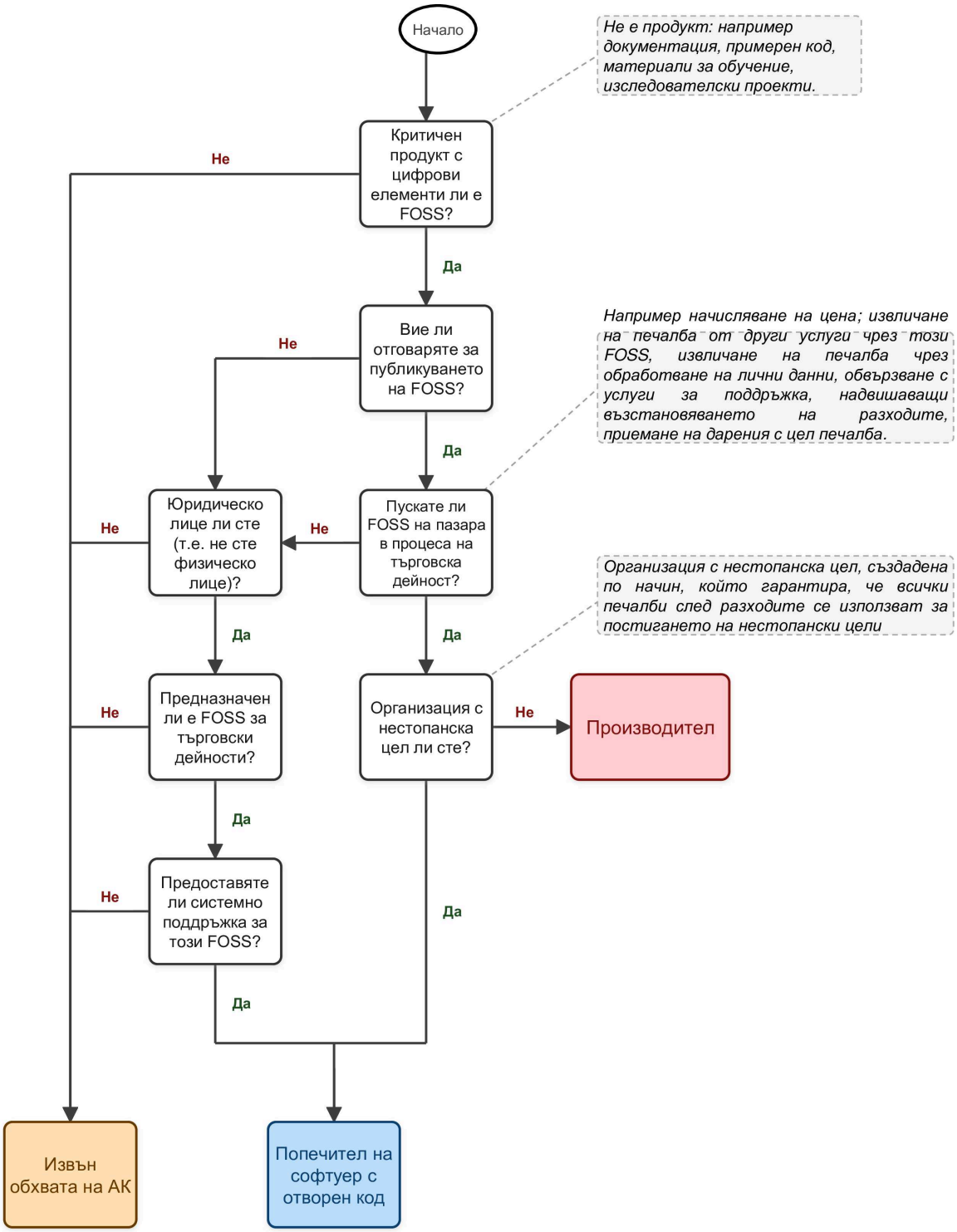
*Пример 34: индивидуален разработчик публикува библиотека FOSS в публично хранилище за пакети за даден програмен език и активно я поддържа. В документацията на пакета разработчикът добавя връзка за събиране на дарения. Производител свободно изтегля тази библиотека от хранилището и я интегрира в свой собствен продукт с цифрови елементи.*

*Спрямо индивидуалния разработчик и хранилището за пакети се прилагат задължения съгласно АК. Производителят, който интегрира библиотеката, трябва да положи дължимата грижа в съответствие с член 13, параграф 5.*

([15]) Освен ако дружество А не е организация с нестопанска цел, създадена по начин, който гарантира, че всички печалби след разходите се използват за постигането на нестопански цели, в който случай тя е попечител на този FOSS.

*Фигура 1*

**Стилизирана схема на обхвата на АК по отношение на свободния софтуер с отворен код**




## 4. СЪЩЕСТВЕНИ ИЗМЕНЕНИЯ И РЕЗЕРВНИ ЧАСТИ

90. Съгласно определението в член 3, параграф 30 от АК „съществено изменение“ означава промяна на продукта с цифрови елементи след пускането му на пазара, която i) засяга съответствието на продукта с цифрови елементи със съществените изисквания за киберсигурност, определени в приложение I, част I; или ii) води до промяна на предназначението, за което е оценен продуктът с цифрови елементи.

91. Понятието „съществено изменение“ е от значение за установяване на задълженията по АК в редица случаи, включително следните:

a) в съответствие с член 21 вносител или дистрибутор, който извършва съществено изменение на продукт с цифрови елементи, който вече е пуснат на пазара, се счита за негов производител;

b) в съответствие с член 22 всяко физическо или юридическо лице, което извършва съществено изменение на продукт с цифрови елементи и го предоставя на пазара, се счита за негов производител;

c) в съответствие с член 69, параграф 2 всяко физическо или юридическо лице, което извършва съществено изменение след 11 декември 2027 г. на продукт с цифрови елементи, пуснат на пазара преди 11 декември 2027 г., и го пуска на пазара, се счита за негов производител;

d) за производителите на продукти с цифрови елементи, пуснати на пазара след 11 декември 2027 г., с цел да се определи дали е необходимо прилагането на нова процедура за оценяване на съответствието на даден продукт с цифрови елементи поради извършени след тази дата промени, по-конкретно с оглед на итеративния характер на разработването на софтуер.

92. Поради това е важно да се предоставят насоки, с които да се подпомогнат икономическите оператори в процеса на разбиране кога дадено изменение на софтуер или хардуер се квалифицира като съществено изменение.

### 4.1. **Физически ремонти**

93. Както е посочено в съображение 42 от АК, „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, 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“. Това е в съответствие с раздел 2.1 от Синьото ръководство, в който се припомня, че „продукт, който е претърпял значителни промени или трансформации, след като е пуснат в действие, трябва да се разглежда като нов продукт, ако: i) първоначалните му работни характеристики, цел или тип са променени, без това да е предвидено в първоначалната оценка на риска; ii) естеството на опасността се е променило или степента на риска се е увеличила предвид съответното законодателство на Съюза за хармонизация; и iii) продуктът се предоставя на пазара (или се пуска в действие, ако приложимото законодателство обхваща и пускането в действие). Това трябва да се преценява за всеки отделен случай, и по-специално в контекста на целите на законодателството и типа на продуктите, обхванати от въпросното законодателство“.

94. Резултатът от операциите по обновяване, поддръжка или ремонт, които водят до физически модификации на продукти с цифрови елементи, които вече са пуснати на пазара, не винаги е съществено изменение. Поради това следва да се извърши оценка за всеки отделен случай, за да се установи дали с такава физическа модификация се засяга съответствието на продукта с цифрови елементи със съществените изисквания, определени в приложение I, част I, или се изменя предназначението на продукта, което е част от обхвата на оценката на киберриска.

95. Замяната на дефектни части или износени елементи с части с по-добри работни характеристики (напр. поради технически прогрес или прекратено производство на старата част) сама по себе си не представлява съществено изменение на ремонтирания продукт с цифрови елементи. Това се случва само ако с промяната в работните характеристики или начина, по който работи ремонтираният продукт с цифрови елементи, i) се засяга неговото съответствие със съществените изисквания или ii) се изменя предназначението, което не е част от обхвата на оценката на риска.

*Пример 35: производителят на компютърен сървър извършва операция по ремонт, като заменя дефектна RAM с нова и по-ефективна. Съответствието на сървъра със съществените изисквания не е засегнато. Сървърът работи по-добре, но новите му работни характеристики остават в рамките на предвидената му употреба, както е разгледано в оценката на киберриска. Компютърният сървър не се счита за съществено изменен.*

4.2. **Резервни части**

96. Съгласно член 2, параграф 6 от АК резервни части, предназначени за замяна на идентични компоненти и произведени съгласно същите спецификации като тези компоненти, не са обект на АК. В съображение 29 допълнително се посочва, че това освобождаване обхваща както резервните части за ремонт на заварени модели продукти, предоставени преди датата, от която се прилага АК, така и резервните части, които вече са преминали процедура за оценяване на съответствието съгласно АК.

97. Освобождаването по член 2, параграф 6 от АК следва да се разбира като приложимо само когато резервната част се доставя специално за ремонт или за удължаване на трайността на даден продукт с цифрови елементи, който вече е пуснат на пазара (преди или след 11 декември 2027 г.). Когато продукт с цифрови елементи се доставя като самостоятелен продукт, без това да е свързано с поддръжката или ремонта на съществуващ продукт с цифрови елементи, той се пуска на пазара по смисъла на АК и не следва да се счита за резервна част, попадаща в обхвата на член 2, параграф 6. Целта на поддръжката или ремонта следва да бъде очевидна от контекста на доставката — например чрез идентифициране на продукта с цифрови елементи или на семейството продукти в поръчката или търговската оферта или чрез доставка посредством канали за следпродажбено обслужване или сервиз. В тази връзка подкрепящи доказателства също следва да са на разположение на органите за надзор на пазара. Фактът, че даден продукт с цифрови елементи технически би могъл да се използва за замяна на компонент, сам по себе си не е достатъчен, за да бъде включен този продукт в обхвата на освобождаването при липса на такива елементи.

98. Съответно, когато резервната част е идентична с компонент на продукт с цифрови елементи, който е пуснат на пазара преди датата, от която се прилага АК, или в съответствие с АК, тази резервна част сама по себе си не е обект на АК.

99. При преценката дали една резервна част следва да се счита за идентична с даден компонент следва да се акцентира върху нейната функционална роля в продукта с цифрови елементи и характеристиките, които могат да бъдат от значение за киберсигурността. Въпреки че винаги е необходима оценка за всеки отделен случай, разликите, с които не се засягат характеристиките за сигурност или киберрисковия профил на компонента, сами по себе си не са основание за изключване на тази резервна част от обхвата на член 2, параграф 6 от АК.

100. За разлика от тях разликите в свързаните с киберсигурността на компонента характеристики като алгоритми, протоколи, криптографски механизми, функции за контрол на достъпа или други свързани със сигурността характеристики могат да са основание да се счита, че новата част не е идентична с компонента, за чиято замяна е предназначена.

101. Когато резервната част не е идентична с оригиналния компонент, сама по себе си тази резервна част представлява продукт с цифрови елементи и следователно попада в обхвата на АК. В такива случаи съответствието със съществените изисквания трябва да се оценява с оглед на предназначението на заменящия компонент. От особено значение е функцията на заменящия компонент за осигуряване на съвместимост или оперативна съвместимост със съществуващ продукт с цифрови елементи, включително когато този продукт с цифрови елементи е пуснат на пазара преди датата, от която се прилага АК. Когато определени съществени изисквания не могат разумно да бъдат изпълнени поради това предназначение или технически ограничения, производителят трябва да отрази това в оценката на киберриска и да приложи подходящи алтернативни или компенсаторни мерки за намаляване на риска, така че да не бъде застрашена сигурността на продукта с цифрови елементи. Както е разгледано и в раздел *2.6 Сложни системи*, техническата документация и информацията и инструкциите за ползвателя са от решаващо значение за прозрачното описване на идентифицираните ограничения, свързаните киберрискове и приложените мерки за намаляване на риска. Както е разяснено в раздел *4.1 Physical repairs*, замяната на дефектни части или износени елементи с части с по-добри работни характеристики сама по себе си не представлява съществено изменение на ремонтирания продукт с цифрови елементи.

*Пример 36: производител е пуснал свързани контролери на пазара на ЕС. В единия случай контролерът е пуснат на пазара през 2026 г., т. е. преди датата, от която се прилага АК. В другия случай контролерът е пуснат на пазара през 2028 г. в съответствие с АК. През 2028 г. модул за цифрова комуникация и в двата вида контролери се повреждa. Производителят доставя като резервна част заменящ модул, който е идентичен и произведен съгласно същите спецификации като оригиналния.*

*И в двата случая заменящият модул попада в обхвата на освобождаването по член 2, параграф 6. Резервната част сама по себе си не е обект на АК, въпреки че е продукт с цифрови елементи, тъй като с нея се заменя идентичен компонент в продукт с цифрови елементи. Ремонтът не представлява съществено изменение на продукта с цифрови елементи.*

*Пример 37: производител е пуснал свързан промишлен контролер на пазара на ЕС през 2026 г., т. е. преди датата, от която се прилага АК. През 2028 г. комуникационна интегрална схема в този контролер се повредила. Тъй като производителят вече не произвежда тази интегрална схема, той доставя като резервна част по-нова интегрална схема с еквивалентна функционалност, но с различна криптографска реализация и актуализиран механизъм за защитено зареждане, за да се поддържа съвместимост и непрекъсната работа.*

*В този случай заменящата интегрална схема не може да се счита за идентична, тъй като разликите в криптографската реализация и механизма за защитено зареждане засягат свързаните с киберсигурността на интегралната схема свойства. Поради това тя не попада в обхвата на освобождаването по член 2, параграф 6 и представлява продукт с цифрови елементи, който е предмет на АК. Съответствието на заменящата част трябва да бъде оценено с оглед на нейното предназначение, включително нейната роля за осигуряване на оперативна съвместимост с продукта с цифрови елементи, пуснат на пазара преди датата, от която се прилага АК.*

*Пример 38: производител пуска на пазара контролер за интелигентни сгради през 2028 г. в съответствие с АК. През 2029 г. безжичният модул в този контролер се повредил. Тъй като производителят вече не произвежда този модул, той доставя като резервна част нов модул, който изпълнява същата функция чрез същите комуникационни протоколи и механизми за сигурност, но е базиран на различен набор от интегрални схеми и е с актуализиран софтуер на производителя, който не променя характеристиките, които могат да бъдат от значение за киберсигурността.*

*В този случай заменящият модул може да се счита за идентичен. Поради това модулът попада в обхвата на освобождаването по член 2, параграф 6 и не е предмет на АК.*

102. Освобождаването се прилага за резервни части независимо дали със съответната резервна част се заменя компонент на продукт с цифрови елементи или цял продукт с цифрови елементи, който сам по себе си е част от по-голям продукт, включително когато този по-голям продукт с цифрови елементи се състои от няколко интегрирани компонента, при условие че заменящата част е специално доставена като резервна част, както е обяснено в предходните параграфи.

*Пример 39: през 2027 г. производител пуска на пазара система за индустриална автоматизация, която включва програмируем логически контролер (PLC) като един от своите компоненти. През 2031 г. централният процесор (CPU) на PLC се повредил. Производителят предлага две опции за ремонт: i) доставка на заменящ CPU, който може да се счита за идентичен с първоначално инсталирания CPU; или ii) доставка на заменящ PLC, който може да се счита за идентичен с първоначално инсталирания PLC. Във всеки от случаите заменящият елемент се доставя чрез канала за следпродажбено обслужване на производителя като резервна част и системата за индустриална автоматизация, за която е предназначен заменящият елемент, е ясно идентифицирана. И в двата случая заменящият елемент попада в обхвата на освобождаването по член 2, параграф 6, независимо дали замяната се отнася до компонент на PLC или самия PLC.*

### 4.3. **Софтуерни актуализации като съществени изменения**

103. По своята същност разработването на софтуер е повтарящ се процес, като софтуерните продукти с цифрови елементи, които вече са пуснати на пазара, се актуализират често и непрекъснато. В този контекст е удачно да се предоставят повече насоки относно установяването на случаите, когато даден софтуер трябва да се счита за съществено изменен. Целта на тези насоки е по-конкретно да се подпомогнат производителите на софтуерни продукти с цифрови елементи, които извършват промени в собствените си продукти, да определят дали съответната промяна представлява съществено изменение.

104. В съображение 39 се посочва, че даден продукт с цифрови елементи се счита за съществено изменен, когато се променя нивото на киберриска и производителят не е взел предвид променения или допълнителния риск в първоначалната оценка на риска и при съответствието със съществените изисквания впоследствие. Поради това производителят следва да оцени за всеки отделен случай дали с дадена софтуерна актуализация се въвеждат нови или увеличени киберрискове и дали тези рискове вече са били разгледани в неговата оценка на риска.

105. Когато производител въвежда нови функционалности в продукт с цифрови елементи, които водят до промяна на предназначението на продукта като цяло, има вероятност производителят да не е взел предвид тези промени в своята оценка на риска. При такива обстоятелства промяната обикновено би се квалифицирала като съществено изменение.

*Пример 40: производител пуска на пазара табло за събиране на данни от машини и за показване на тенденции и предупреждения, без да има възможност за управление на тези машини. Впоследствие производителят разработва нова версия на това табло, въвеждайки функционалности, които му позволяват да управлява машините, включително чрез регулиране на работните параметри и рестартиране на машините след повреда. В резултат на тези промени е налице развитие по отношение на предназначението на таблото, предвидено в оценката на риска, тъй като то се превръща от инструмент за ситуационна осведоменост в продукт с цифрови елементи, предназначен за оперативен контрол върху други устройства. Следователно таблото е съществено изменено.*

*Пример 41: производител пуска на пазара потребителско софтуерно приложение, предназначено за организиране и показване на лични данни като имейли, съобщения или документи и за поддържане на основни функции за търсене и филтриране. Впоследствие производителят въвежда актуализация, с която се позволява на приложението автоматично да анализира потребителското съдържание с цел генериране на поведенчески профили и вземане на автоматизирани решения относно приоритизирането, потискането или препоръчването на съдържание без намесата на ползвателя. В резултат на тази промяна предназначението на софтуера се изменя от инструмент за управление на информацията от ползвателя на система за автоматизирано вземане на решения, което не е било предвидено в оценката на риска. Следователно приложението е съществено изменено.*

106. В същото време обаче е възможно производителят постепенно да въвежда нови функции, които вече са включени в неговата оценка на риска или които сами по себе си не променят киберрисковия профил на продукта с цифрови елементи. Това може да бъде случаят например, когато производителят е предвидил разработването на тези функции, вече е описал и оценил свързаните рискове и е приложил подходящи мерки за смекчаване, за да осигури продължаващо изпълнение на съществените изисквания. Такъв също може да бъде случаят, когато с новите функции не се извършват промени, в резултат на които възникват нови или увеличени рискове. Поради това актуализации от този характер не следва да се считат за съществени изменения, тъй като с тях не се увеличава киберрискът и съответно не се променя изпълнението на съществените изисквания.

*Пример 42: приложение за съобщения първоначално се пуска с функция, ограничена до съобщения между двата ползватели. В обхвата на оценката на риска на производителя е включено въвеждането на групови съобщения на по-късен етап, включително например повишената сложност на маршрутизирането на съобщенията. В последваща актуализация производителят добавя функция за групов чат заедно с администраторски контроли и инструменти за модериране, които вече са били предвидени и оценени в първоначалния дизайн. С актуализацията се въвеждат функции, които са в обхвата на първоначалното предназначение и оценка на риска. Следователно приложението за съобщения не е съществено изменено.*

*Пример 43: система за мониторинг на производството се пуска на пазара с активирани табла само за четене, докато функциите за автоматизирано управление са част от архитектурата на системата, но остават дезактивирани. В обхвата на извършената от производителя оценка на риска изрично е включено бъдещото активиране на автоматизирани цикли на управление, включително свързаните с управлението в затворени цикли киберрискове и защитни мерки като механизми за ръчна намеса от оператора и безопасно състояние в случай на авария. В по-нова актуализация производителят активира функциите за автоматизирано управление и защитните мерки, както е първоначално оценено. Следователно системата за мониторинг на производството не е съществено изменена.*

107. Обратно, в резултат на функции, които са ограничени или привидно от несъществено значение, могат да възникнат значителни киберрискове, засягащи съответствието със съществените изисквания. Поради това оценката на дадено съществено изменение не следва да се основава на мащаба или сложността на промяната, а на нейното потенциално неблагоприятно въздействие върху киберрисковия профил на продукта с цифрови елементи и съответно върху изпълнението на съществените изисквания.

