2025/2392

1.12.2025 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2025/2392 НА КОМИСИЯТА

от 28 ноември 2025 година

относно техническото описание на категориите важни и критични продукти с цифрови елементи съгласно Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид 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]), и по-специално член 7, параграф 4 от него,

като има предвид, че:

(1) С Регламент (ЕС) 2024/2847 се определят правила относно киберсигурността на продуктите с цифрови елементи. По-специално, в приложение III към посочения регламент са определени категориите важни продукти с цифрови елементи, които при пускането си на пазара подлежат на процедури за оценка на съответствието, които са по-строги от тези, приложими за други продукти с цифрови елементи. В приложение IV към Регламент (ЕС) 2024/2847 са определени категориите критични продукти с цифрови елементи, за които производителите могат да бъдат задължени да получат европейски сертификат за киберсигурност съгласно европейска схема за сертифициране на киберсигурността в съответствие с Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета ([2]) или които подлежат на задължителна оценка на съответствието от трета страна, когато се пускат на пазара.

(2) Съгласно член 7, параграф 1 и член 8, параграф 1 от Регламент (ЕС) 2024/2847 основната функционална възможност на продукт с цифрови елементи определя дали този продукт с цифрови елементи отговаря на техническото описание на категория важни или критични продукти с цифрови елементи и следователно на приложимите процедури за оценяване на съответствието.

(3) При разработването на продукт с цифрови елементи и с цел да постигнат желания набор от функционални възможности, производителите обикновено интегрират в своите продукти с цифрови елементи други компоненти, които също са продукти с цифрови елементи и които могат да отговарят на техническото описание на категория важни или критични продукти. Съгласно Регламент (ЕС) 2024/2847 всеки продукт с цифрови елементи подлежи на процедурите за оценяване на съответствието, приложими за важни или критични продукти с цифрови елементи, ако този продукт като цяло е важен или критичен продукт, както е определено в приложения III и IV към посочения регламент. Например интегрирането на вграден браузър като компонент на приложение за новини за използване в смартфони само по себе си не прави приложението за новини обект на процедурата за оценяване на съответствието, приложима за продукти с цифрови елементи, чиято основна функционална възможност е „отделни и вградени браузъри“. Въпреки това, в съответствие с Регламент (ЕС) 2024/2847, производителят трябва да гарантира, че продуктът с цифрови елементи като цяло отговаря на основните изисквания за киберсигурност. Поради това производителят трябва да оцени сигурността на целия продукт, като при необходимост вземе предвид сигурността на компонентите или функционалните възможности, които са интегрирани в него. Например, за да докаже, че неговият продукт с цифрови елементи е в съответствие с Регламент (ЕС) 2024/2847, производителят на приложение за новини трябва да докаже, че приложението за новини като цяло отговаря на приложимите изисквания, като при необходимост вземе предвид сигурността на вградения браузър, който е интегриран в приложението.

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

([2]) Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019 г., стр. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) Фактът, че продукт с цифрови елементи изпълнява функции, различни от или допълнителни към тези, подробно описани в техническите описания, изложени в настоящия регламент, сам по себе си не означава, че продуктът с цифрови елементи не притежава основната функционална възможност на продуктова категория, определена в приложения III и IV към Регламент (ЕС) 2024/2847. Например продуктите с цифрови елементи, чиято основна функционална възможност е „операционни системи“, често включват софтуер, който изпълнява спомагателни функции, които не са включени в техническото описание на тази продуктова категория, като калкулатори или прости графични редактори. Продуктите с цифрови елементи често включват и компоненти, които имат функционалната възможност на друг важен или критичен продукт с цифрови елементи, като например операционна система, интегрираща функционалната възможност на браузър, или маршрутизатор, интегриращ функционалната възможност на защитна стена. Това само по себе си обаче не означава, че такива продукти с цифрови елементи не притежават основната функционална възможност съответно на „операционни системи“ или „маршрутизатори, модеми, предназначени за връзка с интернет, и комутатори“.