*Пример 44: производител въвежда актуализация на софтуерно приложение, като добавя функция за запомняне или за постоянно влизане, с която локално се съхраняват токени за автентификация с цел по-голямо удобство за ползвателя. Въпреки че функцията е ограничена по обхват, с нея се въвеждат нови рискове, свързани с кражба на токени, непозволен достъп и отвличане на сесии, които не са били взети предвид в оценката на риска. Следователно актуализацията засяга съответствието със съществените изисквания. Софтуерното приложение е съществено изменено.*

*Пример 45: производител добавя нова функция за регистриране и диагностика към съществуващ софтуерен продукт с цифрови елементи, с която се позволява експортирането на подробни системни регистри за целите на отстраняването на неизправности. Въпреки че функцията изглежда незначителна, чрез нея се събират и съхраняват чувствителни оперативни данни в некриптиран формат, в резултат на което се въвеждат рискове от излагане на данни, които не са били предварително оценени или намалени. Следователно промяната може да има значително въздействие върху киберрисковия профил на продукта с цифрови елементи. Софтуерният продукт с цифрови елементи е съществено изменен.*

108. В съответствие със съображение 39 от АК актуализациите за сигурност по принцип не следва да се считат за съществени изменения, тъй като тяхната основна цел е да се намали нивото на киберриска, свързан с даден продукт с цифрови елементи. Поради това дадена актуализация за сигурност, с която не се променя предназначението на такъв продукт и не се въвеждат нови киберрискове, не следва да се счита за съществено изменение дори когато с нея могат да се въведат значителни технически промени. Това включва случаите, в които определени функции са изменени или ограничени единствено с цел смекчаване на установени уязвимости и осигуряване на продължаващо съответствие със съществените изисквания.

*Пример 46: производител внедрява актуализация за сигурност с цел отстраняване на уязвимост в кодовата база на продукт с цифрови елементи чрез коригиране на грешка при валидирането на входящите данни, в резултат на която буферът може да се препълни, или чрез коригиране на логически дефект, в резултат на който удостоверяването на автентичността може да се заобиколи чрез неправилно валидиране на токени за сесия. С актуализацията се променя вътрешното изпълнение на софтуера, без да се засяга предназначението на продукта или да се въвежда излагане на риск. Такава актуализация е предназначена единствено за нападаване на киберриска. Актуализацията за сигурност не следва да се счита за съществено изменение.*

*Пример 47: производител въвежда актуализация за сигурност, с която се укрепват съществуващите конфигурации за сигурност, като например прилагане на по-строги правила на защитната стена, дезактивиране на неизползвани мрежови портове, промяна на политиките за пароли на администратора по подразбиране или въвеждане на задължително многофакторно удостоверяване на автентичността, когато такава функция вече е била налична или предвидена. Въпреки че с актуализацията може да се засегне начина на конфигуриране на продукта с цифрови елементи или осъществяването на достъп до него от страна на ползвателите, чрез нея не се променя предназначението му и единствената ѝ цел е да се подобри неговия модел на киберсигурност. Актуализацията за сигурност не следва да се счита за съществено изменение.*

*Пример 48: производител пуска на пазара софтуерен продукт с цифрови елементи за обезпечаване на сигурността на комуникациите чрез конфигурируема рамка за криптиране, поддържаща множество криптографски алгоритми и размери на ключове, както е описано в техническата документация и оценката на риска на продукта. В обхвата на оценката на риска са включени всички опции за криптиране, предоставени като част от продукта с цифрови елементи, и се предвижда извеждането на определени алгоритми от употреба в бъдеще. В оценката на риска също са включени мерки за смекчаване като криптогъвкавост, вътрешно управление на ключове и тестване за съвместимост. В отговор на новоиздадени насоки за криптиране производителят внедрява актуализация за сигурност, с която дезактивира остарял алгоритъм и активира по-стабилна алтернатива, която вече се поддържа, без да въвежда нови външни зависимости или да променя информационните потоци. Тъй като с актуализацията се прилага мярка за сигурност, която е била предвидена и оценена като част от първоначалния дизайн, и с нея не се въвеждат нови киберрискове, актуализацията за сигурност не следва да се счита за съществено изменение.*

109. За разлика от това актуализация за сигурност може да се класифицира като съществено изменение, когато, независимо от нейната цел по отношение на сигурността, с нея се променя първоначално предвиденото предназначение на продукта с цифрови елементи или се въвеждат нови или увеличени киберрискове. Такъв може да бъде случаят например, когато с актуализацията съществено се променят границите или структурата на зависимостите на продукта по начин, който не е предвиден в оценката на риска, например чрез съществена промяна на информационните потоци или добавяне на нови външнодостъпни интерфейси.

*Пример 49: производител пуска на пазара софтуерен продукт с цифрови елементи, предназначен за осигуряване на локално криптиране на файлове за данни, които се съхраняват на устройството на ползвателя, чрез който ползвателят може да криптира и декриптира файлове при поискване. След откриването на уязвимост в работния процес на криптиране, производителят внедрява актуализация за сигурност, с която се премахва функцията за локално криптиране и вместо това се изисква всички файлове да бъдат качвани, съхранявани и обработвани чрез услуга за криптиране от разстояние, управлявана от производителя. В резултат на тази промяна продуктът с цифрови елементи вече не функционира като средство за локално криптиране, както е било първоначално предвидено, а вместо това функционира като услуга за криптиране и обработване на данни от разстояние. Въпреки че актуализацията е въведена от съображения за сигурност, с нея фундаментално се променя предназначението на продукта по начин, който не е предвиден в оценката на риска, и следователно се квалифицира като съществено изменение.*

*Пример 50: производител пуска на пазара софтуерен продукт с цифрови елементи, който зависи от установен протокол за криптиране и вътрешно управляван жизнен цикъл на ключовете за обезпечаване на комуникациите между компонентите на продукта с цифрови елементи. В отговор на новоустановени криптографски слабости производителят въвежда актуализация за сигурност, с която заменя съществуващия механизъм за криптиране с друг протокол, чрез който се изисква използването на външна услуга за управление на ключове, управлявана от трета страна. В резултат на тази промяна зависимостите и информационните потоци на продукта с цифрови елементи са съществено променени, като се въвеждат нови външни интерфейси и зависимост от услуги на трети страни, които не са били взети предвид в оценката на риска. Въпреки че актуализацията е насочена към сигурността, с нея се въвеждат нови киберрискове и следователно се квалифицира като съществено изменение.*

110. Както е посочено в точка 104 по-горе, оценката за установяване дали една софтуерна актуализация представлява съществено изменение следва да се извършва за всеки отделен случай. При извършването на тази оценка производителите могат да вземат предвид, по неизчерпателен начин, дали в резултат на софтуерната актуализация:

a) се въвеждат нови вектори на заплаха като допълнителни интерфейси, комуникационни канали, среди за изпълнение или външни зависимости, чрез които заплахите биха могли да се материализират;

b) са възможни нови сценарии на атака, включително например нови начини за осъществяване на непозволен достъп, манипулиране, намеса или неправилна употреба по отношение на продукта с цифрови елементи или във връзка с обработваните от него данни;

c) се променя вероятността от реализиране на вече идентифицираните сценарии на атака — например чрез намаляване на усилията или квалификацията, необходима за тяхното използване, увеличаване на нивото на изложеност на ненадеждни участници или отслабване на съществуващите защитни мерки;

d) се променя потенциалното въздействие на вече идентифицирани сценарии на атака, като например обхватът на засегнатите данни или функции, сериозността на оперативните, свързаните с безопасността или икономическите последици, или способността за откриване, ограничаване или възстановяване след инцидент.

111. В някои случаи със софтуерната актуализация не се въвеждат нови вектори на заплаха или нови сценарии на атака и не се променя съществено вероятността от реализиране на вече идентифицираните сценарии на атака или тяхното въздействие. Това може да означава, че с актуализацията не се въвеждат нови или увеличени киберрискове, при условие че предположенията и мерките за смекчаване, на които се основава оценката на риска, остават валидни и ефективни. Следователно съществува вероятност актуализацията да не се квалифицира като съществено изменение.

112. Обратно, в резултат на софтуерната актуализация може да се въведат нови вектори на заплаха, да са възможни нови сценарии на атака или съществено да се промени вероятността от реализиране на съществуващите сценарии на атака или тяхното въздействие. В такива случаи производителят следва да извърши повторна оценка на киберрисковете, свързани с продукта с цифрови елементи, и да определи дали продължава да е налице съответствие със съществените изисквания, включително дали с актуализацията се въвеждат нови или увеличени рискове, които не са били предвидени в оценката на риска.

113. Квалифицирането на дадена софтуерна актуализация като съществено изменение е от значение при определянето на това дали се прилагат определени задължения по АК, както е посочено в точка 91. Независимо от това квалифициране обаче, производителите продължават да носят отговорност за гарантиране на сигурността на софтуерните актуализации и на своя продукт с цифрови елементи по време на периода на поддръжка в съответствие с изискванията относно отстраняването на уязвимости, определени в приложение I, част II към АК. Освен това, независимо дали софтуерните актуализации се квалифицират като съществени изменения, или не, производителите са задължени да поддържат оценката на риска и техническата документация точни, пълни и постоянно актуализирани в съответствие с член 13, параграф 7 и член 31, параграф 2.

### 4.4. **Последици от съществено изменение**

114. Последиците от съществено изменение, извършено от лице, различно от производителя на даден продукт с цифрови елементи, който вече е пуснат на пазара, са разгледани в членове 21 и 22 от АК. Член 21 се отнася за вносителите и дистрибуторите, а член 22 се отнася за всяко физическо или юридическо лице, различно от производителя, вносителя или дистрибутора.

115. Когато съществената изменение се извършва от първоначалния производител на продукта с цифрови елементи, последиците произтичат от общоприетата концепция за съществено изменение съгласно съображение 41 от АК и са допълнително разяснени в раздел 2.1 от Синьото ръководство. В този раздел се посочва, че продукт, който е претърпял значителни промени или трансформации, след като е пуснат на пазара, трябва да се разглежда като нов продукт, ако първоначалните му работни характеристики, цел или тип са променени, естеството на опасността се е променило или степента на риска се е увеличила и продуктът с цифрови елементи се предоставя на пазара.

116. Следователно общоприетото заключение е, че когато модификация на продукт с цифрови елементи се квалифицира като съществено изменение и модифицираният продукт с цифрови елементи бъде предоставен на пазара, той трябва да се третира като нов продукт с цифрови елементи за целите на АК. В резултат на това предоставянето на съществено изменен продукт на пазара представлява ново пускане на пазара. Това се прилага независимо дали съществената промяна се извършва от първоначалния производител, или от друго лице. С цел гарантиране на прилагането на АК по еднакъв и пропорционален начин за различните категории участници, които може да извършат съществено изменение, в подразделите по-долу са разгледани задълженията, които възникват за лицето, извършващо съществено изменение, при пускането на съответния съществено изменен продукт с цифрови елементи на пазара. Последиците за периода на поддръжка на продукта с цифрови елементи са разгледани в раздел *5. Период на поддръжка*.

4.4.1. *Съществени изменения, които се извършват от лице, различно от първоначалния производител*

117. В съответствие с членове 21 и 22, когато съществено изменение на продукт с цифрови елементи, който вече е пуснат на пазара, се извършва от физическо или юридическо лице, различно от производителя на продукта с цифрови елементи, лицето, което извършва съществената промяна и предоставя изменения продукт с цифрови елементи на пазара, се счита за производител на изменения продукт с цифрови елементи, независимо дали това лице е участвало в първоначалното проектиране или пускане на пазара на този продукт.

118. В член 22 допълнително се пояснява, че задълженията по членове 13 и 14 се прилагат по отношение на лицето, което извършва изменението, само за частта от продукта с цифрови елементи, която е засегната от съществената промяна, ако съществената промяна не оказва въздействие върху киберсигурността на продукта с цифрови елементи като цяло.

119. Когато съществено изменение засяга съответствието със съществените изисквания, но не оказва отрицателно въздействие върху киберсигурността на продукта с цифрови елементи като цяло, по отношение на лицето, което извършва изменението, се прилагат член 13 (включително задължението за гарантиране на съответствието със съществените изисквания и за извършване на процедура за оценяване на съответствието) и член 14 (задължения за докладване) само за частта от продукта с цифрови елементи, която е била съществено изменена ([16]). Освен това задълженията на първоначалния производител съгласно АК продължават да се прилагат за първоначалния продукт с цифрови елементи, пуснат на пазара, като се гарантира приемственост по отношение на отстраняването на уязвимостите и съответствието за непроменените части.

120. Извършването на съществено изменение следва да не се бърка с извършването на интегриране, при което дадено лице сглобява компоненти (включително чрез модифицирането им, когато е целесъобразно) в нов продукт с цифрови елементи, който това лице пуска на пазара. В такива случаи интеграторът не модифицира продукт с цифрови елементи, който вече е пуснат на пазара от друг производител, а пуска на пазара нов продукт с цифрови елементи, който е негова собствена разработка. Интеграторът е производител на този нов продукт с цифрови елементи за целите на АК и е задължен да спазва регламента в неговата цялост по отношение на продукта с цифрови елементи като цяло. Когато производителят интегрира компоненти, които са обект на АК, той може да се позове на свързаните със съответствието дейности на производителите на компонентите, за да улесни гарантирането на съответствието на собствения си продукт с АК.

*Пример 51: дружество закупува готови микроконтролерни модули и компоненти за свързаност от доставчици трети страни, разработва собствено микропрограмно осигуряване и пакет датчици и ги сглобява в свързан продукт с цифрови елементи за мониторинг в сектора на селското стопанство, който пуска на пазара под своето име. Въпреки че дружеството е модифицирало основните микроконтролерни модули и ги е комбинирало с други компоненти, то не извършва съществено изменение на продукт с цифрови елементи, който вече е пуснат на пазара, а пуска на пазара нов продукт с цифрови елементи. Дружеството е производител на този продукт за мониторинг в сектора на селското стопанство за целите на АК и е задължено да спазва регламента по отношение на продукта като цяло.*

([16]) В съответствие с раздел 2.1 от Синьото ръководство „не е необходимо да се повтарят изпитвания и да се изготвя нова документация във връзка с аспекти, които не са засегнати от модификацията. Отговорност на физическото или юридическото лице, което извършва или възлага извършването на промените на продукта, е да докаже, че не всички елементи на техническата документация трябва да бъдат актуализирани. Физическото или юридическото лице, което извършва промените или възлага извършването на промени в продукта, носи отговорност за съответствието на модифицирания продукт и съставя декларация за съответствие дори ако използва съществуващи изпитвания и налична техническа документация“.

121. Когато съществено изменение, извършено от лице, различно от първоначалния производител, оказва отрицателно въздействие върху киберсигурността на продукта с цифрови елементи като цяло, например поради факта, че изменението вече не е насочено или ограничено до конкретен компонент или подсистема, измененият продукт с цифрови елементи, предоставен на пазара, следва да се третира като нов продукт с цифрови елементи, за който се прилага АК в неговата цялост. В такива случаи общият киберрисков профил на този продукт се е променил и изменението не може да бъде оценено, без да се вземе предвид продуктът с цифрови елементи като цяло. Задълженията по членове 13 и 14 се прилагат по отношение на лицето, което извършва изменението, за изменения продукт с цифрови елементи като цяло.

4.4.2. *Съществени изменения, извършени от първоначалния производител*

122. Когато съществената промяна се извършва от първоначалния производител, включително в контекста на повтарящия се процес на разработване на софтуерни продукти с цифрови елементи, този производител продължава да се счита за производител за целите на АК. Съществено измененият продукт с цифрови елементи обаче трябва да се счита за наскоро въведен на пазара.

123. В съответствие с раздел 2.1 от Синьото ръководство първоначалният производител, който пуска съществено изменения продукт с цифрови елементи на пазара, може да използва повторно съществуващата документация и изпитвания за аспектите на продукта с цифрови елементи, които не са засегнати от съществената промяна. По-конкретно, когато производителят пуска на пазара съществено изменени версии на един и същ продукт с цифрови елементи, процедурата за оценяване на съответствието следва да бъде съсредоточена върху съществено изменените части на продукта с цифрови елементи. По същия начин, когато се извършва оценяване на съответствието от трета страна, в оценката си органът за оценяване на съответствието следва да се съсредоточи върху съществено изменените части. За непроменените части на продукта с цифрови елементи той може да използва повторно съществуващата документация и резултати от изпитванията.

124. Изложените в предходния подраздел съображения за пропорционалност се прилагат еднакво за всички съществени изменения, извършени от първоначалния производител на продукт с цифрови елементи, пуснат на пазара преди 11 декември 2027 г. Такова съществено изменение, извършено от първоначалния производител, само по себе си не е основание да се изисква от производителя да приведе целия продукт с цифрови елементи, пуснат на пазара преди тази дата, в пълно съответствие с АК, освен ако изменението не оказва отрицателно въздействие върху киберсигурността на продукта с цифрови елементи като цяло. Когато изменението не оказва отрицателно въздействие върху киберсигурността на продукта с цифрови елементи като цяло, задълженията на първоначалния производител във връзка с изменението следва да бъдат ограничени до съществено изменените части.

## 5. **ПЕРИОД НА ПОДДРЪЖКА**

125. В съответствие с член 13, параграф 8 от АК производителите определят периода на поддръжка, през който уязвимостите на продукта с цифрови елементи, включително неговите компоненти, се отстраняват ефективно и в съответствие със съществените изисквания за киберсигурност, определени в приложение I, част II. Периодът на поддръжка отразява продължителността, през която се очаква продуктът с цифрови елементи да бъде в употреба (очакваното време за използване), и следва да бъде определен, като се вземат предвид критериите по член 13, параграф 8, 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 ([17]). Като цяло тези критерии трябва да се вземат предвид по начин, с който се гарантира пропорционалност при определянето на периода на поддръжка.

([17]) Допълнителните критерии, които могат да се вземат предвид в съответствие с член 13, параграф 8, включват 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 АК, и от Комисията.

126. Съгласно член 13, параграф 8 допълнително се изисква периодът на поддръжка да бъде най-малко пет години, освен ако не се очаква продуктът с цифрови елементи да бъде в употреба по-малко от пет години, в който случай периодът на поддръжка съответства на очаквания период на употреба. Поради това минималният период на поддръжка се прилага само като предпазна мярка, чрез която се гарантира отстраняване на уязвимостите за достатъчно дълъг период и се предоставя възможност на производителите да вземат предвид продукти с цифрови елементи с действително по-кратък очакван период на употреба. В съображение 60 се предоставят повече насоки в това отношение, като се пояснява, че за продуктите с цифрови елементи, за които разумно се очаква да се използват повече от пет години, следва съответно да се гарантират по-дълги периоди на поддръжка. Поради това периодът на поддръжка от пет години не следва да се счита за период на поддръжка по подразбиране за всички продукти с цифрови елементи. Вместо това производителят следва да определи подходящия период на поддръжка въз основа на критериите, посочени в член 13, параграф 8.

127. С член 13, параграф 19 се установява изискването производителите да гарантират, че крайната дата на периода на поддръжка (най-малко месецът и годината) е ясно и разбираемо посочена в момента на покупката. В съответствие с него производителите също трябва да показват нотификация до ползвателите, с която ги информират, че техният продукт с цифрови елементи е достигнал края на своя период на поддръжка, когато това е технически осъществимо с оглед на естеството на продукта с цифрови елементи. Това задължение има за цел да се осигури прозрачност за ползвателите по отношение на продължителността, за която може да се очаква поддръжка на сигурността.

128. По отношение на софтуерни продукти с цифрови елементи, които често се разработват и пускат чрез итерации и при които съществено изменени версии могат да бъдат пускани на пазара често във времето, периодът на поддръжка трябва да се разбира с оглед на този модел на разработване. За всяка съществено изменена версия на софтуерен продукт с цифрови елементи, пусната на пазара, трябва да се посочва период на поддръжка, който е в съответствие с член 13, параграф 8. Това включва минималния период на поддръжка от пет години, освен ако очакваният период на употреба на тази версия не е доказано по-кратък, както е пояснено и в съображение 60. В раздел *5.1 Съществени изменения и период на поддръжка* допълнително се пояснява, че когато със съществената промяна не се променят факторите, въз основа на които е определен първоначално очакваният период на употреба на продукта с цифрови елементи, първоначалният период на поддръжка остава непроменен (т.е. включително в случаите, когато оставащият период на поддръжка е по-малък от пет години).

129. В член 13, параграф 10 се предвижда гъвкавост по отношение на софтуерните продукти с цифрови елементи — производителите могат да гарантират съответствие със изискването за отстраняване на уязвимости, определено в приложение I, част II, точка 2 (справяне с уязвимости и отстраняването им), само за последната пусната на пазара версия на софтуерния продукт с цифрови елементи. Това е разрешено, 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.

130. За целите на член 13, параграф 10 понятието „допълнителни разходи“ следва да се тълкува по практически и пропорционален начин, като се вземат предвид нормалните и очакваните практики при поддръжката и експлоатацията на софтуер. В обхвата му не се включват разумни оперативни усилия, присъщи на прилагането на софтуерни актуализации или поддържането на сигурна оперативна среда, като например време на персонала, рутинно тестване, корекции на конфигурацията или надграждане на базови софтуерни зависимости, които са необходими за справяне с компоненти, които излизат от употреба, или известни свързани със сигурността уязвимости. Понятието „допълнителни разходи“ се отнася до тежести извън обхвата на нормално очакваните в контекста на софтуерните актуализации, като например задължителни покупки на нов хардуер, подмяна на инфраструктура или фундаментални промени в оперативната среда.