(5) От друга страна, продукт с цифрови елементи, който има способността да изпълнява функциите на дадена продуктова категория, посочена в приложения III и IV към Регламент (ЕС) 2024/2847, но чиято основна функционална възможност е различна от тази на въпросната продуктова категория, не се счита за отговарящ на техническото описание на тази продуктова категория. Например 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, да ги анализира и да ги представя като полезна информация за целите на сигурността. Въпреки това, тъй като основната му функционална възможност не е тази на SIEM, софтуерът SOAR по принцип не се счита за отговарящ на техническото описание на „системите за управление на информацията за безопасност и на събитията, свързани със сигурността (SIEM)“. По същия начин смартфонът обикновено интегрира компоненти, които изпълняват функциите на няколко продуктови категории, посочени в приложения III и IV към Регламент (ЕС) 2024/2847, като например операционна система или интегриран мениджър на пароли. Въпреки това, тъй като основната функционална възможност на смартфона не е тази на операционна система или на мениджър на пароли, по принцип не се счита за отговарящ на техническото описание на такива категории продукти.

(6) Съгласно член 13, параграфи 2 и 3 от Регламент (ЕС) 2024/2847 производителите на продукти с цифрови елементи трябва да прилагат съществените изисквания за киберсигурност, определени в част I от приложение I към Регламент (ЕС) 2024/2847, по начин, който е пропорционален на рисковете, свързани с продукта с цифрови елементи, въз основа на предназначението и разумно предвидимата употреба, както и на условията за употреба на продукта с цифрови елементи, като се взема предвид продължителността, през която се очаква продуктът да бъде в употреба. В съответствие с член 13, параграфи 2 и 3 от същия регламент и независимо от това дали продуктът с цифрови елементи се счита за важен или критичен продукт с цифрови елементи, производителите трябва да извършат цялостна оценка на риска за киберсигурността и да посочат как се прилагат съществените изисквания за киберсигурност, както е вписано в оценката на риска, включително тяхното изпитване и ниво на увереност. Когато основната функционална възможност на техния продукт с цифрови елементи отговаря на техническото описание на важен или критичен продукт с цифрови елементи, производителите трябва да докажат съответствие, като следват специфичните процедури за оценяване на съответствието, установени в член 32, параграфи 2, 3, 4 и 5 от Регламент (ЕС) 2024/2847.

(7) Настоящият регламент включва примери за продукти с цифрови елементи, чиято основна функционална възможност отговаря на техническото описание на определени важни или критични продукти с цифрови елементи. Тези примери са дадени само с цел онагледяване и не представляват изчерпателен списък.

(8) С цел да се осигури правна сигурност на производителите, категориите продукти с цифрови елементи, а именно — защитени от външна намеса микропроцесори, защитени от външна намеса микроконтролери и смарт карти и подобни устройства, включително защитени елементи — следва да се разграничават въз основа на нивото на устойчивост срещу потенциална възможност за използване на недостатъци или слабости, за което са проектирани. Нивото AVA_VAN е широко използван и стандартизиран начин за изразяване на такова ниво на устойчивост. Нивата на AVA_VAN са определени в обществено достъпните стандарти за общи критерии и обща методика за оценка, които са в основата на съществуващите рамки за сертифициране, широко приети на пазара, като например Регламент за изпълнение (ЕС) 2024/482 на Комисията ([3]). В Регламент за изпълнение (ЕС) 2024/482 е установена европейска схема

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

за сертифициране на киберсигурността, която може да се използва за сертифициране на продукт на определено ниво на увереност. Въз основа на световните практики, в Регламент за изпълнение (ЕС) 2024/482 се предвижда възможността до края на 2027 г. да се издават сертификати въз основа на по-стари версии на стандартите. Следователно в контекста на Регламент (ЕС) 2024/2847 е целесъобразно да се даде възможност нивата на AVA_VAN да бъдат изразени чрез позоваване на последната версия или на по-старите версии на тези стандарти.