131. По отношение на непрекъснато развиващи се софтуерни продукти с цифрови елементи производителите могат да пускат последователни съществено изменени версии на пазара през сравнително кратки интервали и да очакват ползвателите да ги актуализират редовно. В такива случаи обявеният период на поддръжка за всяка съществено изменена версия трябва да бъде в съответствие с член 13, параграф 8 към момента на пускането ѝ на пазара. С други думи, производителят трябва да обяви нов период на поддръжка за тази съществено изменена версия. Производителите обаче могат да се позоват на член 13, параграф 10, за да преустановят справянето с уязвимости и тяхното отстраняване за по-стари версии, след като ползвателите могат да надстроят до по-нова версия безплатно и

без допълнителни разходи, както е посочено по-горе, дори ако резултатът от това е по-кратък ефективен период на поддръжка за тези по-стари версии ([18]). По отношение на производителя продължават да се прилагат другите изисквания относно отстраняването на уязвимости съгласно Приложение I, част II и задълженията за докладване съгласно член 14. Както е обяснено и в съображение 40, тези изисквания включват, наред с другото, следното по отношение на всички последващи съществено изменени версии на софтуерния продукт с цифрови елементи, пуснати на пазара: i) въвеждане и прилагане на политика относно координирано оповестяване на уязвимости; и ii) мерки за улесняване на споделянето на информация относно потенциални уязвимости ([19]).

*Пример 52: производител пуска модел смартфон на пазара на ЕС и обявява период на поддръжка от X години от датата на пускане на пазара, през който ще предоставя актуализации за сигурност с цел справяне с уязвимости. През този период производителят пуска редовни софтуерни актуализации и съществено изменени версии на операционната система, които ползвателите могат да инсталират безплатно, без да е необходим нов хардуер.*

*Производителят може, в съответствие с член 13, параграф 10, да се справя с уязвимостите и да ги отстранява за най-новата версия на операционната система, предоставена за този модел смартфон, при условие че по-старите версии могат да бъдат надстроени безплатно и без допълнителни разходи. За срока на периода на поддръжка, по отношение на производителя продължават да се прилагат другите изисквания относно отстраняването на уязвимости, като например координирано оповестяване на уязвимости и мерки за споделяне на информация.*

*Пример 53: производител пуска на пазара корпоративен софтуерен продукт с цифрови елементи и пуска съществено изменени версии на всеки няколко месеца, с които се отразяват подобрения в сигурността, нови функции и съвместимост с актуализирани операционни системи и платформи. Всяка версия се пуска на пазара с обявен период на поддръжка в съответствие с член 13, параграф 8. Производителят очаква ползвателите редовно да извършват надстройване като част от нормалната експлоатация и безплатно предоставя достъп до най-новата версия. За извършването на надграждане може да са необходими разумни оперативни усилия, като тестване или корекции на конфигурацията, но не се изискват допълнителни разходи, като например закупуване на нов хардуер или фундаментални промени в инфраструктурата. В този контекст производителят може да се позове на член 13, параграф 10, за да преустанови справянето с уязвимости и тяхното отстраняване за по-стари версии, след като ползвателите могат да надстроят до най-новата версия, като същевременно продължава да спазва другите изисквания относно отстраняването на уязвимости за всички последващи съществено изменени версии.*

### 5.1. **Съществени изменения и период на поддръжка**

132. Както е посочено в раздел *4.4 Последици от съществено изменение,* когато модификация на продукт с цифрови елементи се квалифицира като съществено изменение и модифицираният продукт с цифрови елементи бъде предоставен на пазара, той трябва да се третира като нов продукт с цифрови елементи за целите на АК, а предоставянето на съществено изменения продукт с цифрови елементи на пазара представлява ново пускане на пазара. Поради това е удачно да се поясни въздействието на новото пускане на пазара върху периода на поддръжка на съществено изменения продукт с цифрови елементи.

133. Периодът на поддръжка на съществено изменен продукт с цифрови елементи следва да се определя съобразно очакваното време за използване на този продукт въз основа на критериите, посочени в член 13, параграф 8 от АК. Поради това дадено съществено изменение следва да подлежи на повторна оценка спрямо тези критерии, като това не е основание за автоматично повторно определяне на периода на поддръжка или дори удължаването му. Уместният въпрос е дали съществената промяна засяга факторите, въз основа на които е определено първоначалното очаквано време за използване на този продукт и съответно първоначалният период на поддръжка.

([18]) Следва да се припомни, че с член 13, параграф 19 се установява изискването производителите, когато това е технически осъществимо с оглед на естеството на продукта с цифрови елементи, да показват нотификация до ползвателите, с която ги информират, че техният продукт с цифрови елементи е достигнал края на своя период на поддръжка. Поради това, когато справянето с уязвимости и тяхното отстраняване за по-стари версии се преустановяват, се очаква ползвателите, които не са надстроили до най-новата версия, да бъдат информирани, ако това е технически осъществимо.

([19]) Следва да се отбележи, че когато ползвателите могат да надстроят до най-новата версия на софтуера без допълнителни разходи, производителите могат да изберат да продължат да се справят с уязвимостите и да ги отстраняват в по-стари версии на този софтуер, включително срещу заплащане или съгласно други търговски договорености. АК не изисква от производителите безплатно да предоставят актуализации във връзка със сигурността за такива по-стари версии.

134. Когато съществено изменение не засяга тези фактори, първоначалното очаквано време за използване, определено въз основа на посочените в член 13, параграф 8 критерии, остава непроменено, а периодът на поддръжка на модифицирания продукт с цифрови елементи следва да съответства на оставащото очаквано време за използване на продукта, както е първоначално пуснат на пазара. Това обикновено е случаят, когато очакваното време за използване е определено, в значителна степен, въз основа на оставащи непроменени в резултат на модификацията фактори, като например физическата дълготрайност на хардуерните компоненти, когато съществено изменение засяга единствено софтуерната функционалност или сървърните (бекенд) услуги.

*Пример 54: производител пуска на пазара прахосмукачка робот с очаквано време за използване от X години, определено въз основа на естеството на продукта с цифрови елементи, включително физическата дълготрайност и характеристиките на износване на хардуерните компоненти, и предвид разумните очаквания на ползвателите относно жизнения цикъл на този продукт. Производителят определя период на поддръжка от X години. След Y години производителят пуска квалифицираща се като съществено изменение софтуерна актуализация, с която се добавят нови режими на почистване и функции за навигация. Със софтуерната актуализация не се засяга физическата дълготрайност на хардуера и не се променят разумните очаквания на ползвателите относно жизнения цикъл на този продукт. Поради това очакваното време за използване въз основа на критериите, посочени в член 13, параграф 8, остава непроменено. Периодът на поддръжка на модифицирания продукт с цифрови елементи съответства на оставащото очаквано време за използване, както е първоначално определено.*

*Пример 55: производител пуска на пазара предназначен за промишления сектор сложен машиностроителен продукт с цифрови елементи със сървърна система в изчислителен облак, който представлява решение за обработване на данни от разстояние. Очакваното време за използване е X години, определено въз основа на разумните очаквания на ползвателите и естеството на продукта с цифрови елементи, като например физическата дълготрайност на хардуера на машината и очакваното износване. Периодът на поддръжка е определен в съответствие с това очаквано време за използване от X години. След Y години производителят преработва сървърната система в изчислителен облак (решението за обработване на данни от разстояние), в резултат на което се въвеждат нови API и информационни потоци по начин, който се квалифицира като съществено изменение на продукта с цифрови елементи, но не се променя естеството на този продукт и не се засягат очакванията на ползвателите. Поради това очакваното време за използване въз основа на критериите, посочени в член 13, параграф 8, остава непроменено. Периодът на поддръжка на модифицирания продукт с цифрови елементи съответства на оставащото очаквано време за използване, както е първоначално определено.*

135. Когато съществено изменение засяга факторите, въз основа на които е определено първоначалното очаквано време за използване на продукта с цифрови елементи, производителят следва да преизчисли периода на поддръжка, за да отрази новото очаквано време за използване чрез съответно прилагане на критериите, посочени в член 13, параграф 8. Такъв може да бъде случаят, когато се извършват модификации с цел хардуерно обновяване, чрез които се удължава експлоатационният живот на продукт, или съществено се препрограмира или пренаписва основния софтуер на продукта, чрез което съществено се променя очакваното време за използването му ([20]).

*Пример 56: производител пуска на пазара програмируем логически контролер (PLC) с очаквано време за използване от X години, определено основно въз основа на естеството на продукта с цифрови елементи и дълготрайността на базовия хардуер. Периодът на поддръжка се определя съответно. Няколко години след първоначалното пускане на пазара производителят извършва съществено изменение, като заменя вградената изчислителна платформа на PLC, включително процесора, палетата и средата за изпълнение, с компоненти от ново поколение, проектирани за значително по-дълъг жизнен цикъл. В резултат на изменението разумните очаквания на ползвателите и естеството на продукта с цифрови елементи се променят: ползвателят на PLC вече може разумно да очаква, че с осигурената чрез новата изчислителна платформа поддръжка PLC ще остане в продуктивна употреба след първоначално обявеното очаквано време за използване. Поради това очакваното време за използване въз основа на критериите по член 13, параграф 8 е по-дълго и производителят преизчислява периода на поддръжка за този конкретен PLC съответно.*

## 6. **ВАЖНИ И КРИТИЧНИ ПРОДУКТИ С ЦИФРОВИ ЕЛЕМЕНТИ**

136. В съответствие с член 7, параграф 1 от АК продуктите с цифрови елементи, които имат основната функционална възможност на дадена продуктова категория, определена в приложение III от регламента, се считат за „важни продукти с цифрови елементи“. В приложение III важните продукти с цифрови елементи допълнително се разделят на клас I и клас II. По подобен начин член 8, параграф 1 установява, че продуктите с цифрови елементи, които имат основната функционална възможност на дадена продуктова категория, определена в приложение IV към АК, се считат за „критични продукти с цифрови елементи“ ([21]).

([20]) Следва да се припомни, че както е посочено в раздел *4.1 Физически ремонти,* операциите по обновяване, поддръжка или ремонт обикновено не се считат за съществени изменения.

([21]) Регламент за изпълнение (ЕС) 2025/2392 определя техническото описание на категориите важни и критични продукти.

137. Класифицирането на продукт с цифрови елементи като важен или критичен или, обратно, като принадлежащ към категорията „по подразбиране“ ([22]) е от значение при определянето на процедурата за оценяване на съответствието, която производителят трябва да следва в съответствие с член 32, преди да може да пусне този продукт с цифрови елементи на пазара. По-специално, по отношение на продуктите с цифрови елементи в категорията по подразбиране винаги може да се приложи процедурата за вътрешен контрол въз основа на модул А („самооценка“) ([23]). Важните продукти с цифрови елементи от клас I или II и критичните продукти с цифрови елементи подлежат на по-строги процедури за оценяване на съответствието. Това не включва важни продукти с цифрови елементи от клас I или II, които се квалифицират като свободен софтуер с отворен код, пуснат на пазара, за които производителите могат да следват приложимите за категорията по подразбиране процедури в съответствие с член 32, параграф 5.

138. Поради това концепцията за основна функционална възможност е от съществено значение за производителя при определянето на приложимата процедура за оценяване на съответствието. Тази концепция обаче не е изрично дефинирана в АК. Продуктите с цифрови елементи могат да изпълняват редица функции, някои от които могат да бъдат спомагателни спрямо основната функционална възможност на този продукт и не следва да са от значение за класифицирането на продукта като продукт по подразбиране, важен продукт от клас I, важен продукт от клас II или критичен продукт. Поради това е удачно да се предоставят повече насоки за подпомагане на производителите при извършването на съответните процедури за оценяване на съответствието по правилен начин и за подпомагане на органите за надзор на пазара при осигуряването на хармонизирано прилагане на АК в целия ЕС.

### 6.1. **Основна функционална възможност**

139. Основната функционална възможност на даден продукт с цифрови елементи се отнася до основните характеристики и технически възможности на този продукт, без които предназначението му не може да бъде изпълнявано. Тя може да бъде оценена с оглед на специфичния контекст и условията на употреба на този продукт, като се вземе предвид, наред с другото, предоставената от производителя информация в инструкциите за употреба, рекламните или търговските материали и изявления, както и в техническата документация.

*Пример 57: софтуерен продукт с цифрови елементи осигурява слой за абстракция над базовия хардуер и управлява изпълнението на софтуерни компоненти. Основните му характеристики включват инициализация на хардуера и периферните устройства, управление на процесите и паметта, контрол на входа и изхода, планиране, разпределение на ресурсите и предоставяне на системни услуги и приложно-програмни интерфейси (API), чрез които приложенията взаимодействат с хардуерните и софтуерните ресурси на устройството. В техническата документация се посочва, че продуктът с цифрови елементи оркестрира изчислителни ресурси, прилага системни конфигурации и предоставя стандартизирани интерфейси за софтуерни модули и свързани периферни устройства. Производителят подчертава, че чрез тези възможности платформата функционира като централна софтуерна среда, в която приложенията могат надеждно да работят. Продуктът с цифрови елементи има основната функционална възможност на операционна система, както е описано в приложение I, точка 11 към Регламент за изпълнение (ЕС) 2025/2392.*

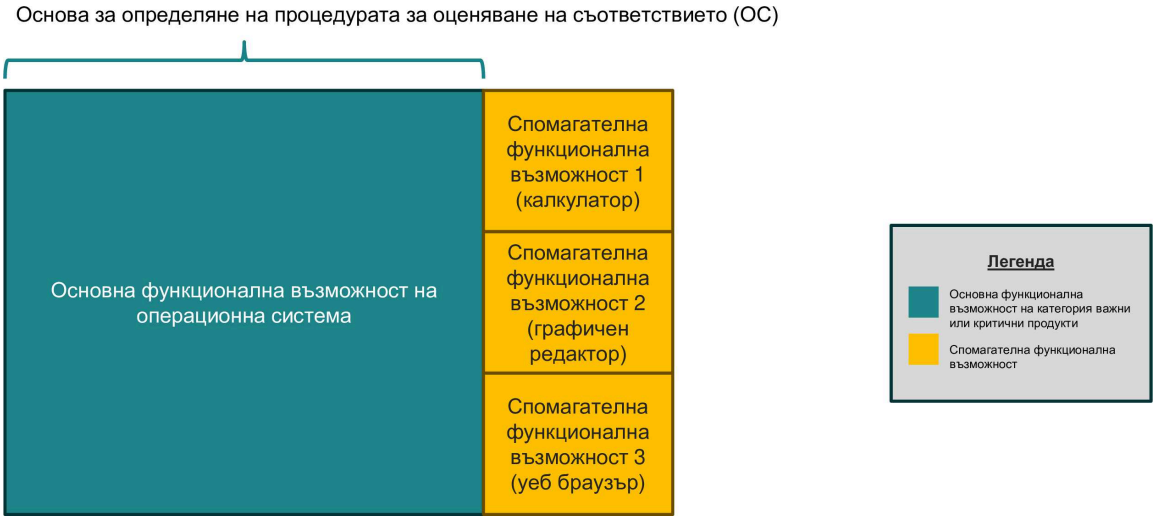
140. Функционалността на даден продукт с цифрови елементи рядко е ограничена изключително до неговата основна функционална възможност, тъй като продуктите с цифрови елементи често, ако не винаги, изпълняват допълнителни функции, които не допринасят за основната функционална възможност на продукта. Това може също да включва компоненти, които сами по себе си имат функционалната възможност на друг важен или критичен продукт с цифрови елементи. Самият факт, че продукт с цифрови елементи изпълнява функции, различни от посочените в техническото описание на важни или критични продукти с цифрови елементи или допълващи ги, обаче не означава, че продуктът не може да има такава основна функционална възможност.

([22]) Понятието „по подразбиране“ не е дефинирано в АК. Използването на понятието в настоящия документ се отнася до продукти с цифрови елементи, които нямат основната функционална възможност на дадена продуктова категория, определена в приложение III или IV към АК, и които съответно подлежат на процедурата за оценяване на съответствието, посочена в член 32, параграф 1.

([23]) Въпреки това производителят винаги може да избере да приложи по-строга процедура за оценяване на съответствието, както е предвидено в член 32, параграф 1.

*Фигура 2*

**Илюстрация на начина, по който приложимата процедура за оценяване на съответствието се определя въз основа на основната функционална възможност, а не въз основа на спомагателните функционални възможности**




141. Възможно е даден продукт с цифрови елементи да може да изпълнява функциите на важна или критична продуктова категория, но въпреки това да има основна функционална възможност, различна от тази на съответната продуктова категория. В тези случаи този продукт с цифрови елементи не се квалифицира като важен или критичен продукт с цифрови елементи. Както изрично е посочено в член 7, параграф 1 от АК, по отношение на важни продукти с цифрови елементи (и прилагайки същата логика за критични продукти с цифрови елементи) самото интегриране на важен или критичен продукт с цифрови елементи не е основание продуктът с цифрови елементи да се счита за важен или критичен продукт с цифрови елементи.

*Пример 58: смартфон интегрира операционна система, която предоставя функционалните възможности, описани в приложение I, точка 11 към Регламент за изпълнение (ЕС) 2025/2392. Докато с операционната система се позволява управлението на хардуерни ресурси и изпълнението на софтуерни приложения, смартфонът като цяло има различна основна функционална възможност (напр. възможност ползвателите да комуникират и да имат достъп до информация и услуги). Самото интегриране на операционна система не означава, че смартфонът има основната функционална възможност на операционна система.*

142. Някои продукти с цифрови елементи могат да бъдат подобни на принадлежащи към дадена категория важни или критични продукти или да принадлежат към едно общо семейство продукти, но да имат основна функционална възможност, чийто обхват е значително по-голям или по-малък от този на основната функционална възможност на съответната категория. Това не е така, когато продукт с цифрови елементи има допълнителни функционални възможности, които само допълват или подобряват основната функционална възможност, която сама по себе си съответства на тази на дадена категория важни или критични продукти; в такива случаи продуктът с цифрови елементи запазва основната функционална възможност на тази категория и се класифицира съответно. Тази оценка следва да се основава на основните характеристики и технически възможности на този продукт, разгледани обективно с оглед на предназначението му, а не на начина, по който продуктът с цифрови елементи е описан или предлаган на пазара, когато в това описание не са отразени действителните технически характеристики на продукта.

*Пример 59: софтуерът за оркестрация, автоматизация и реакция в областта на сигурността (SOAR) често има способността да изпълнява функциите на продукти с цифрови елементи от категорията „системи за управление на информацията за безопасност и на събитията, свързани със сигурността (SIEM)“, т.е. да събира данни от множество източници и да ги анализира и съотнася, както и да представя тези данни като полезна информация за целите на сигурността. Обхватът на основната функционална възможност на софтуера обаче е значително по-голям от определения за тази на SIEM, включително услуги като реакция при инциденти като основни елементи на неговите технически възможности. Поради това обикновено не се счита, че SOAR има основната функционална възможност на SIEM.*

*Фигура 3*

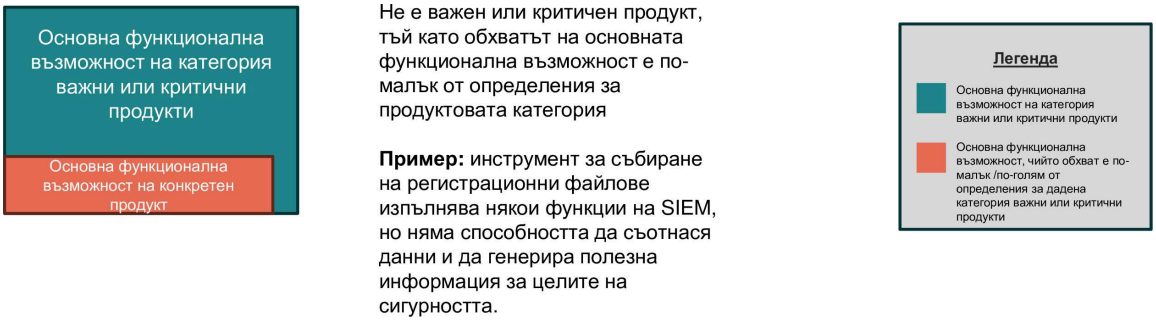
**Илюстрация на основната функционална възможност на продукт с цифрови елементи, чийто обхват е значително по-голям от определения за дадена категория важни или критични продукти**




*Пример 60: някои инструменти за събиране и визуализация на регистрационни файлове имат способността да приемат регистрационни данни и да представят основни табла за показване на системни събития. Въпреки че тези инструменти могат да поддържат дейности по мониторинг на сигурността, обхватът на тяхната основна функционалност е значително по-малък от определения за тази на SIEM, тъй като те не извършват съотнасяне на данни и не предоставят полезна информация относно сигурността. Поради това обикновено трябва да се счита, че такива инструменти нямат основната функционалност на SIEM.*

*Фигура 4*

**Илюстрация на основната функционалност на продукт с цифрови елементи, чийто обхват е значително по-малък от определения за дадена категория важни или критични продукти**

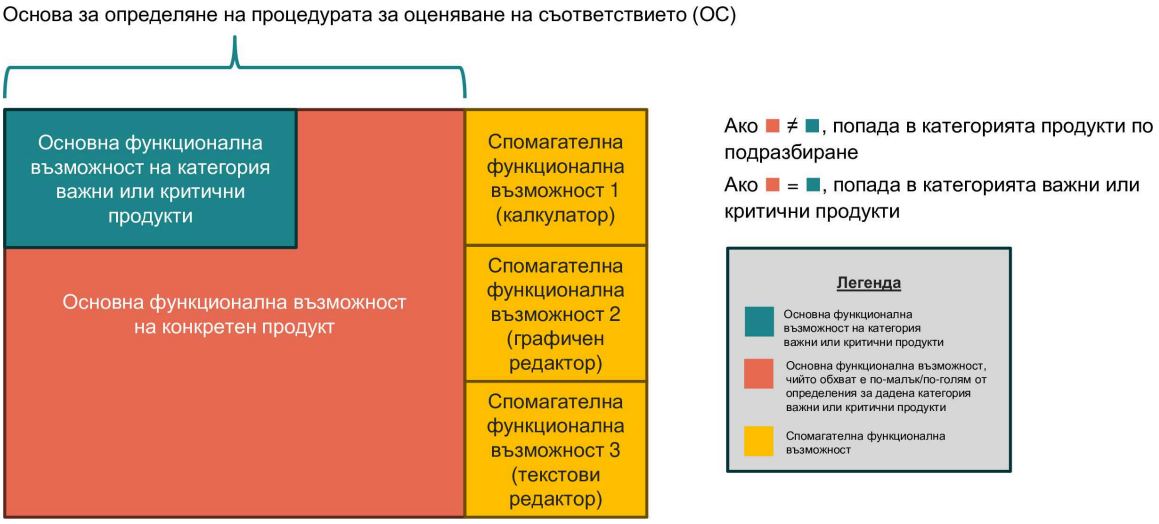



143. Производителят не може да представя погрешно основната функционалност на своя продукт с цифрови елементи с цел избягване на процедурата за оценяване на съответствието, приложима за важни или критични продукти с цифрови елементи, напр. чрез прекомерно подчертаване или омаловажаване на ролята на определени функционалности, в резултат на което свързаният с продукта обхват на дадена основна функционалност е значително по-голям или по-малък. Такъв би бил случаят, когато са налице явни несъответствия между рекламните материали, инструкциите за употреба и техническата документация.

144. Даден продукт с цифрови елементи не може да има повече от една основна функционалност за целите на определянето на приложимата процедура за оценяване на съответствието. В съответствие с приложение VII към АК, като част от техническата документация на продукта, производителите са задължени да опишат предназначението на своя продукт с цифрови елементи и процедурата за оценяване на съответствието, която са следвали. Поради това основната функционалност следва да бъде ясно идентифицирана. Това позволява правилното идентифициране на приложимата процедура за оценяване на съответствието и предоставя възможност на органите за надзор на пазара да контролират и проверяват правилното прилагане на регламента.

*Фигура 5*

**Илюстрация на начина, по който продуктовият клас и съответно приложимата процедура за оценяване на съответствието се определят въз основа на основната функционалност на конкретен продукт с цифрови елементи**




145. Някои продукти с цифрови елементи се пускат на пазара като единични продукти с цифрови елементи, но се състоят от отделни модули с различни функции. Когато даден производител също така предоставя тези модули на пазара поотделно, като например чрез предлагане за отделно закупуване, лицензиране или абонамент, тези модули сами по себе си представляват самостоятелни продукти с цифрови елементи. Като такива, те трябва да бъдат класифицирани въз основа на съответните им основни функционални възможности (и следователно да подлежат на подходящата процедура за оценяване на съответствието въз основа на основната функционална възможност на всеки модул). Това не засяга модулите, които се доставят единствено като компоненти на интегриран продукт с цифрови елементи и не се предоставят поотделно; в такива случаи основната функционална възможност се определя на нивото на интегрирания продукт с цифрови елементи.

*Пример 61: производител пуска на пазара унифициран пакет за сигурност, комбиниращ множество модули, включително SIEM, алармена система против проникване и модул за анализи. Производителят предлага тези модули и чрез отделни абонаменти. В този сценарий всеки модул е отделен продукт с цифрови елементи и се класифицира въз основа на собствената си основна функционална възможност. Модулът SIEM подлежи на процедурата за оценяване на съответствието, приложима за важни продукти с цифрови елементи от клас I, тъй като неговата основна функционална възможност е тази на „системи за управление на информацията за безопасност и на събитията, свързани със сигурността (SIEM)“. Алармената система против проникване подлежи на процедурата за оценяване на съответствието, приложима за важни продукти с цифрови елементи от клас II, тъй като нейната основна функционална възможност е тази на „защитни стени, системи за установяване и/или предотвратяване на проникване“. Модулът за анализи подлежи на процедурата за оценяване на съответствието, приложима за продукти с цифрови елементи по подразбиране, тъй като той няма основната функционална възможност на дадена категория важни или критични продукти.*

146. Неспазването на задълженията, предвидени в член 32 от АК, може да е основание за административни глоби в съответствие с член 64, параграф 3.

### 6.2. Оценяване на съответствието за важни и критични продукти с цифрови елементи

147. След като производителят е определил основната функционална възможност на своя продукт с цифрови елементи, той трябва да извърши една от приложимите процедури за оценяване на съответствието. Производителят трябва да гарантира, че продуктът с цифрови елементи като цяло отговаря на съществените изисквания, като вземе предвид, както е целесъобразно, сигурността на компонентите или интегрираните в него функционалности.

148. За важни продукти с цифрови елементи от клас II (с изключение на тези, които се квалифицират като свободен софтуер с отворен код в съответствие с член 32, параграф 5) и за критични продукти с цифрови елементи задължително се прилага по-строга процедура за оценяване на съответствието с участието на трета страна (въз основа на модул B+C, модул H или схеми за сертифициране на киберсигурността) ([24]). За разлика от тях важните продукти с цифрови елементи от клас I (с изключение на тези, които се квалифицират като свободен софтуер с отворен код в съответствие с член 32, параграф 5) подлежат на процедура за оценяване на съответствието от трета страна само ако производителят не е приложил или е приложил само частично съответните хармонизирани стандарти, данните за които са публикувани в *Официален вестник на Европейския съюз* (наричани по-долу „хармонизираните стандарти“), общи спецификации или европейски схеми за сертифициране на киберсигурността поне с ниво на увереност „съществено“ ([25]).

149. Поради това, за да отговаря даден продукт с цифрови елементи от клас I на условията за процедурата за вътрешен контрол, i) трябва да бъдат приложени всички приложими изисквания на съответния хармонизиран стандарт; и ii) в обхвата на стандарта трябва да са включени поне всички киберрискове, свързани с основната функционална възможност на този продукт.

150. Обхватът на продукта с цифрови елементи може да бъде по-широк от обхвата, предвиден в съответния хармонизиран стандарт, и такива допълнителни функции могат да представляват различни или допълнителни киберрискове. Производителят винаги е задължен да извършва оценка на риска съгласно член 13, параграф 2 и впоследствие следва да проверява дали с прилагането на хармонизиран стандарт се обхващат всички рискове, свързани с продукта с цифрови елементи. Когато с прилагането на хармонизиран стандарт не се обхващат всички рискове, производителят следва да гарантира чрез други средства, че неговият продукт с цифрови елементи е в съответствие със съществените изисквания.

151. Поради това, ако производителят на важен продукт с цифрови елементи от клас I е приложил съответен хармонизиран стандарт, чийто обхват включва рисковете, свързани с основната функционална възможност на този продукт, той може да реши да използва процедурата за вътрешен контрол, за да докаже съответствието на своя продукт. Като част от своите дейности по оценяване на съответствието, производителят остава задължен да докаже, че са разгледани всички съответни рискове, свързани с неговия продукт с цифрови елементи. Следователно, когато има разлика между обхвата на хармонизирания стандарт и обхвата на продукта с цифрови елементи като цяло, производителят остава задължен да документира въведените от него допълнителни мерки за справяне с тези рискове.

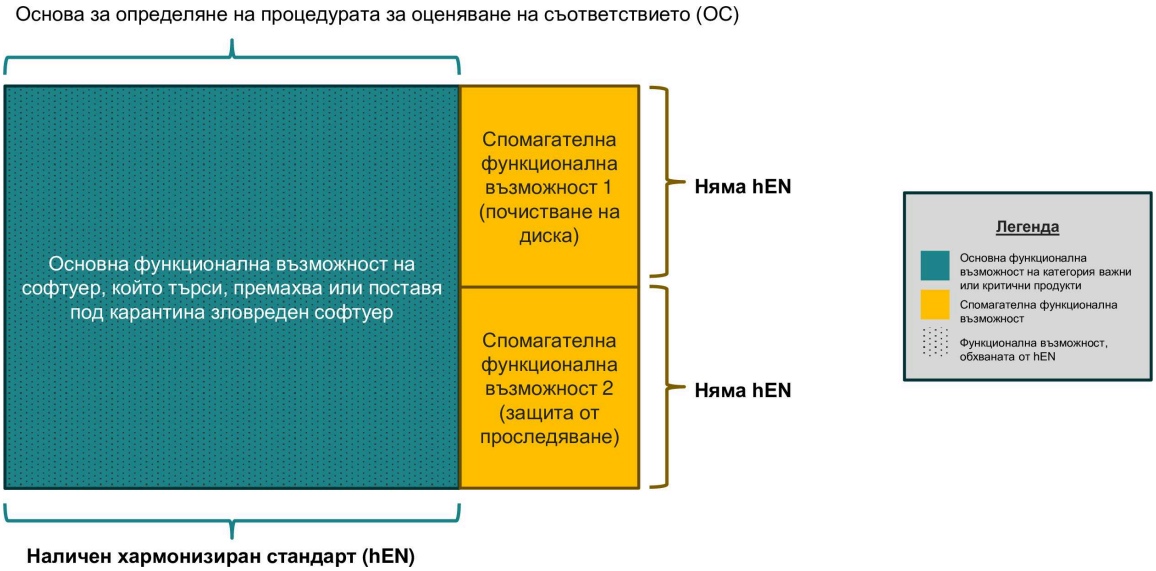
*Пример 62: антивирусен софтуер има основната функционална възможност на софтуер, който търси, премахва или поставя под карантина зловреден софтуер, както е описано в приложение I, точка 4 към Регламент за изпълнение (ЕС) 2025/2392. Този продукт с цифрови елементи включва и допълнителни функции, а именно функция за почистване на диска и функция за защита от проследяване, предпазваща ползвателя при навигация в мрежата. Производителят извършва оценка на риска, в чийто обхват е включен продуктът с цифрови елементи в неговата цялост, включително основната функционална възможност на антивирусния софтуер и функциите за почистване на диска и за защита от проследяване. Той прилага хармонизиран стандарт, в чийто обхват са включени рисковете, свързани с основната функционална възможност на антивирусния софтуер, и допълнителни мерки за справяне с рисковете, произтичащи от допълнителните функции. Производителят може да използва процедурата за вътрешен контрол за оценяване на съответствието по отношение на продукта с цифрови елементи като цяло, включително функциите за почистване на диска и за защита от проследяване.*

([24]) Такъв е и случаят, когато се прилага европейска схема за сертифициране на киберсигурността поне с ниво на увереност „съществено“, тъй като се изисква участието на орган за сертифициране трета страна.

([25]) За краткост, в останалата част от настоящия раздел се прави позоваване само на хармонизирани стандарти, данните за които са публикувани в *Официален вестник на Европейския съюз*. Въпреки това същите насоки се прилагат и за общите спецификации, приети в съответствие с член 27, параграф 2, и за европейските схеми за сертифициране на киберсигурността, когато това е посочено от Комисията чрез делегирани актове в съответствие с член 27, параграф 9.

*Фигура 6*

**Илюстрация на начина, по който приложимата процедура за оценяване на съответствието се определя от хармонизиран стандарт, в чийто обхват е включена само основната функционална възможност**




152. Такъв е и случаят, когато продуктът с цифрови елементи интегрира допълнителна функция, която сама по себе си е функционалност на друг важен или критичен продукт с цифрови елементи. Всъщност именно основната функционална възможност на продукта с цифрови елементи като цяло, а не функционалността на интегрираните компоненти, взети предвид поотделно, се използва при определянето на продукта с цифрови елементи като принадлежащ към категорията важни или критични продукти (и следователно на приложимата процедура за оценяване на съответствието). Ако например даден продукт с цифрови елементи има основната функционална възможност на важен продукт с цифрови елементи от клас I, този продукт като цяло подлежи на процедурата за оценяване на съответствието, приложима за важни продукти с цифрови елементи от клас I, дори ако интегрира компонент, който сам по себе си е критичен продукт с цифрови елементи. В тези случаи производителят може да използва процедурата за вътрешен контрол, ако прилага хармонизиран стандарт, в чийто обхват са включени рисковете, свързани с основната функционална възможност на този продукт.

*Пример 63: хардуерен продукт с цифрови елементи има основната функционална възможност на маршрутизатор, както е описано в приложение I, точка 12 към Регламент за изпълнение (ЕС) 2025/2392. Този продукт с цифрови елементи има и допълнителни функции, включително функционални възможности на защитна стена, тъй като интегрира компонент на защитна стена. Производителят извършва оценка на риска, в чийто обхват е включен продуктът с цифрови елементи в неговата цялост, включително основната функционална възможност на маршрутизатора и функционалността на защитна стена. Той прилага хармонизиран стандарт, в чийто обхват са включени рисковете, свързани с основната функционална възможност на маршрутизатор, и допълнителни мерки за справяне с рисковете, произтичащи от допълнителните функции. Например производителят може да приложи хармонизирания стандарт за защитни стени, за да покрие рисковете, свързани с функционалността на защитна стена. Производителят може да използва процедурата за вътрешен контрол за оценяване на съответствието по отношение на продукта с цифрови елементи като цяло, включително функционалността на защитна стена.*

### 6.3. Последствия за презумпцията за съответствие

153. Съгласно член 27, параграф 1 от АК, за продуктите с цифрови елементи и процесите, въведени от производителя, които съответстват на хармонизираните стандарти или на части от тях, данните за които са публикувани в *Официален вестник на Европейския съюз (ОВ на ЕС)*, се приема, че съответстват на съществените изисквания за киберсигурност, определени в приложение I, обхванати от тези стандарти или части от тях ([26]). С член 27,

([26]) Както е ясно посочено в раздел 4.1.2.2 от Синьото ръководство, „в законодателството за хармонизация, свързано с рисковете, [...], дори и при използване на хармонизирани стандарти, чиито данни са публикувани в *Официален вестник на Европейския съюз*, производителите носят пълната отговорност за оценяване на всички рискове на продукта си, за да установят кои съществени (или други) изисквания са приложими. След тази оценка производителят може да реши да приложи технически спецификации, дадени в хармонизирани стандарти, чиито данни са публикувани в *Официален вестник на Европейския съюз*, за да изпълни „мерките за намаляване на рисковете“, които са определени от хармонизираните стандарти“.

параграф 5 се разширява обхватът на тази презумпция за съответствие чрез включване на продуктите с цифрови елементи и процесите, въведени от производителя, които са в съответствие с общите спецификации, установени от Комисията с актове за изпълнение, а в член 27, параграф 8 се установява презумпция за съответствие за продуктите с цифрови елементи и процесите, въведени от производителя, за които е издадена ЕС декларация за съответствие или сертификат по европейска схема за сертифициране на киберсигурността, приета съгласно Регламент (ЕС) 2019/881, ако това е определено чрез делегирани актове в съответствие с член 27, параграф 9 ([27]).

154. Следователно, когато производителят е приложил хармонизиран стандарт, данните за които са публикувани в ОВ на ЕС, той се ползва от презумпцията за съответствие за рисковете, обхванати от този стандарт. Такъв би могъл да бъде случаят, когато например хармонизираният стандарт обхваща всички рискове, свързани с основната функционална възможност на даден продукт с цифрови елементи, и няма допълнителни функционалности, които представляват киберрискове. Очаква се например хармонизираният стандарт за маршрутизатори да обхваща поне рисковете, свързани с основната функционална възможност на тези продукти с цифрови елементи. Ако такъв продукт няма допълнителни функционалности или ако тези допълнителни функционалности не представляват рискове, които не са обхванати от стандарта, продуктът с цифрови елементи може да се ползва с презумпция за съответствие.

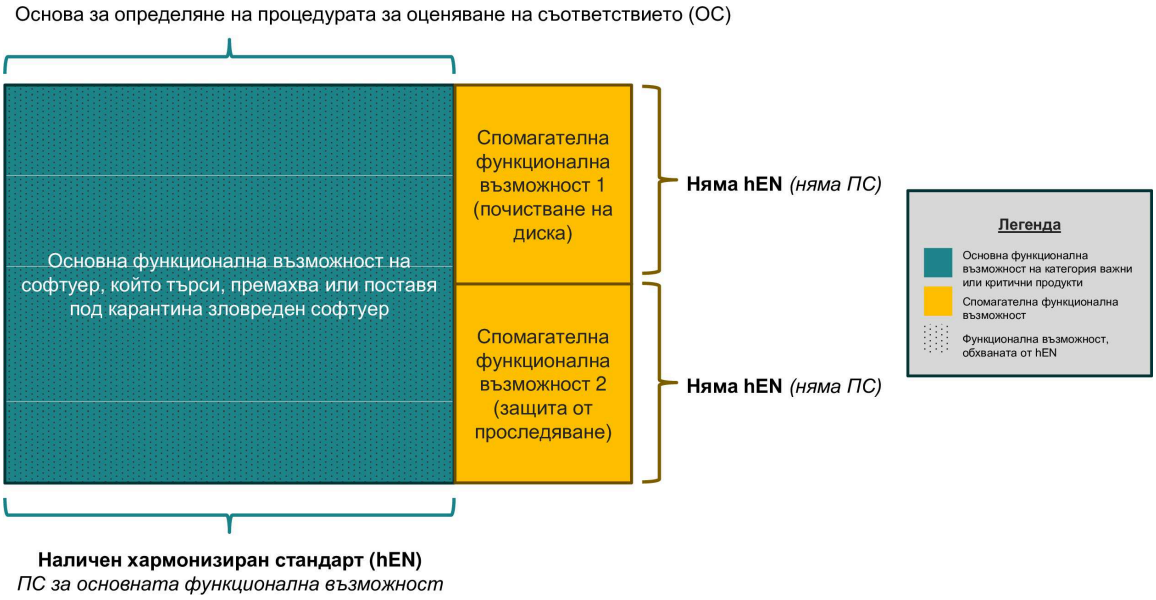
155. В случаите, разгледани в точки 151 и 152, производителят може да използва процедурата за вътрешен контрол, тъй като хармонизираният стандарт обхваща рисковете, свързани с основната функционална възможност на продукта с цифрови елементи. Обхватът на описаните в тези примери продукти с цифрови елементи обаче може да е по-голям от този на хармонизираните стандарти и допълнителните функционалности могат да представляват киберрискове, които не са обхванати от съответния хармонизиран стандарт. Поради това тези продукти с цифрови елементи не може да се ползват с презумпция за съответствие за тези допълнителни функционалности.

*Пример 64: антивирусен софтуер има основната функционална възможност на софтуер, който търси, премахва или поставя под карантина зловреден софтуер, а свързаните с тази основна функционална възможност рискове са обхванати от хармонизирания стандарт. Този продукт с цифрови елементи също има допълнителни функционалности, а именно функция за почистване на диска и функция за защита от проследяване, предпазваща ползвателя при навигация в мрежата, чиито рискове не са обхванати от хармонизирания стандарт. Ако се прилага хармонизираният стандарт, производителят може да използва процедурата за вътрешен контрол за оценяване на съответствието. Той ще се ползва от презумпцията за съответствие за рисковете, свързани с основната функционална възможност на този продукт, но не и за свързаните с допълнителните функционалности рискове.*

([27]) Както е посочено по-горе, за краткост, в останалата част от настоящия раздел се прави позоваване само на хармонизирани стандарти, чиито данни са публикувани в *Официален вестник на Европейския съюз*. Същите насоки обаче също се прилагат за общите спецификации и за европейските схеми за сертифициране на киберсигурността.