(9) Мерките, предвидени в настоящия регламент, са в съответствие със становището на комитета, създаден съгласно член 62, параграф 1 от Регламент (ЕС) 2024/2847,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Определения

За целите на настоящия регламент се прилагат следните определения:

1) „общи критерии“ означава общите критерии за оценка на сигурността на информационните технологии, както са определени в член 2, параграф 1 от Регламент за изпълнение (ЕС) 2024/482 или както са определени в стандартите, посочени в член 3, параграф 2, букви а) и б) от същия регламент за изпълнение;

2) „обща методика за оценка“ означава общата методика за оценка на сигурността на информационните технологии, както е определена в член 2, параграф 2 от Регламент за изпълнение (ЕС) 2024/482 или както е определена в стандартите, посочени в член 3, параграф 2, букви в) и г) от същия регламент за изпълнение.

Член 2

1. Техническото описание на категориите продукти с цифрови елементи от класове I и II, изброени в приложение III към Регламент (ЕС) 2024/2847 , е като посоченото в приложение I към настоящия регламент.

2. Техническото описание на категориите продукти с цифрови елементи, изброени в приложение IV към Регламент (ЕС) 2024/2847, е като посоченото в приложение II към настоящия регламент.

Член 3

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

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

Съставено в Брюксел на 28 ноември 2025 година.

За Комисията
Председател
Ursula VON DER LEYEN

ПРИЛОЖЕНИЕ I

ВАЖНИ ПРОДУКТИ С ЦИФРОВИ ЕЛЕМЕНТИ

Клас I

Категория на продуктите	Техническо описание
1. Системи за управление на самоличността и софтуер и хардуер за управление на привилегирован достъп, включително четци за автентификация и контрол на достъпа, включително биометрични четци	Системите за управление на самоличността са продукти с цифрови елементи, които предоставят механизми за автентификация или предоставяне на разрешение и които могат също да осигурят механизми за управление на жизнения цикъл на идентификационните данни на физически лица, юридически лица, устройства или системи, като регистрация, предоставяне, поддържане, дерегистрация. Тези системи включват системи за управление на достъпа, които контролират достъпа на физически лица, юридически лица, устройства или системи до цифрови ресурси или физически местоположения. Софтуерът за управление на привилегирован достъп е система за управление на достъпа, която контролира и наблюдава правата за достъп до системи за ИТ или ОТ, и чувствителна информация в рамките на дадена организация, включително системи, които прилагат диференцирани политики за контрол на достъпа за привилегировани потребители. Тази категория включва, но не се ограничава само до четци за автентификация и контрол на достъпа, биометрични четци, софтуер за единна автентификация, софтуер за интегрирано управление на самоличността, софтуер за еднократни пароли, хардуерни устройства за автентификация, като генератори на еднократни кодове за удостоверяване на трансакции (TAN), софтуер за автентификация и софтуер за двуфакторна автентикация.
2. Отделни и вградени браузъри	Софтуерни продукти с цифрови елементи, които позволяват на крайните потребители да имат достъп, да визуализират и да взаимодействат с уебсъдържание и услуги, хоствани на сървъри, свързани с мрежи като интернет. Те обикновено включват уеб браузър за интерпретиране и показване на съдържание, написано на маркиращ език (напр. HTML), поддръжка на уеб протоколи (напр. HTTP, HTTPS), възможност за изпълнение на скриптове и управление на потребителски входни данни, както и съхранение на временни или постоянни данни от уебсайтове (бисквитки). Тази категория включва, но не се ограничава само до отделни приложения, които изпълняват функциите на браузъри, вградени браузъри, предназначени за интегриране в друга система или приложение, както и браузъри с интегриран AI агент.
3. Мениджъри на пароли	Продукти с цифрови елементи, които съхраняват пароли локално на устройство или на отдалечен сървър, включително дейности като генериране на пароли, както и споделяне на пароли и интеграция с локални или външни приложения за използване на пароли. Тази категория включва, но не се ограничава само до локални мениджъри на пароли, мениджъри на пароли, предоставяни като разширения за браузъри, корпоративни мениджъри на пароли, както и мениджъри на пароли, базирани на хардуер.