*Фигура 7*

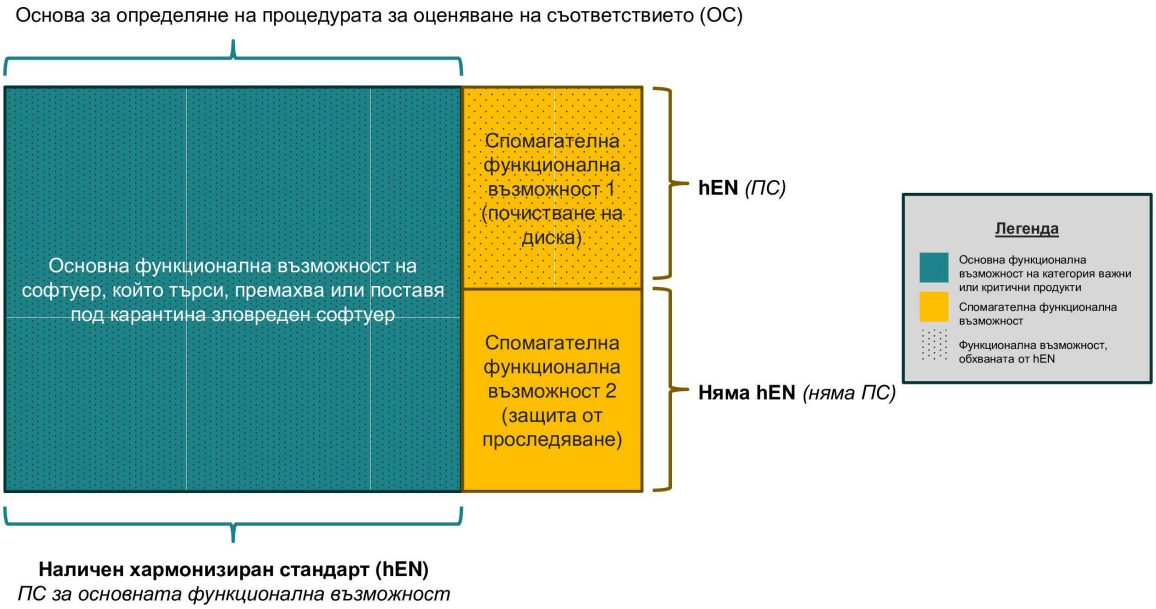
**Хармонизираният стандарт предоставя презумпция за съответствие (ПС) за основната функционална възможност, тъй като обхваща всички рискове, свързани с тази основна функционална възможност, но не и за спомагателните функционални възможности**




*Пример 65: в сценария, изложен в предходния пример, хармонизираният стандарт вече е актуализиран, за да обхване и рисковете, свързани с една от допълнителните функционалности, а именно функцията за почистване на диска, но не и другата (т.е. функцията за защита от проследяване). Ако се прилага хармонизираният стандарт, производителят може да използва процедурата за вътрешен контрол за оценяване на съответствието. Той ще се ползва от презумпцията за съответствие за рисковете, свързани с основната функционална възможност на този продукт и с функцията за почистване на диска, но не и за свързаните с функцията за защита от проследяване рискове.*

*Фигура 8*

**Хармонизираният стандарт предоставя ПС за основната функционална възможност и за спомагателна функционална възможност 1, тъй като обхваща всички рискове, свързани с тези две функционални възможности, но не и за спомагателна функционална възможност 2**



## 7. **ОЦЕНКА НА КИБЕРРИСКА И ИНТЕГРИРАНЕ НА ПРОДУКТИ С ЦИФРОВИ ЕЛЕМЕНТИ И КОМПОНЕНТИ**

### 7.1. **Оценка и третиране на киберрисковете**

156. За целите на оценката на киберриска, предвидена в член 13, параграф 2 от АК, производителите идентифицират съответните рискове и оценяват тяхното потенциално въздействие върху продукта с цифрови елементи. Производителите също трябва да прилагат подходящи мерки за справяне с тези рискове в съответствие със съществените изисквания, определени в приложение I.

157. При управлението на организационния риск оценяването на рисковете обикновено се извършва въз основа на критерии за приемане, произтичащи от вътрешните цели или рисковия апетит на организацията. За разлика от това, съгласно АК остатъчният киберриск следва да се оценява с оглед на изискването продуктът с цифрови елементи, пуснат на пазара, да гарантира подходящо ниво на киберсигурност въз основа на рисковете, като се вземат предвид неговото предназначение и разумно предвидима употреба.

158. Съответно вътрешната толерантност към риск на производителя, търговската стратегия или свързаните единствено с разходите съображения са от значение при определянето дали рисковете са разгледани. За целите на член 13, параграфи 2 и 3 производителите трябва да са в състояние да преценят дали идентифицираните киберрискове са разгледани, в достатъчна степен, чрез прилагането на съществените изисквания, определени в приложение I, част I, с оглед на предназначението, разумно предвидимата употреба и условията за употреба, включително, когато е целесъобразно, оперативната среда (например ползвателите на продукта с цифрови елементи по предназначение) и активите, които трябва да бъдат защитени, като се вземе предвид продължителността, през която се очаква продуктът да бъде в употреба.

159. Остатъчният киберриск е присъщ резултат от оценката на риска и от третирането на риска. Признава се, че на практика киберрисковете не могат да бъдат напълно елиминирани. Съществуването на остатъчен риск обаче не означава, че всеки риск може да бъде приет по преценка на производителя. Даден продукт с цифрови елементи може да бъде пуснат на пазара само когато остатъчните рискове, след като са предприети подходящи мерки, са разгледани, в достатъчна степен, чрез прилагането на съществените изисквания, като се вземат предвид предназначението и разумно предвидимата употреба на продукта с цифрови елементи.

160. В съответствие с член 13, параграф 3, когато са идентифицирани киберрисковете, производителите трябва да се справят с тях чрез подходящи мерки, включително на ниво продукт. В зависимост от обстоятелствата те могат да включват ограничаване на повърхностите, уязвими за атаки, прилагане на технически предпазни мерки, ограничаване или адаптиране на функционалността или по-прецизно определяне на предназначението на продукта с цифрови елементи. Производителите могат също да предприемат действия за оформяне на разумно предвидимата употреба на продукта с цифрови елементи, например чрез съобщаване на информация за риска, насоки за ползвателите или дизайн на потребителския интерфейс, за да насочат поведението на ползвателите към модели на сигурна употреба.

161. В АК не се предвижда прехвърляне на киберриска или отговорността към ползвателите или към трети страни, за да се компенсират недостатъци в дизайна на продукта или да се оправдае липсата на третиране на киберрисковете. Отговорността за пускане на пазара на сигурен продукт с цифрови елементи и за доказване на съответствието със съществените изисквания е на производителя.

162. Информацията и инструкциите, предоставени на ползвателите, могат да се използват за подпомагане на сигурното внедряване и експлоатация на продукта с цифрови елементи, включително когато производителят е избрал да ограничи предназначението на този продукт до надеждни среди, и да информира ползвателите за остатъчните рискове по начин, който е подходящ с оглед естеството на продукта с цифрови елементи и неговите ползватели по предназначение.

*Пример 66: производител разработва пропишлен датчик за използване в надеждни среди. Производителят не прилага мерки за защита от физически атаки срещу самия датчик, за да може датчикът правилно да изпълнява функционалната си възможност. С цел намаляване на свързаните рискове, идентифицирани в оценката на риска, производителят ограничава предназначението на датчика до използване само в надеждни среди, като по този начин се предотвратява непозволен физически достъп до продукта с цифрови елементи. В информацията и инструкциите, предоставени на ползвателите, ясно се посочва това ограничение при използването на датчика по начин, който е подходящ с оглед естеството на продукта с цифрови елементи и неговите ползватели по предназначение.*

*Пример 67: производител разработва предназначено за професионална употреба софтуерно приложение за управлявани настолни компютри и мобилни устройства. Приложението обработва локално съхранявани чувствителни данни и създадено от ползвателите съдържание. По време на оценката на риска производителят идентифицира риска от непозволен достъп до такива данни, ако те се съхраняват на устройството под формата на обикновен текст. Вместо да проектира и прилага собствен механизъм за криптиране в самото приложение, производителят избира да разчита на функциите за криптиране и управление на ключове, предоставени по подразбиране от операционната система, въз основа на която се предвижда да работи приложението, тъй като вградените криптографски услуги на операционната система са зрели и редовно поддържани.*

163. Когато чрез оценката на киберриска се идентифицират рискове, които не могат да бъдат надлежно третирани чрез подходящи мерки, с цел спазване на АК може да се изискват промени в дизайна, функционалността или предназначението на продукта с цифрови елементи. Съображенията, свързани единствено с разходите или търговската осъществимост, не представляват достатъчно основание за липсата на третиране на такива рискове, когато това би засегнало съответствието на продукта с цифрови елементи със съществените изисквания.

### 7.2. Проектиране, разработване и производство на продукти с цифрови елементи по такъв начин, че да гарантират подходящо ниво на киберсигурност въз основа на рисковете

164. Съгласно съществените изисквания за киберсигурност, посочено в приложение I, част I, точка 1 към АК, продуктите с цифрови елементи се проектират, разработват и произвеждат по такъв начин, че да гарантират подходящо ниво на киберсигурност въз основа на рисковете.

165. Това съществено изискване е насочено към справяне с всички киберрискове, идентифицирани като част от оценката на киберриска. По-конкретно то се прилага за киберрисковете, които не са подходящо разгледани по друг начин като част от изпълнението на съществените изисквания, определени в приложение I, част I, с изключение на точка 1. Това съществено изискване се различава от правното задължение за извършване на оценка на киберриска в съответствие с член 13, параграф 2.

166. Когато всички съответни киберрискове, свързани с даден продукт с цифрови елементи, се третират чрез прилагане на подходящи мерки с цел съответствие с приложимите съществени изисквания, с изключение на посоченото в точка 1, предвиденото в приложение I, част I, точка 1 съществено изискване се счита за изпълнено. Обратно, когато при оценката на киберриска бъдат идентифицирани допълнителни рискове, които не са напълно третирани чрез такива мерки, производителите са задължени да приложат подходящи мерки по отношение на продукта с цифрови елементи, за да се справят с тези рискове, така че да осигурят съответствието им със съществото изискване, посочено в приложение I, част I, точка 1. На практика, в повечето случаи се очаква това изискване да бъде изпълнено в резултат на спазването на другите съществени изисквания.

### 7.3. Оценка на риска и дължима грижа във връзка с външни зависимости и интегрирани компоненти

167. АК установява две отделни, но допълващи се задължения за производителите във връзка с управлението на киберриска. Първо, с член 13, параграф 2 се установява изискването производителите да извършват оценка на киберрисковете, свързани със самия продукт с цифрови елементи. Второ, с член 13, параграф 5 се установява задължението производителите да полагат дължимата грижа по отношение на интегрираните компоненти. Заедно тези две задължения се установяват с цел да се гарантира, че продуктът с цифрови елементи остава сигурен, включително когато зависи от решения за обработване на данни от разстояние, услуги от разстояние или софтуерни или хардуерни компоненти на трети страни.

168. Оценката на киберриска се отнася до идентифицирането и управлението на съответните рискове, които могат да засегнат продукта с цифрови елементи, включително рискове, които произтичат извън самия продукт, като външни мрежи, фактори на околната среда или други външни аспекти, които биха могли да засегнат продукта с цифрови елементи или от които продуктът зависи. АК не изисква от производителите да контролират или управляват външната среда по отношение на такива външни рискове. Вместо това производителите са задължени да идентифицират такива рискове и да ги смекчават чрез проектирането и разработването на самия продукт с цифрови елементи. Това включва прилагане на подходящите съществени изисквания, определени в приложение I, част I, и, когато е необходимо, предоставяне на информация и инструкции на ползвателите относно рисковете при интегриране или внедряване.

169. Например даден производител може да идентифицира риск от достъп на неупълномощени лица до сървърни системи, които не са част от самия продукт с цифрови елементи, докато продуктът е в експлоатация, и от опит да се изпратят зловредни команди към продукта с цифрови елементи. Когато не са проектирани и разработени от производителя или под негова отговорност или не поддържат някоя от функциите на продукта с цифрови елементи, такива сървърни системи не представляват решения за обработване на данни от разстояние и следователно не попадат в обхвата на продукта с цифрови елементи за целите на АК. Въпреки това АК задължава производителя да се справи с риска, който те могат да представляват, чрез мерки на ниво продукт, като например изискване за криптографско удостоверяване на автентичността на команди от разстояние, проверка на целостта на промените в конфигурацията или генериране на регистрационни файлове или сигнали, свързани със сигурността, когато се открие необичайно поведение. По същия начин, когато даден производител идентифицира произтичащ от недостъпността на такава външна услуга риск, например поради прекъсване на електрозахранването или повреди в инфраструктурата, съгласно АК може да се изискват мерки за смекчаване на ниво продукт срещу такива киберрискове като гарантиране, че резултатът от прекъсването не е преминаване на продукта с цифрови елементи в несигурни състояния. В такива случаи АК урежда начина на реагиране на продукта с цифрови елементи на тези външни рискове; той не въвежда задължения относно начина на организиране, обслужване или експлоатиране на сървърната инфраструктура, нито третира тази инфраструктура като част от продукта с цифрови елементи.

170. Дължимата грижа се отнася до елементи, които са част от самия продукт с цифрови елементи, по-специално интегрирани софтуерни или хардуерни компоненти, предоставени от трета страна. Производителите са задължени да предприемат подходящи мерки, за да гарантират, че с такива компоненти не се засяга съответствието на продукта с цифрови елементи със съществените изисквания. Това може да бъде постигнато само чрез определяне на изискванията на продукта с цифрови елементи спрямо компонентите му, за да се постигнат неговите цели по отношение на киберсигурността, и чрез основана на риска проверка, за да се потвърди съответствието на тези компоненти с нуждите на продукта, както е посочено и в съображение 34.

171. В съответствие с извършената от него оценка на киберриска производителят трябва да идентифицира изискванията, на които следва да отговаря интегрираният компонент. Ако например продуктът с цифрови елементи зависи от предоставени от компонент криптографски функции, механизми за актуализиране или сигурни комуникации, производителят трябва, като част от своята дължима грижа, да идентифицира тези нужди и да провери дали компонентът ги удовлетворява. Доказателствата за тази цел могат да бъдат под формата на получена от производителя на компонента документация, като например технически спецификации, документация за сигурност или съответна документация за съответствие или ниво на сигурност. Когато е целесъобразно, производителят може също да извърши изпитвания, за да провери дали тези компоненти изпълняват съответните функции по подходящ начин. Въпреки че дължимата грижа е отделно правно задължение, тя е в подкрепа и съставлява основата на способността на производителя да докаже съответствието със съществените изисквания относно продукта с цифрови елементи като цяло.

172. При оценката на рисковете, свързани с продукта с цифрови елементи като цяло, външните за него елементи като фактори на околната среда, външна инфраструктура, други системи или мрежи трябва да бъдат взети предвид в оценката на киберриска и, когато е целесъобразно, да бъдат разгледани чрез мерки на ниво продукт, за да се гарантира съответствието на продукта с цифрови елементи със съществените изисквания. Компонентите, които са физически или логически интегрирани в продукта с цифрови елементи, но са доставени от трета страна, също трябва да се разглеждат като част от оценката на риска. За целите на съответствието обаче производителят следва да ги третира като външно доставени компоненти, чиито свойства се проверяват чрез дължима грижа при интегрирането, тъй като производителят може да не ги е проектирал или разработил повторно.

173. Същата логика се прилага в процеса на разработването и интегрирането на компоненти. Когато производителят самостоятелно разработва функционалности, той трябва директно да приложи съществените изисквания. Когато производителят интегрира разработени от други лица компоненти, той трябва да гарантира чрез дължима грижа, че тези компоненти могат да се използват по начин, чрез който се осигурява съответствието на продукта с цифрови елементи като цяло. И в двата случая целта е една и съща: по отношение на продукта с цифрови елементи, както е пуснат на пазара, се осигурява подходящо ниво на киберсигурност в съответствие с АК предвид рисковете, идентифицирани в оценката на киберриска.

### 7.4. **Повторно използване на оценки на риска и документация за съответствие за семейства продукти с цифрови елементи**

174. Производителите могат да пускат на пазара сходни продукти с цифрови елементи, като например различни варианти, модели или конфигурации на едно и също продуктово семейство. Когато такива продукти с цифрови елементи имат една и съща архитектура, свързан със сигурността дизайн и предназначение и са изложени на едни и същи киберрискове, АК не установява изискване производителите да третират всеки вариант като напълно отделен продукт с цифрови елементи за целите на оценката на риска и оценяването на съответствието.

175. В такива случаи, при условие че свързаните с всички засегнати варианти съответни рискове и съществени изисквания са обхванати по подходящ начин, производителите могат да се позоват на: i) единна оценка на киберриска, извършена в съответствие с член 13, параграф 2 от АК; ii) единен комплект техническа документация; и iii) единна процедура за оценяване на съответствието. В този случай също се разрешава издаването на единна ЕС декларация за съответствие за групата продукти с цифрови елементи, при условие че в нея ясно са идентифицирани вариантите на продукта, за които се отнася.

176. Решаващият фактор е дали разликите между вариантите са от значение за киберсигурността. За варианти, които не засягат параметрите на киберсигурността на продукта с цифрови елементи като разлики в цвета, типоразмера, капацитета на паметта или други характеристики, които не са свързани със сигурността, не се изискват отделни оценки на риска или оценяване на съответствието. Обратно, в някои случаи с разликите между вариантите, като например различни интерфейси за комуникация, софтуерна стекова памет, механизми за актуализиране или свързаност от разстояние, може да се засяга изпълнението на съществените изисквания. В такива случаи тези разлики трябва да бъдат отразени в оценката на риска и, когато е необходимо, в оценката на съответствието и в техническата документация.

177. Производителите продължават да носят отговорност за гарантирането на точното отразяване на пуснатите на пазара продукти с цифрови елементи в оценката на риска и свързаната документация. Когато с нов вариант се въвеждат нови киберрискове или се променя начинът на прилагане на съществените изисквания, съществуващата оценка на риска и документация за съответствие трябва да бъдат съответно актуализирани. Позоваването на единна оценка на съответствието е възможно единствено в степента, в която продуктите с цифрови елементи не се различават по отношение на своите свързани с киберсигурността параметри.

## 8. **ОБРАБОТВАНЕ НА ДАННИ ОТ РАЗСТОЯНИЕ**

178. Съгласно определението в член 3, параграф 1 от АК „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“. В този контекст производителят трябва да разглежда продукта с цифрови елементи като цяло, включително неговите решения за обработване на данни от разстояние (РОДР). Когато например се доказва, че продуктът с цифрови елементи е в съответствие със съществените изисквания, определени в приложение I, трябва да се вземат предвид РОДР, като се започне с оценката на риска (член 13, параграф 2). Същото е в сила и по отношение на задълженията във връзка с жизнения цикъл, като например докладването относно активно използвани уязвимости и сериозни инциденти (член 14).

179. Целта на настоящите насоки е да се предостави допълнителна подкрепа на производителите при определянето дали техният продукт с цифрови елементи разполага с РОДР, съгласно определението в АК, и при изпълнението на задълженията им за съответствие в това отношение. След първоначален анализ на определенията и съображенията, изложени в АК, с настоящите насоки ще се предоставят въпроси, чрез които да се насочат производителите при изясняването дали техният продукт с цифрови елементи включва РОДР (вж. раздел *8.1 Какво се счита за решение за обработване на данни от разстояние по отношение на* даден продукт с цифрови елементи?). Впоследствие в тях ще се разяснят техническите последици от РОДР и начинът на оценяване на съответствието с АК (вж. раздел *8.2 Практически и технически последици от решенията за обработване на данни от разстояние и разчитането на решения на трети страни*).

180. Всъщност съгласно определението в член 3, параграф 2 понятието „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“. Следователно РОДР се определя като софтуерните елементи („частта от електронна информационна система, която се състои от компютърен код“, както е определено в член 3, параграф 4) на обработването на данни от разстояние. Не е предвидено хардуерът, от който може да зависи обработването на данни от разстояние, да бъде включен в обхвата на продукта с цифрови елементи.

181. В съображения 11 и 12 са изложени допълнителни разяснения относно начина, по който това понятие следва да се тълкува. В съображение 11 се пояснява, че целта на обхващането на решението за обработване на данни от разстояние е да се 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“. В него също се посочва, че „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“.

182. Следователно, като се вземе предвид изложеното в съображение 11, целта е установените в АК изисквания да не се прилагат за цялата ИТ инфраструктура на дадена организация, а само за софтуерните компоненти, които позволяват изпълнението на решението за обработване на данни. Например вътрешните системи, свързани със собствените човешки ресурси на производителя, ведомостите за заплати, управлението на взаимоотношенията с клиентите, процесите за непрекъсната интеграция/непрекъснато предоставяне (CI/CD) и разпространението на актуализации за сигурност до крайни точки, не следва да се считат за РОДР. По същия начин системите, свързани с дейности по одит и изпитване като извършване на тестове за проникване, улавяне на заплахи и тестова кибератака с цел подобряване на сигурността, са извън обхвата на даден продукт с цифрови елементи предмет на АК. Важно е да се отбележи, че макар изпълнението на ефективни и редовни проверки и прегледи на сигурността на продукта с цифрови елементи да е съществено изискване съгласно приложение I, част II, точка 3 към АК, това не означава, че такива дейности трябва да се считат за РОДР за продукта с цифрови елементи.

183. В съображение 12 се разглеждат услугите в облак и се разясняват обстоятелствата, при които услугите могат да се считат за РОДР. В края на съображението се припомня, че услугите в облак и моделите на услуги в облак попадат в обхвата на Директива (ЕС) 2022/2555 (МИС 2) ([28]), която установява изисквания относно управлението на риска в областта на киберсигурността за доставчиците на компютърни услуги „в облак“. Тези изисквания са допълнително определени в Регламент за изпълнение (ЕС) 2024/2690 ([29]) на Комисията.

### 8.1. **Какво се счита за решение за обработване на данни от разстояние по отношение на даден продукт с цифрови елементи?**

184. Определението за обработване на данни от разстояние, дадено в член 3, параграф 2, се основава на три елемента: i) дали обработването на данни се извършва „от разстояние“; ii) дали липсата на такова обработване би попречила на продукта с цифрови елементи да изпълнява една от своите функции; и iii) дали софтуерът е проектиран и разработен от производителя или под негова отговорност. Тези елементи се разглеждат по-подробно в следващите три подраздела.

([28]) Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2) (ОВ L 333, 27.12.2022 г., стр. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) Регламент за изпълнение (ЕС) 2024/2690 на Комисията от 17 октомври 2024 г. за определяне на правила за прилагане на Директива (ЕС) 2022/2555 по отношение на техническите и методологичните изисквания относно мерките за управление на риска в областта на киберсигурността и за доуточняване на случаите, в които даден инцидент се счита за значителен по отношение на доставчиците на DNS услуги, регистрите на имена на домейни от първо ниво, доставчиците на компютърни услуги „в облак“, доставчиците на услуги на центрове за данни, доставчиците на мрежи за доставяне на съдържание, доставчиците на управлявани услуги, доставчиците на управлявани услуги за сигурност, доставчиците на онлайн места за търговия, на онлайн търсачките и на платформите на услуги за социални мрежи и доставчиците на удостоверителни услуги (ОВ L 2024/2690, 18.10.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1. *Понятието „от разстояние“*

185. Понятието „от разстояние“, посочено в член 3, параграф 2, е уместно, но не е достатъчно, за да се определи дали даден продукт с цифрови елементи включва РОДР. Освен това, като се вземе предвид разнообразието от решения, които могат да попаднат в обхвата на това понятие, не е възможно да се предостави изчерпателно определение за понятието „от разстояние“. Производителят трябва да извърши оценка за всеки отделен случай.

186. В съображение 11 от АК се прави разграничение между данни, които се обработват или съхраняват „от разстояние от производителя“, и данни, които се обработват или съхраняват „локално на устройството на ползвателя“. Обработването на данни от разстояние обикновено се извършва извън средата на ползвателя на даден продукт с цифрови елементи или извън оперативната среда на дадена организация (за професионален ползвател). Това обаче не е пречка обработването да се извършва и в близост до устройството („в периферията“). Предаването на данни може да се извършва с кабел (напр. кабел за Етернет) или без кабел (напр. чрез безжична локална мрежа или блутут). Компютърните услуги „в облак“, включително периферните изчисления, са типичен пример за обработване на данни, което се извършва „от разстояние“. Например в случай на базирана в облак функция, достъпна за ползвателя от мобилно приложение, част от обработването на данни се извършва в облака — извън средата на ползвателя.

187. Важно е да се отбележи, че РОДР не функционират непременно в инфраструктура за компютърни изчисления в облак на трета страна. Обработването на данни от разстояние, което се извършва на локални сървъри в помещенията на производителя, също може да представлява РОДР. С други думи, функциониращо в помещенията и в частен облак решение е също толкова вероятно да се квалифицира като РОДР, колкото и функциониращо в публичен облак и извън помещенията решение.

188. Двата решаващи и кумулативни въпроса, въз основа на които се определя дали обработването на данни попада в обхвата на АК като решение за обработване на данни от разстояние, са посочени в раздели *8.1.2* и *8.2* по-долу. Ако отговорът и на двата въпроса е утвърдителен, обработването на данни от разстояние се квалифицира като РОДР.

8.1.2. *Липсата на такова обработване би ли попречила на продукта с цифрови елементи да изпълнява една от своите функции?*

189. Както е посочено в определението за „обработване на данни от разстояние“, дадено в член 3, параграф 2, за да се квалифицира дадено обработване на данни от разстояние като РОДР, липсата му трябва да е пречка продуктът с цифрови елементи да изпълнява една от своите функции. Понятието „функции“, използвано в това определение, не се ограничава до „основната функционална възможност“ или „предназначението“ на продукта с цифрови елементи, тъй като АК не установява такова ограничение. Функциите в обхвата на АК са както функции, чрез които продуктът с цифрови елементи директно изпълнява предназначението си, както се възприема от ползвателите, така и функции, чрез които се поддържа цялостното представяне на продукта.

190. Примери за функции, при които може да се извършва обработване на данни от разстояние и които биха попречили на продукт с цифрови елементи да изпълнява една от своите функции: i) изпращане на команди към устройство; ii) синхронизиране на файлове; iii) присъединяване на ползвателя; iv) конфигуриране (персонализиране на продукта с цифрови елементи); v) автоматизирано разпространение на актуализации, включително актуализации на функции и софтуерни поправки за сигурност; vi) управление на самоличността и достъпа.

191. В някои случаи ползвателят може да използва дадена функция както от разстояние, така и ръчно (напр. включване или изключване на електрическа крушка чрез приложение или ръчно). Наличието на тази опция не е основание за изключване на квалифицирането на обработването на данни, свързано с изпълнението на функцията от разстояние, като РОДР. Изпълнението на тази функция от разстояние също се счита за част от функциите на продукта с цифрови елементи.

192. За разлика от това, когато липсата на дадено обработване на данни не пречи на продукта с цифрови елементи да изпълнява една от своите функции, това обработване не се счита за РОДР по смисъла на АК. Това включва например анализ на телеметрични данни, събирани единствено за статистически цели или за бъдещо разработване на продукти, от разстояние.

193. Въпреки това, дори когато с обработването на данни не се поддържа функция на продукт с цифрови елементи, производителите може да трябва да преценят дали чрез тези компоненти от разстояние се въвеждат рискове за продукта с цифрови елементи като част от тяхната оценка на киберриска (напр. с оглед на оперативната среда на продукта) и да намалят тези рискове съответно (напр. чрез мерки за смекчаване на ниво продукт).

194. Уебсайтовете са специфичен случай, по отношение на който е целесъобразно да се предоставят допълнителни разяснения, както е обяснено и в *раздел 2.1 Пускане на пазара*. Уебсайтовете не попадат в обхвата на РОДР, ако не поддържат функция на продукт с цифрови елементи, както е обяснено в съображение 11 от АК. Не е достатъчно даден уебсайт да съдържа информация за продукт с цифрови елементи, за да се счита за попадащ в обхвата на РОДР, дори ако продуктът пренасочва към такъв уебсайт. Например пренасочването на ползвателите към външна уебстраница, която предоставя информация и инструкции на ползвателите, не представлява РОДР. За разлика от това даден уебсайт може да попада в обхвата на РОДР, ако чрез него се активира или поддържа функция на продукт с цифрови елементи. Например портал за удостоверяване на автентичността, който издава удостоверения за самоличност или токени, необходими за функционирането на продукта с цифрови елементи, би се считал за РОДР (при условие че са изпълнени и другите критерии на определението).

8.1.3. *Проектиран и разработен ли е софтуерът от производителя или под негова отговорност?*

195. В определението за „обработване на данни от разстояние“, дадено в член 3, параграф 2 от АК, допълнително се уточнява, че софтуерът за такова обработване на данни от разстояние трябва да бъде проектиран и разработен от производителя или под негова отговорност. Дадено обработване на данни от разстояние, изцяло разработено и проектирано от производителя (на вътрешнофирмено ниво), автоматично се квалифицира като РОДР. Това би било така и ако производителят разчита на външен доставчик на услуги за разработването и проектирането на дадено решение (т.е. „под негова отговорност“). Изразът „под отговорността на производителя“ се отнася до решения за обработване на данни от разстояние, които са специално разработени за производителя. Това са случаи, при които производителят не само лицензира съществуващ продукт с цифрови елементи или услуга, която доставчик на услуги предлага на своите клиенти, или техни незначително изменени версии. „[П]од отговорността на производителя“ означава, че софтуерът е създаден единствено от производителя или от името на производителя въз основа на предоставени от него дизайни и спецификации.

196. По отношение на разбирането на РОДР концепцията за експлоатиращо решението лице не е решаващ фактор, тъй като определението в АК се отнася само до проектирането и разработването на РОДР. Това е в съответствие с установения в АК подход, според който изискванията и задълженията са насочени към производителите, а не към експлоатацията на продукта с цифрови елементи. Ако производителите проектират и разработват решения, които след това се експлоатират от трета страна, те продължават да носят отговорност за спазването на съществените изисквания на АК относно продукта с цифрови елементи, който пускат на пазара.

197. Необходимо е да се прави разлика между случаите, в които проектирането и разработването се извършват от производителите (или под тяхна отговорност), и случаите, в които се разчита на решения на трети страни, които не са проектирани и разработени от производителите (или под тяхна отговорност). Като пример е удачно да се разгледат най-често срещаните модели на услуги в облак, чрез които се осигуряват различни нива на контрол върху ползвателите и които също са посочени в съображение 12 от АК, а именно софтуер като услуга (SaaS), платформа като услуга (PaaS) и инфраструктура като услуга (IaaS).

198. В случай на решение IaaS на трета страна, производителят не управлява и не контролира основните физически и виртуални ресурси (като например основния хардуер и хипервайзора на доставчика на услуги в облак), но може да внедрява и изпълнява софтуер по избор, използвайки такива ресурси, като операционни системи и приложения. Такъв софтуер е проектиран и разработен от производителя или под негова отговорност и поради това може да се квалифицира като РОДР (при условие че са изпълнени и другите критерии на определението).

199. В случай на решение PaaS на трета страна, производителят внедрява свое собствено (създадено или придобито) приложение, използвайки програмни езици и среди за изпълнение, предоставени от доставчика на услуги в облак, и интегрира приложението в своя продукт с цифрови елементи. Производителят има контрол върху приложението и евентуално върху настройките за конфигуриране на средата за изпълнение. Следователно приложението е проектирано и разработено от производителя или под негова отговорност и поради това може да се квалифицира като РОДР (при условие че са изпълнени и другите критерии на определението).

200. В случай на решение SaaS на трета страна доставчикът на SaaS предлага на производителя напълно разработено приложение, което да бъде интегрирано в продукта с цифрови елементи на производителя. Производителят има ограничена възможност да управлява специфичните за ползвателя настройки за конфигуриране на приложението. Следователно приложението не е проектирано и разработено от производителя или под негова отговорност.

201. Въпреки това, когато определени елементи не се квалифицират като РОДР (напр. хипервайзорът в случай на инфраструктура IaaS на трета страна, операционната система в случай на решение PaaS на трета страна или приложението SaaS на трета страна), но са интегрирани в продукта с цифрови елементи по начин, който засяга неговата сигурност, такива решения следва да се считат за подобни на компонентите на трети страни. Производителят е задължен да идентифицира и оценява рисковете, свързани с интегрирането на тези елементи, и да ги третира чрез прилагане на съществените изисквания относно самия продукт с цифрови елементи. Това може, когато е целесъобразно, да бъде подпомогнато от функциите за сигурност, предоставени от доставчика на услуги в облак чрез неговия модел на споделена отговорност, при който производителят използва или конфигурира тези функции с цел справяне с идентифицираните рискове. Освен това се очаква производителят да изпълнява задължение, подобно на задължението за полагане на дължимата грижа съгласно член 13, параграф 5, във връзка със сигурността на тези компоненти по начин, пропорционален на риска, който се въвежда с решението от разстояние по отношение на сигурността на продукта с цифрови елементи.

202. Следователно може да се обобщи, че:

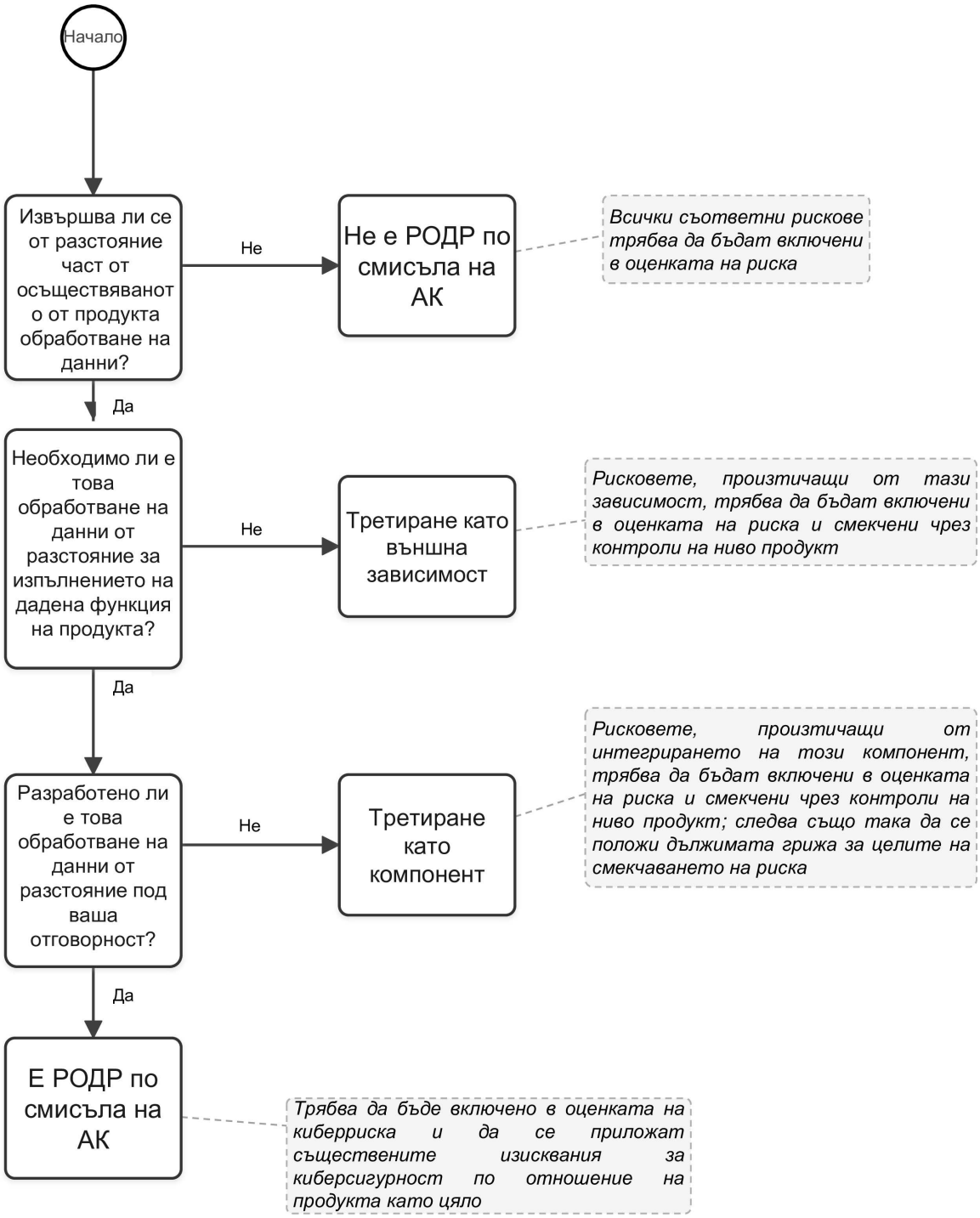
a) с цел квалифициране на дадено обработване на данни като РОДР отговорът и на двата въпроса в раздели *8.1.2 Липсата на такова обработване би ли попречила на продукта с цифрови елементи да изпълнява една от своите функции?* и *8.1.3 Проектиран и разработен ли е софтуерът от производителя или под негова отговорност?* трябва да бъде утвърдителен;

b) ако отговорът на въпроса в раздел *8.1.2 Липсата на такова обработване би ли попречила на продукта с цифрови елементи да изпълнява една от своите функции?* е отрицателен, производителите следва да оценят рисковете, произтичащи от съществуването на такова обработване на данни, като част от своята оценка на риска;

c) ако отговорът на въпроса в раздел *8.1.2 Липсата на такова обработване би ли попречила на продукта с цифрови елементи да изпълнява една от своите функции?* е утвърдителен, а отговорът на въпроса в раздел *8.1.3 Проектиран и разработен ли е софтуерът от производителя или под негова отговорност?* е отрицателен, производителите следва да третират решението на третата страна като компонент. Като част от оценката на риска производителите следва да оценят рисковете, произтичащи от интегрирането на такова решение, и да ги намалят съответно. Освен това производителите следва да полагат дължимата грижа.

*Фигура 9*

**Стилизирана схема за определяне дали даден продукт с цифрови елементи включва РОДР**




### 8.2. Практически и технически последици от решенията за обработване на данни от разстояние и разчитането на решения на трети страни

203. АК установява основан на риска подход, както е изложено в член 13, параграфи 2 и 3 и в първото съществено изискване, посочено в приложение I, част I, съгласно което „продуктите с цифрови елементи се проектират, разработват и произвеждат по такъв начин, че да гарантират подходящо ниво на киберсигурност въз основа на рисковете“. Съответно следва да се вземе предвид основан на риска подход при прилагането на изискванията на АК за РОДР и третирането на рисковете, произтичащи от интегрирани в продукта с цифрови елементи услуги на трети страни.

204. Първо, производителите следва i) да посочат в техническата документация, че техният продукт с цифрови елементи включва РОДР или зависи от предоставяни от трета страна решения от разстояния, и ii) да опишат тези решения. Ако с едно и също РОДР се поддържат няколко продукта с цифрови елементи, РОДР трябва да бъде посочено в техническата документация на всеки продукт. Документацията относно РОДР, с което се обслужват няколко продукта с цифрови елементи и е изготвена при дадено оценяване на съответствието на продукта може да бъде повторно използвана за целите на друго оценяване.

205. Както е посочено в съображение 11, РОДР, които са част от продукта с цифрови елементи и следователно част от оценяването на съответствието на продукта, следва да бъдат ограничени до онези софтуерни модули, чрез които се осъществява функционалната възможност на продукта с цифрови елементи, и до интерфейсите, чрез които тези модули използват външни услуги. Допълнителните сървърни системи, които извършват последващо обработване и не са в пряко взаимодействие с продукта с цифрови елементи, не се считат за РОДР.

206. Въпреки това тези сървърни системи остават външни зависимости, които трябва да бъдат оценени като част от оценката на киберриска и намалени чрез мерки на ниво продукт. Всъщност производителят следва да вземе предвид следното при оценяването на риска: i) рисковете, свързани с РОДР; ii) рисковете, свързани с разчитането на решения от разстояние на трети страни (подобни на компонентите на трети страни); и iii) рисковете, свързани с продуктовата среда (напр. основният хардуер). Производителите следва да прилагат контроли за сигурност спрямо самия продукт с цифрови елементи, за да намалят тези рискове.

207. Освен това, като част от оценяването на съответствието и/или изпълнението на задълженията за дължима грижа, свързани с услуги от разстояние на трети страни, следният неизчерпателен списък от артефакти в полза на нивото на увереност може да бъде използван повторно в подкрепа на оценката на производителя:

a) доказателство за изпълнение на задълженията съгласно Регламент за изпълнение (ЕС) 2024/2690 на Комисията;

b) доказателство за изпълнение на задълженията съгласно Регламент (ЕС) 2022/2554 (DORA);

c) декларация за съответствие или сертификат, издаден по европейска схема за сертифициране на киберсигурността (приета съгласно Регламент (ЕС) 2019/881 — Актът за киберсигурността);

d) доказателство за съответствие с ISO/IEC 27017:2015 или ISO/IEC 27001:2022.

208. И накрая, при взаимодействията си с доставчици на услуги от разстояние, които са трети страни, производителите трябва да прилагат най-подходящите мерки за сигурност въз основа на своята оценка на риска (и, когато е целесъобразно, подкрепени от модела на споделена отговорност на доставчика). Тези мерки за смекчаване следва да включват контроли за сигурност за техните продукти с цифрови елементи и проверка на мерките за сигурност, предоставени от самите доставчици трети страни (дължима грижа). Инструмент за намаляването на такива рискове може да бъде включването на гаранции за сигурност в техните споразумения за нивото на обслужване (SLA) с доставчици трети страни, включително уверения за отстраняване от страна на доставчиците на уязвимостите по подходящ начин. Дадена значителна промяна в решенията, предоставени от доставчиците на услуги от разстояние, които са трети страни, не следва да се квалифицира като съществено изменение на продукта с цифрови елементи, тъй като тези елементи не са под отговорността на производителя. Въпреки това, като част от своите задължения за дължима грижа и за намаляване на рисковете, произтичащи от използването на услуги на доставчици трети страни, по надлежен начин, производителите се насърчават да гарантират, че техните доставчици на услуги в облак, които са трети страни, ги информират за промените, които прилагат в своите решения, по подходящ начин. Въз основа на такава информация може да е необходимо производителите да преразгледат своята оценка на риска. В актуализираната оценка на риска следва да се вземе предвид дали доставчиците на услуги, които са трети страни, продължават да предоставят достатъчни гаранции по отношение на киберсигурността и дали мерките за сигурност на ниво продукт все още са подходящи. В някои случаи може да е необходимо производителите да модифицират тези контроли или да сменят съответните доставчици на услуги, които са трети страни.

### 8.3. **Случаи на употреба за решения за обработване на данни от разстояние**

С цел предоставяне на производителите на допълнителни практически насоки в настоящия раздел се разглежда поредица от примерни случаи на употреба, в които се описват архетипни продукти с цифрови елементи, които зависят от обработване на данни от разстояние, и се илюстрира дали съответното обработване се квалифицира като решение за обработване на данни от разстояние по смисъла на АК.

8.3.1. *Приложение за мобилно банкиране*

Финансов субект пуска на пазара приложение за мобилно банкиране. Сървърните системи на приложението поддържат, наред с другото, удостоверяване на автентичността, оторизация, управление на акаунти и плащания. С цел поддържане на функционалните възможности на приложението финансовият субект прилага хибридна стратегия, като използва вътрешна инфраструктура и решения от разстояние на трети страни. Те включват:

*Самостоятелно хоствана инфраструктура, разработена от финансовия субект:*

— Клиентът отваря приложението за мобилно банкиране, при което се извършва удостоверяване на автентичността чрез банковия интерфейс — самостоятелно хоствано решение, разработено от финансовия субект, което получава заявките на приложението и връща съответните отговори. Банковият интерфейс проверява самоличността на клиента чрез заявка към системата за управление на акаунти и предоставя достъп до приложението.

— Клиентът инициира превод чрез приложението. Приложението изпраща инструкцията към банковия интерфейс, който подава съответната заявка към системата за регистриране.

— Системата за управление на акаунти и системата за регистриране, които са самостоятелно хоствани, но логически отделени от банковия интерфейс, записват трансакцията.

— Системата за регистриране връща статуса на трансакцията към банковия интерфейс, който представя резултата на клиента.

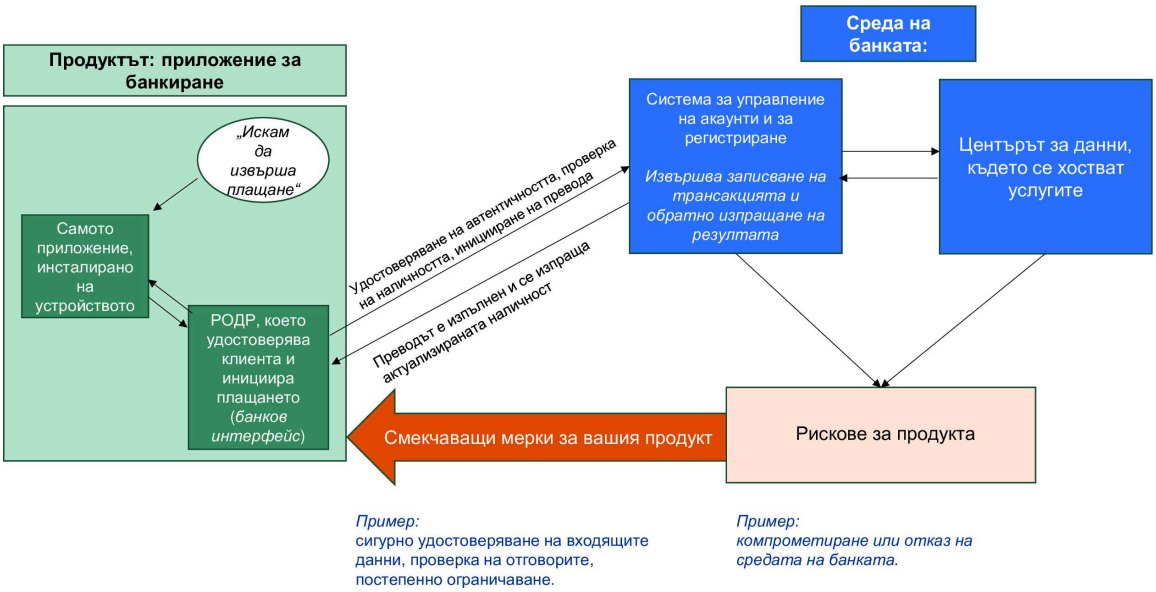
*Последици за РОДР:*

— Банковият интерфейс е необходим, за да може приложението да изпълнява функциите си, а именно удостоверяване на клиента, подаване на инструкциите от клиента, включително инструкции за плащане и превод, и връщане на получения статус. Банковият интерфейс е проектиран и разработен под отговорността на производителя. Тъй като отговорът и на двата въпроса, представени в предходни раздели, е утвърдителен, банковият интерфейс трябва да се счита за РОДР. Следователно той трябва да бъде включен в оценката на киберриска и в процеса на прилагане на съществените изисквания по отношение на продукта с цифрови елементи като цяло. Последващото обработване на инструкция след подаването ѝ, по-специално записването на трансакцията в системите за управление на акаунти и за регистриране, сетълментът и клирингът, се извършват от системи, с които приложението не взаимодейства директно и на това основание не представлява РОДР.

— Системата за управление на акаунти и системата за регистриране не се квалифицират като РОДР по отношение на приложението за мобилно банкиране. Приложението не взаимодейства директно с тях (вместо това то взаимодейства с банковия интерфейс, който на свой ред зависи от тях). Въпреки че тяхната наличност може да е необходима за изпълнението на дадена функция, АК обхваща само онези части от системата, които взаимодействат директно с продукта с цифрови елементи. Следователно те не попадат в обхвата на определението за РОДР за целите на АК. Въпреки това тези системи остават външни зависимости, в резултат на които могат да възникнат значителни киберрискове за продукта с цифрови елементи. Ако например системата за регистриране бъде компрометирана, е възможно извършител на атака да повлияе на резултатите от трансакциите, които впоследствие се показват в приложението. Поради това производителят е задължен да идентифицира и оцени тези рискове като част от оценката на киберриска и да ги намали чрез мерки на ниво продукт, като например сигурно удостоверяване на интерфейсите на сървърните системи, защита на целостта на данните за трансакциите, сигурни комуникационни канали и проверка на отговорите, получени от приложението.

*Фигура 10*

**Стилизирана схема на приложение за банкиране, което зависи от РОДР**




*SaaS на трета страна за клиентска поддръжка:*

— Финансовият субект интегрира в своето приложение решение за чат за клиентска поддръжка, разработено и управлявано от доставчик трета страна; доставчикът трета страна е написал кода на сървъра за чат, изградил е потребителския интерфейс и управлява инфраструктурата, където е внедрен чатът (т.е. модел SaaS).

— Когато клиентът инициира заявка за поддръжка, приложението свързва клиента с услугата на третата страна, за да установи чат сесия и да обработи потока от съобщения, без да предоставя на третата страна достъп до основните банкови системи.

*Последици за РОДР:*

— Решението за чат за поддръжка е необходимо, за да може продуктът с цифрови елементи да изпълнява една от функциите си, но не е проектирано и разработено от финансовия субект или под негова отговорност; следователно то не е РОДР. То обаче следва да се третира като компонент на трета страна. В резултат на използването на тази услуга на трета страна може да възникнат киберрискове за приложението за банкиране, ако например извършител на атака използва канала за чат, за да се представи за банката или да достави зловредно съдържание на ползвателите. Финансовият субект трябва да вземе предвид тези рискове в своята оценка на киберриска и да ги намали чрез мерки на ниво продукт, като например изолиране на функцията за чат от основните функции за банкиране, контролиране на информационните потоци и валидиране на съдържанието. По отношение на SaaS също следва да се положи дължима грижа.

8.3.2. *Интелигентен термостат*

С интелигентен термостат ползвателите могат да контролират температурата в своя дом чрез мобилно приложение. Мобилното приложение и интелигентният термостат зависят от обработване на данни от разстояние, за да обменят данни (напр. заявка за повишаване на температурата) и да съхраняват данни (напр. предпочитания на ползвателя). Тези функции са разработени и проектирани под отговорността на производителя, но работят върху основна физическа и виртуална инфраструктура, предоставена от трета страна (IaaS на трета страна).

Тъй като интелигентният термостат не може да изпълнява своите интелигентни функционални възможности без това обработване на данни от разстояние, липсата на това обработване би попречила на продукта с цифрови елементи да изпълнява една или повече от своите функции. Освен това софтуерът е разработен и проектиран под отговорността на производителя на интелигентния термостат. Поради това обработването на данни от разстояние се квалифицира като РОДР, както е определено в АК.

За целите на съответствието с АК производителят на интелигентния термостат трябва да документира РОДР и използването на IaaS на трета страна в техническата документация на продукта с цифрови елементи, включително подробности за договорената услуга. Производителят трябва да вземе предвид тези елементи в оценката на риска, в която са включени предназначението и разумно предвидимата употреба на продукта с цифрови елементи. Производителят прилага съществените изисквания на АК въз основа на рисковете по отношение на РОДР. За IaaS на третата страна производителят трябва да гарантира, че мерките за сигурност, предоставени от доставчика трета страна, са подходящи, и/или да предприеме съответните мерки по отношение на инфраструктурата. За целта производителят може например да изиска доказателства относно изпълнението на задълженията по МИС 2.

8.3.3. *Електронен четец*

Производител на софтуер за електронен четец използва SaaS на трета страна като услуга за съхранение на електронни книги, закупени от страна на клиентите, и за предоставяне на клиентите на достъп до книгите им. Липсата на тази услуга за съхранение би попречила на продукта с цифрови елементи да изпълнява една от своите функции, но SaaS на третата страна не е разработен от производителя или под отговорността на производителя; доставчикът на SaaS предоставя на клиентите услугата за съхранение за всякакви случаи на употреба.

Този SaaS не отговаря на определението за РОДР. Производителят на електронния четец обаче разчита на тази външна услуга с оглед функционирането на неговия продукт с цифрови елементи и поради това трябва да вземе предвид свързаните рискове в своята оценка на киберриска. Производителят на електронния четец следва да третира SaaS като компонент. Производителят трябва да прилага подходящи мерки за сигурност на ниво продукт, като например сигурно удостоверяване на автентичността, криптиране и защита на целостта на комуникациите спрямо услугата за съхранение. Полагането на дължима грижа при избора на доставчик на SaaS и интегрирането на SaaS също ще е в подкрепа на задълженията на производителя относно осигуряване на съответствието на продукта с цифрови елементи като цяло със съществените изисквания.

8.3.4. *Промишлен робот*

На промишлен робот е възложена задачата да взема части. Роботът изпраща събрана чрез камери информация до услуга от разстояние, проектирана и разработена от производителя. Тази услуга работи върху основна физическа и виртуална инфраструктура, предоставена от доставчик на услуги, който е трета страна (IaaS на трета страна). Услугата в облак изчислява позицията на частта въз основа на информационните потоци от камерите и изпраща команди обратно към робота, за да вземе той частите.

Липсата на това обработване на данни би попречила на промишления робот да взема части, т. е. да изпълнява една от своите функции. Освен това софтуерът, работещ върху инфраструктурата, е проектиран и разработен от производителя. Софтуерът, проектиран и разработен от производителя, отговаря на определението за РОДР.

Производителят на промишления робот трябва да документира РОДР и зависимостта от IaaS на трета страна в техническата документация на продукта с цифрови елементи (включително подробности за договорената услуга). Производителят също трябва да вземе предвид тези елементи в оценката на риска, в която се включват предназначението и разумно предвидимата употреба на продукта с цифрови елементи. Производителят прилага съществените изисквания на АК за продукта с цифрови елементи, включително неговото РОДР, въз основа на рисковете. Полагането на дължима грижа при избора на доставчик на IaaS също ще е в подкрепа на задълженията на производителя. Например производителят може да изиска доказателства относно изпълнението на задълженията по МИС 2.

8.3.5. *Клетъчна мрежа*

Смартфон зависи от мрежа 5G, за да осигури връзка с интернет, телефонни разговори и съобщения на своите ползватели (мобилна свързаност). Клетъчната мрежа е разработена и проектирана от телекомуникационни оператори. Мрежата се състои от малки клетки, клетъчни антени и друго мрежово оборудване.

Продуктът с цифрови елементи следва да може да се свързва с мрежата по правилен начин; това е една от неговите функции. Функционирането на тази мрежа или липсата му обаче не е от значение за установяване дали продуктът с цифрови елементи работи правилно. Мрежата е само комуникационен канал и не е необходима, за да изпълнява продуктът с цифрови елементи функцията си за свързване с мрежа по правилен начин. По същия начин даден кабел за Етернет, маршрутизатор или сигнал на безжична локална мрежа не се счита за обработване на данни, чиято липса би попречила на продукта с цифрови елементи да изпълнява една от своите функции, а за средство за комуникация/свързаност.

Следователно клетъчната мрежа не отговаря на определението за РОДР. Мрежата не следва да се счита за компонент на трета страна, тъй като в продукта с цифрови елементи няма интегриран софтуер, а продуктът единствено използва тази мрежа. Поради това не е необходимо производителят да изпълнява задължения за дължима грижа спрямо доставчика на мрежови услуги.

## 9. **ДОПЪЛНИТЕЛНИ ЕЛЕМЕНТИ**

### 9.1. **Задължения за докладване**

209. Съгласно член 14, параграфи 1 и 3 от АК производителят е задължен да нотифицира едновременно определения за координатор ЕРИКС и ENISA за i) всяка активно използвана уязвимост, съдържаща се в продукта с цифрови елементи, за която е узнал; и ii) всеки сериозен инцидент, за който е узнал, който оказва въздействие върху сигурността на продукта с цифрови елементи.

210. В съответствие с член 69, параграф 3 и член 71, параграф 2, второ изречение задълженията по член 14 се прилагат от 11 септември 2026 г. за всички продукти с цифрови елементи, които попадат в обхвата на АК, включително продукти с цифрови елементи, пуснати на пазара преди 11 декември 2027 г. Освен това, за разлика от задълженията за отстраняване на уязвимости, които са в сила само през периода на поддръжка на продукта, прилагането на задълженията за докладване продължава и след като продуктът с цифрови елементи вече не се поддържа. Когато продукт с цифрови елементи е бил пуснат на пазара преди 11 декември 2027 г. или когато периодът му на поддръжка е изтекъл, задълженията за отстраняване на уязвимости, определени в приложение I, част I, не се прилагат за производителя.

211. Следва да се припомни, че задължението за нотифициране на такива събития се прилага, след като производителят е узнал, че дадена уязвимост се използва активно или че е възникнал сериозен инцидент, в резултат на който е компрометирана сигурността на неговия продукт с цифрови елементи. Поради това насоките относно това кога производителят се счита за узнал следва да са от помощ на производителите при определяне на момента, от който започват да текат приложимите срокове за докладване.

212. За производителите могат да се прилагат сравними задължения за докладване съгласно различни актове на ЕС. С цел гарантиране последователно тълкуване на понятието „узнал“ и улесняване на спазването на тези задължения от страна на производителите тези насоки са приведени в съответствие със съображение 31 от Регламент за изпълнение (ЕС) 2024/2690 на Комисията и раздел II, точка А) от Насоки 9/2022 относно уведомяването за нарушение на сигурността на личните данни съгласно ОРЗД.

213. В някои случаи производителят ще открие подозрително събитие или трета страна, като например физическо лице, клиент, субект, орган, медийна организация или друг източник, ще насочи вниманието му към потенциален инцидент или уязвимост. В такива случаи производителят следва незабавно да оцени подозрителното събитие, за да определи дали то представлява активно използвана уязвимост или сериозен инцидент, който оказва въздействие върху сигурността на продукта с цифрови елементи. Следователно се счита, че производителят е узнал, когато след такава първоначална оценка той е установил с достатъчна степен на сигурност, че: i) уязвимост, съдържаща се в неговия продукт с цифрови елементи, се използва активно; или (ii) е възникнал сериозен инцидент, в резултат на който е компрометирана сигурността на неговия продукт с цифрови елементи.

214. Следователно моментът, в който може да се счита, че производителят е узнал, ще зависи от обстоятелствата, свързани с конкретната активно използвана уязвимост или с конкретния сериозен инцидент. В някои случаи ще е относително ясно от самото начало, че дадена уязвимост се използва активно или че сериозен инцидент оказва въздействие върху сигурността на съответния продукт с цифрови елементи. В други случаи може да отнеме известно време, за да се установи дали даден продукт с цифрови елементи е засегнат от уязвимост и дали тази уязвимост се използва от злонамерен участник, или дали инцидент оказва въздействие върху сигурността на съответния продукт с цифрови елементи. Акцентът обаче следва да бъде върху предприемането на незабавни действия за извършване на първоначалната оценка, за да се определи дали тези условия действително са изпълнени, по-специално когато уязвимостта може да представлява значителен риск, и ако е така, да се предприемат коригиращи действия и да се извърши нотифициране в съответствие с АК.

215. Освен това производителите трябва, в съответствие със структурата на задълженията за докладване, да актуализират своите нотификации поетапно с напредването на вътрешните им разследвания и с придобиването на по-подробна информация относно активно използваната уязвимост или инцидента. По-конкретно производителят е задължен да представя нотификация за ранно предупреждение, в която се включва ограничена информация, без ненужно забавяне и при всички случаи в рамките на 24 часа, след като е узнал. Впоследствие се изисква предоставяне на допълнителна информация като част от нотификацията, без ненужно забавяне и при всички случаи в рамките на 72 часа, след като производителят е узнал („нотификацията в рамките на 72 часа“). Окончателният доклад трябва да бъде представен не по-късно от 14 дни, след като коригираща или смекчаваща мярка стане налична, в случай на активно използвана уязвимост или не по-късно от един месец след нотификацията в рамките на 72 часа в случай на сериозен инцидент.

216. Както е припомнено и в раздел *3.3.1 Устойчива подкрепа и гарантиране на жизнеспособността на FOSS*, от попечителите на софтуер с отворен код също се изисква да докладват за активно използвани уязвимости в съответствие с член 24, параграф 3 ([30]). Това задължение се прилага, когато попечителят е узнал за активно използвана уязвимост, а не само когато съществува уязвимост в кодовата база на FOSS, чийто попечител е този субект. На практика, тъй като компонентите на FOSS обикновено се интегрират надолу по веригата в други продукти с цифрови елементи, е вероятно попечителят да е узнал за активно използване чрез доклади от трети страни, в които се идентифицира използване в компоненти на FOSS, интегрирани в други продукти с цифрови елементи. Такъв може да бъде случаят, когато производител на продукт с цифрови елементи открие активно използване в компонент на FOSS, интегриран в неговия собствен продукт, и докладва за това на попечителя на този компонент; или когато ползвател или изследовател в областта на сигурността открие доказателства за използване на компонент на FOSS, интегриран в продукт с цифрови елементи, и докладва за това активно използване на попечителя на компонента.

217. Следва също така да се поясни, че тъй като задължението за докладване на активно използвани уязвимости се прилага, когато производителят е узнал за активно използване, производителят няма задължение да докладва за уязвимости, за чието активно използване е узнал преди 11 септември 2026 г. (датата, от която задължението за докладване започва да се прилага). Следователно АК не установява изискване за докладване с обратна сила по отношение на такива уязвимости. За разлика от това задължението се прилага, когато производителят е знаел за уязвимост преди 11 септември 2026 г., но към този момент не е знаел за активно използване на тази уязвимост (тъй като все още не е било настъпило или производителят не е бил узнал за него). Ако след 11 септември 2026 г. настъпи активно използване или производителят узнае за него, уязвимостта се счита за активно използвана и е предмет на задължението за докладване.

218. По същия начин производителят е задължен да докладва само за активно използвани уязвимости, съдържащи се в неговия продукт с цифрови елементи. Когато продукт с цифрови елементи съдържа активно използвана уязвимост, произтичаща от компонент на трета страна, производителят на продукта с цифрови елементи е задължен да нотифицира тази активно използвана уязвимост. Ако обаче производителят е узнал, че компонент на трета страна съдържа уязвимост, но тази уязвимост i) не може да бъде използвана в неговия продукт с цифрови елементи (напр. поради недостъпност на уязвимия код) или ii) не е била използвана в неговия продукт с цифрови елементи, тази уязвимост не се квалифицира като активно използвана уязвимост, съдържаща се в неговия продукт с цифрови елементи, и следователно не е предмет на задължително докладване за този производител. Производителят обаче може доброволно да нотифицира тази уязвимост в съответствие с член 15 от АК. Той също така е задължен да спазва изискванията относно отстраняването на уязвимости, определени в приложение I, част II към АК, и да докладва за уязвимостта на лицето или субекта, който произвежда или поддържа компонента, в съответствие с член 13, параграф 6 и както допълнително е обяснено в раздел *9.2.1 Докладване нагоре по веригата и споделяне на корекции за сигурност*.

([30]) Доколкото попечителят участва в разработването на съответния продукт с цифрови елементи.

219. След като е узнал за активно използвана уязвимост или сериозен инцидент, производителят също така е задължен, в съответствие с член 14, параграф 8, да информира засегнатите ползватели и, когато е целесъобразно, всички ползватели. Ако производителят не информира своевременно ползвателите, нотифицираните определени за координатори ЕРИКС могат да предоставят тази информация на ползвателите, когато това се счита за пропорционално и необходимо с цел предотвратяване или смекчаване на въздействието на уязвимостта или инцидента.

220. В съответствие с основания на риска подход, установен в АК, задължението за информиране на ползвателите по член 14, параграф 8 трябва да се прилага въз основа на рисковете и по пропорционален начин. По-конкретно предоставянето на информация за активно използвана уязвимост или сериозен инцидент не означава, че такава информация трябва да се оповестява публично или да се разкрива без ограничение. Когато е целесъобразно и с оглед на естеството на продукта с цифрови елементи, засегнатите ползватели и потенциалното въздействие на уязвимостта или инцидента, производителите могат да ограничат разкриването на подробна информация до съответните засегнати ползватели или клиенти. Това се отнася по-специално за продуктите с цифрови елементи, използвани в чувствителни или критични среди, където чрез самото публично разкриване на технически подробности може да се увеличат киберрисковете или да се улесни по-нататъшното използване.

221. След като уязвимостта бъде отстранена или смекчена по подходящ начин, разширяването на обхвата на разкриването може да бъде целесъобразно. Такъв би бил случаят, когато например с разкриването се допринася за повишаване на общата информираност или се позволява на ползвателите да проверят дали техните продукти с цифрови елементи вече не са засегнати. В такива случаи нивото на детайлност и моментът на всяко разкриване с по-голям обхват следва да останат пропорционални и да се основават на свързаните с използването остатъчни рискове, естеството на продукта с цифрови елементи и интересите на засегнатите ползватели. Освен това в съответствие с изискването съгласно приложение I, част II, точка 4 производителите публично разкриват информация за коригираните уязвимости, след като бъде предоставена актуализация за сигурност.

### 9.2. **Отстраняване на уязвимости**

#### 9.2.1. *Докладване нагоре по веригата и споделяне на корекции за сигурност*

222. Съгласно член 13, параграф 6 от АК производителите докладват за уязвимостите в интегрирани компоненти на лицето или субекта, който произвежда или поддържа съответния компонент („докладване нагоре по веригата“).

223. Производителите са задължени да докладват нагоре по веригата само по отношение на версията на компонента, която интегрират. Когато лицето или субектът, който произвежда или поддържа компонента, е установил политики за сигурност, координирано оповестяване на уязвимости или специални канали за докладване на уязвимости, производителите следва да докладват в съответствие с тях, по-специално когато киберрисковете могат да бъдат увеличени в резултат на предварително оповестяване на некоригирани уязвимости. Освен това, за да се намали тежестта за структурите по поддръжката нагоре по веригата, по-специално по отношение на проекти с отворен код, от производителите не се изисква да докладват нагоре по веригата, когато могат да потвърдят, че лицето или субектът, който произвежда или поддържа даден компонент, е узнал за съществуването на съответната уязвимост. Производителите се насърчават да предприемат разумни действия с цел избягване на подаването на дублирани доклади — например чрез проверка на публично достъпни бази данни за уязвимости, специфични за проекта препоръки за сигурност или установени системи за проследяване на проблеми, преди да извършат докладване нагоре по веригата.

224. От производителите се изисква да докладват нагоре по веригата единствено за уязвимости, които съществуват в самия интегриран компонент, а не за уязвимости, които съществуват в резултат на интеграцията между компонента и друг код, разработен от производителя, или чрез интеграцията на други компоненти. Въпреки това може да има ситуации, в които чрез интегрирането на компонент в специфичен продукт с цифрови елементи се разкриват определени поведения, взаимодействия или свързани със сигурността характеристики на този компонент, които не са били очевидни или лесно установими при изолирани условия. В такива случаи производителите се насърчават да съобщават тази информация на лицето или субекта, който произвежда или поддържа компонента, с цел стимулиране на добри практики за отстраняване на уязвимости, насочени към улесняване на ефективното отстраняване и подобряване на цялостната сигурност на екосистемата от компоненти.

225. И накрая, от производителите също не се изисква да докладват за уязвимостта нагоре по веригата, когато вече няма структура по поддръжката на компонента или когато производителят вече не разчита на първоначалната структура по поддръжката по отношение на нови версии или корекции за сигурност. Независимо от това, в такива случаи производителят се насърчава да информира ползвателите на този компонент чрез разумни алтернативни мерки като съществуващи механизми на общността (напр. списъци с адресати или заявки за отстраняване на проблем) или публични регистри с данни за уязвимости.

226. Освен това съгласно член 13, параграф 6 производителите, които са разработили изменение на софтуера за справяне с уязвимост в интегриран компонент, са задължени да споделят това изменение на софтуера („корекция за сигурност“) с лицето или субекта, който произвежда или поддържа компонента („споделяне нагоре по веригата“).

227. Когато от производителите се изисква да споделят корекция за сигурност съгласно член 13, параграф 6, корекцията следва да бъде предоставена по целесъобразност в машинночетим формат — по начин, който може лесно да бъде проверен — и интегрирана по целесъобразност от лицето или субекта, който произвежда или поддържа компонента. Когато компонентът е свободен компонент с отворен код, корекцията за сигурност следва да бъде споделена по начин, съвместим с лиценза за този компонент — например споделяне чрез същия лиценз или чрез лиценз, съгласно който структурата по поддръжката може да разпространява корекцията чрез собствен лиценз. Когато структурата по поддръжката на този компонент е установила насоки относно начина на споделяне на корекциите за сигурност, производителят следва да спазва тези насоки.

228. Въпреки това АК не установява изискване производителите да гарантират, че техните корекции за сигурност задължително се приемат от лицето или субекта, който произвежда или поддържа компонента. От тях също така не се изисква да гарантират, че тези корекции са интегрирани задължително в хранилището за код на компонента, например когато структурата по поддръжката може да предпочете различен вариант за отстраняване на проблема. По същия начин от производителите не се изисква да приемат предложена корекция, разработена от структурата по поддръжката на компонента, и могат да предпочетат да смекчат проблема по други подходящи начини.

229. В някои случаи лицето или субектът, който произвежда или поддържа компонента, може вече да е предоставил корекция за сигурност за справяне с уязвимостта, но производителят прилага различна стратегия за смекчаване (напр. чрез промяна на друга конфигурация). В такива случаи АК не изисква от производителя да споделя изменението на друга част от системата нагоре по веригата. Въпреки това производителят се насърчава да го направи, когато това може да е в подкрепа на лицето или субекта, който поддържа компонента.

9.2.2. *Уязвимости, които са вече известни и могат да бъдат използвани*

230. В съответствие с едно от съществените изисквания, определени в приложение I, част I към АК, въз основа на оценката на киберриска, посочена в член 13, параграф 2, и когато е приложимо, продуктите с цифрови елементи трябва да се предоставят на пазара без уязвимости, които са вече известни и могат да бъдат използвани.

231. Съгласно определението в член 3, параграф 41 „уязвимост, която може да бъде използвана“ означава „уязвимост, която има потенциала да бъде ефективно използвана от противник при практически оперативни условия“. Не всички уязвимости могат да бъдат използвани при практически оперативни условия, а някои уязвимости могат да бъдат използвани само при теоретични условия (напр. в лаборатория или при симулация) и/или не при условия, които биха възникнали в оперативната среда на продукт с цифрови елементи.

232. АК изисква от производителите да разполагат с подходящи политики и процедури за обработване и отстраняване на потенциални уязвимости в продукта с цифрови елементи, за които е съобщено от вътрешни или външни източници (член 13, параграф 8). Въпреки това в него не се уточнява изрично кога дадена уязвимост, която може да бъде използвана, следва да се счита за вече известна на производителя, чрез което обстоятелство се задейства задължението за спазване на това съществено изискване в момента на пускане на пазара.

233. Уязвимостта следва да се счита за вече известна, когато е включена в съответните публично достъпни бази данни за уязвимости, като например европейската база данни за уязвимости, създадена съгласно член 12, параграф 2 от Директива (ЕС) 2022/2555, или други значими бази данни за уязвимости.

234. Освен това уязвимостта може да бъде вече известна и когато производителят е узнал за нея чрез непублична информация — например чрез координирано оповестяване от изследовател в областта на сигурността или чрез свое вътрешно тестване и анализ, включително при използване на услуги, базирани на ИИ. По същия начин уязвимостта може да бъде вече известна, когато е съобщена публично и на видно място в надеждни медии, включително специализирани публикации в областта на киберсигурността или средства за масово осведомяване.

235. Въпреки това самият факт, че уязвимостта е съобщена или открита, не означава, че тя може да бъде използвана на практика или да бъде приложима по отношение на конкретния засегнат продукт с цифрови елементи. Производителят ще трябва да я проучи и да потвърди верността на такава информация и приложимостта ѝ по отношение на собствения си продукт с цифрови елементи. Съответно може да измине ограничен период от време между първия доклад относно уязвимостта и нейното потвърждаване. Както е посочено в раздел *9.1 Задължения за докладване*, акцентът следва да бъде върху своевременните действия с цел разследване и реакция.

236. Освен това задължението на производителите да спазват съществените изисквания, определени в приложение I, част I, се прилага в момента на пускане на пазара в съответствие с член 13, параграф 1. На практика е възможно нови потенциални уязвимости, които могат да бъдат използвани, да бъдат открити по време на последните етапи от жизнения цикъл на разработването на продукта с цифрови елементи, включително непосредствено преди той да бъде включен в канала за разпространение (и следователно пуснат на пазара).

237. Тъй като задължението за пускане на продукти с цифрови елементи на пазара без уязвимости, които са вече известни и могат да бъдат използвани, е основано на риска задължение, производителят трябва да прецени, въз основа на оценката на киберриска, дали продуктът с цифрови елементи може да бъде безопасно пуснат на пазара в съответствие с АК. Възможно е също така производителят да прецени, че е необходимо да се коригира нова уязвимост, която може да е станала вече известна, преди продуктът с цифрови елементи да бъде пуснат на пазара. При вземането на това решение производителите следва да вземат предвид критичната значимост, степента на използване и потенциалното въздействие на уязвимостта и рисковете, произтичащи за самия продукт с цифрови елементи след въвеждането му в употреба. Те могат също така да вземат предвид рисковете, свързани с отлагането на пускането на продукта, докато уязвимостта не бъде отстранена, например поради факта, че в новата версия също така са отстранени други уязвимости, които могат да бъдат използвани, или че новата версия е необходима за непрекъснатото функциониране на критични системи. Задължението на производителя за ефективно отстраняване на уязвимости в съответствие с изискванията относно отстраняването на уязвимости, определени в приложение I, част II, се прилага във всички случаи след пускането на пазара на продукт с цифрови елементи.

9.2.3. *Ефективни и редовни проверки и прегледи*

238. В съответствие с приложение I, част II, точка 3 производителите изпълняват ефективни и редовни проверки и прегледи на сигурността на продукта с цифрови елементи през целия му период на поддръжка. За извършването на редовни проверки не се изисква механично повторение на непроменена кампания за изпитване през фиксирани интервали. То представлява редовен преглед с цел установяване дали е необходимо, в резултат на нови входящи данни като новоидентифицирани заплахи или новооткрити уязвимости, да се актуализират съществуващите изпитвания и съответно да се извършват изпитвания.

239. Честотата, обхватът и съдържанието на прегледа следва да бъдат пропорционални на киберрисковия профил на продукта с цифрови елементи и неговото развитие във времето и контекста на заплахите. Когато в хода на прегледа се идентифицират значими нови входящи данни, които засягат набора от изпитвания, следва да се разработят или извършат нови или изменени изпитвания на продукта с цел гарантиране, че няма останали неотстранени уязвимости. Това може да включва повторно изпълнение на съществуващи изпитвания, когато такива изпитвания са подходящи с оглед естеството на дадено изменение на продукта с цифрови елементи, като например регресионно изпитване.

240. Когато в хода на прегледа не бъдат идентифицирани такива входящи данни, не е необходимо да се разработват допълнителни изпитвания. Другите задължения за отстраняване на уязвимости, включително задълженията за третиране и отстраняване на уязвимости във връзка с възникналите рискове, се прилагат паралелно.

9.3. **Взаимодействие с други законодателни актове**

9.3.1. *Регламент (ЕС) 2019/2144 и Регламент (ЕС) № 168/2013*

241. В съответствие с член 2, параграф 2 от АК регламентът не се прилага за продукти с цифрови елементи, за които се прилага Регламент (ЕС) 2019/2144. Регламент (ЕС) 2019/2144 се прилага за „превозни средства от категории M, N и O, съгласно определеното в член 4 от Регламент (ЕС) 2018/858, както и за системи, компоненти и отделни технически възли, проектирани и конструирани за такива превозни средства“.

242. По същия начин продуктите с цифрови елементи, попадащи в приложното поле на Регламент (ЕС) № 168/2013, са изключени от обхвата на АК с Делегиран регламент (ЕС) 2025/1535 на Комисията. Регламент (ЕС) 168/2013 се прилага за превозни средства от категория L и „за системи, компоненти и отделни технически възли, проектирани и конструирани за такива превозни средства“ (член 2, параграф 1).

243. Превозните средства, за които се прилагат тези регламенти, не са предмет на АК. Освен това са необходими допълнителни разяснения по отношение на обхвата на изключението за системи, компоненти, отделни технически възли, части и оборудване (наричани „компонентите“ за целите на настоящия раздел), проектирани и конструирани за такива превозни средства, които се считат за продукти с цифрови елементи по смисъла на АК.

244. Счита се, че такива компоненти не са предмет на АК, при условие че са проектирани и конструирани единствено с цел интегриране в превозни средства, обхванати от Регламенти (ЕС) 2019/2144 и № 168/2013. Това се отнася за всички случаи, независимо дали производителят на този компонент го продава директно на производителя на превозното средство, или на друг икономически оператор във веригата на доставки в автомобилната промишленост, ако компонентът е ясно предназначен и подходящ единствено за крайно интегриране в тези превозни средства.

245. За разлика от това производител, който продава общи компоненти, представляващи продукти с цифрови елементи, които могат да бъдат интегрирани в различни видове продукти, а не единствено в обхванатите от тези регламенти превозни средства, попада в обхвата на АК.

246. Преценката дали даден компонент се пуска на пазара по смисъла на АК трябва да се основава на обективните условия, при които той се предоставя. Когато производител предлага компонент, който е подходящ не само за интегриране в такива превозни средства, чрез канали за разпространение, които са достъпни за клиенти извън веригата на доставки в автомобилната промишленост, като например обекти за търговия на дребно от общата мрежа или канали за онлайн продажби, чрез които се приемат поръчки от обществеността, този компонент попада в обхвата на АК, независимо от всички изявления относно предвидената му употреба. При такива обстоятелства компонентът не може да се счита за проектиран и конструиран единствено с цел интегриране в превозни средства, обхванати от Регламенти (ЕС) 2019/2144 и № 168/2013, и производителят е задължен да спазва АК. За разлика от това използването на ограничени канали за разпространение между предприятия, достъпни единствено в рамките на веригата на доставки в автомобилната промишленост, може да е индикатор, че той е проектиран и конструиран единствено за такова интегриране.

9.3.2. *Валидност на сертификатите за ЕС изследване на типа (член 69, параграф 1)*

247. Съгласно член 69, параграф 1 от АК „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 11 юни 2028 г., 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“.

248. Непрекъснатата валидност на такива сертификати и решения за одобрение следва да се разбира като ограничена до киберрисковете и приложимите изисквания, които са обхванати от съответното законодателство на Съюза за хармонизация, въз основа на което са издадени. По отношение на тези рискове производителите не са задължени повторно да оценяват или доказват съответствието единствено за целите на АК по време на периода на валидност, посочен в член 69, параграф 1, за продукти с цифрови елементи, които възнамеряват да пуснат на пазара през периода 11 декември 2027 г.—11 юни 2028 г. ([31]) Това се отнася за сертификати и решения, издавани в случаите, когато приложимото законодателство на Съюза за хармонизация изисква от производителя да извърши процедурата за оценяване на съответствието чрез нотифициран орган, както и когато производителят доброволно е избрал да направи това.

249. Съответно производителите не се освобождават от задължението за извършване на цялостна оценка на киберриска съгласно АК (или от други задължения по него) въз основа на наличието на валиден сертификат или решение за одобрение съгласно друго законодателство на Съюза за хармонизация. Вместо това с такъв документ им се предоставя възможност да се позоват на съществуващо сертифициране като доказателство за съответствие по отношение на тяхната процедура за оценяване на съответствието в степента, в която съответните киберрискове вече са обхванати. Когато обаче срокът на валидност на сертификата или решението за одобрение съгласно друго законодателство на Съюза за хармонизация изтича след 11 юни 2028 г., производителят може да се позовава на такъв сертификат или решение за целите на АК само до 11 юни 2028 г.

250. Когато при извършването на оценката на киберриска съгласно член 13, параграф 2 бъдат установени допълнителни рискове, които не са обхванати от изискванията за киберсигурност, залегнали в основата на съществуващия сертификат или решение за одобрение, производителите продължават да носят отговорност за справянето с тези рискове в съответствие с АК. В такива случаи се изисква, за целите на съответствието, установените пропуски да бъдат оценени и смекчени, независимо от факта, че съществуващият сертификат или решение за одобрение все още е валидно.

251. Това може да бъде илюстрирано със случая, при който продукт с цифрови елементи е предмет на изискванията за киберсигурност, установени в Делегиран регламент (ЕС) 2022/30 на Комисията за допълнение на Директива 2014/53/ЕС (Делегирания акт относно Директивата за радиосъоръженията (ДРС)), и е издаден сертификат за ЕС изследване на типа или решение за одобрение въз основа на тези изисквания. В този случай сертификатът или решението за одобрение продължава да бъде валидно в съответствие с член 69, параграф 1 по отношение на обхванатите в него киберрискове, които са свързани със съществените изисквания за киберсигурност, установени в Директива 2014/53/ЕС (Директивата за радиосъоръженията или ДРС).

252. В такива случаи производителите не са задължени, за целите на АК, повторно да оценяват или доказват съответствието по отношение на тези рискове, които вече са обхванати от тези сертификати, докато съответният сертификат или решение за одобрение продължава да бъде валидно и, при всички случаи, до 11 юни 2028 г. Това включва например киберрискове, свързани със защитата на мрежата, защитата на личните данни и неприкосновеността на личния живот или предотвратяването на измами (доколкото тези рискове са обхванати от този сертификат), свързани със съществените изисквания за киберсигурност, установени в ДРС, и отразени в оценката на съответствието.

253. Когато обаче при извършването на оценката на киберриска съгласно член 13, параграф 2 от АК бъдат установени допълнителни киберрискове, които не са обхванати от тези сертификати, производителите продължават да носят отговорност за справянето с тези рискове в съответствие с АК. Това може да включва например рискове, свързани с процесите за отстраняване на уязвимости, свеждането на данните до минимум и ограничаването на повърхностите, уязвими за атаки, или други специфични за продукта аспекти на киберсигурността, които не са обхванати от тези сертификати или, при всички случаи, не са предмет на съществените изисквания за киберсигурност, установени в ДРС.

254. Съответно самото наличие на валиден сертификат за ЕС изследване на типа или решение за одобрение съгласно ДРС въз основа на установените в нея съществени изисквания за киберсигурност не съставлява доказателство за пълно съответствие с АК. Вместо това с такъв документ се предоставя възможност на производителите да се позоват на този сертификат или решение за одобрение като доказателство за съответствие по отношение на съответните рискове, като същевременно гарантират, че всички други или новоустановени рискове се оценяват и смекчават в съответствие с АК.

([31]) Продуктите с цифрови елементи, пуснати на пазара преди 11 декември 2027 г., са предмет на законодателството на Съюза, приложимо към момента на тяхното пускане на пазара, и, ако са били в съответствие, те могат да бъдат продавани и въвеждани в експлоатация, освен ако не бъдат подложени на съществени изменения на 11 декември 2027 г. или след това. За по-подробна информация относно понятието „пускане на пазара“ и „предоставяне на пазара“ вж. също раздел *2.1 Пускане на пазара* от настоящия документ, както и глава 2 от Синьото ръководство.

255. По същия начин, когато продукт с цифрови елементи е предмет на свързаните с киберсигурността съществени изисквания за безопасност и опазване на здравето, установени в Регламент (ЕС) 2023/1230 (Регламента относно машините), който се прилага изцяло от 20 януари 2027 г., и е издаден сертификат за ЕС изследване на типа или решение за одобрение въз основа на тези изисквания, този сертификат или решение за одобрение остава валидно в съответствие с член 69, параграф 1 от АК по отношение на киберрисковете, обхванати от Регламента относно машините.

256. По-конкретно това се отнася до аспектите на киберсигурността, свързани със защитата срещу увреждане и безопасността и надеждността на системите за управление, както е посочено в раздели 1.1.9 и 1.2.1 от приложение III към Регламента относно машините. По отношение на тези рискове производителите не са задължени, за целите на АК, повторно да оценяват или доказват съответствието, докато съответният сертификат или решение за одобрение продължава да бъде валидно и, при всички случаи, до 11 юни 2028 г. Това се прилага, доколкото тези рискове са разгледани като част от оценката на съответствието съгласно Регламента относно машините.

257. Както и при споменатите по-горе съществени изисквания за киберсигурност, установени в ДРС, когато при извършването на оценката на киберриска съгласно член 13, параграф 2 от АК бъдат установени допълнителни киберрискове, които не са обхванати от съответния сертификат, издаден в съответствие с Регламента относно машините, и които са свързани със свързаните с киберсигурността съществени изисквания за безопасност и опазване на здравето, установени в същия регламент, производителите продължават да носят отговорност за справянето с тези рискове в съответствие с АК.