Категория на продуктите	Техническо описание
4. Софтуер, който търси, премахва или поставя под карантина зловреден софтуер	Софтуерни продукти с цифрови елементи, обикновено наричани антивирусни или антималуерни, които откриват или търсят зловреден софтуер или код на устройства, или премахват или поставят под карантина такъв софтуер или код, с цел да поддържат целостта, поверителността или достъпността на такива устройства. В контекста на тази категория продукти, зловреден софтуер означава софтуер, съдържащ зловредни функции или възможности, които могат да причинят пряка или непряка вреда на потребителя и/или компютърната система, като вируси, компютърни червеи, софтуер за изнудване, шпионски софтуер и троянски коне. Тази категория включва, но не се ограничава само до софтуер, който открива или търси зловреден софтуер в реално време или ръчно, откриване на руткитове и спасителни дискове с основна функционална възможност за търсене, премахване или карантина на зловреден софтуер.
5. Продукти с цифрови елементи с функцията виртуална частна мрежа (VPN)	Продукти с цифрови елементи, които създават криптиран логически тунел, изграден от системните ресурси на физическа или виртуална мрежа. Тази категория включва, но не се ограничава само до клиенти на виртуални частни мрежи, сървъри на виртуални частни мрежи и шлюзове на виртуални частни мрежи.
6. Системи за управление на мрежата	Продукти с цифрови елементи, които управляват свързани мрежови елементи, като сървъри, маршрутизатори, комутатори, работни станции, принтери или мобилни устройства чрез наблюдение и контрол на тяхната мрежова работа и конфигурация. Тази категория включва, но не се ограничава само до системи за управление от край до край и специализирани системи за управление на конфигурацията, като например контролери за софтуерно дефинирани мрежи.
7. Системи за управление на информацията за безопасност и на събитията, свързани със сигурността (SIEM)	Продукти с цифрови елементи, които събират данни от различни източници, анализират и съпоставят тези данни и ги представят като полезна информация за целите на сигурността, като например откриване на заплахи и инциденти, съдебно-техническа експертиза или спазване на нормативните изисквания.
8. Мениджъри за зареждане	Софтуерни продукти с цифрови елементи, които управляват процеса на първоначално стартиране на системата след включване/рестартиране чрез инициализиране на хардуера, качване или прехвърляне на контрола към операционната система или системните ресурси и избор на опции за зареждане. Тази категория включва, но не се ограничава само до микропрограмно осигуряване (фърмуер) по стандарта UEFI, едностепенни и многостепенни зареждащи програми.
9. Инфраструктура на публичния ключ и софтуер за издаване на електронни сертификати	Продукти с цифрови елементи, използвани като част от инфраструктура на публичен ключ (PKI), които управляват валидирането, създаването, издаването, разпространението, публикуването на статуса, подновяването или отмяната на цифрови сертификати, или генерирането, съхранението, доверителното съхранение на ключ, обмена, унищожаването или ротацията на криптографски ключове, свързани с такива цифрови сертификати. Тази категория включва, но не се ограничава само до системи за управление на ключове, системи за управление на цифрови сертификати, респондери по онлайн протокола за статус на сертификат (OCSP) и интегрирани PKI решения.

Категория на продуктите	Техническо описание
10. Физически и виртуални мрежови интерфейси	Физическите мрежови интерфейси са продукти с цифрови елементи, които свързват директно устройство към мрежа чрез приложно-програмен интерфейс (API), предоставен от драйверите на интерфейса, обикновено работещи на ниво канален слой, и които разполагат с хардуерни адаптери към предавателна среда с микропрограмно осигуряване, обикновено работещи на физическо ниво и ниво канален слой. Виртуалните мрежови интерфейси са продукти с цифрови елементи, които пряко или непряко свързват устройство към мрежа чрез API, който емулира този на драйверите на физически мрежови интерфейси, обикновено работещи на ниво канален слой. Тази категория включва, но не се ограничава само до кабелни и безжични мрежови интерфейсни карти, контролери и адаптери, като например за Wi-Fi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee или Fieldbus, както и изцяло виртуални отделни продукти, като виртуални мрежови интерфейсни карти, контейнерни мрежови интерфейси и VPN интерфейси.
11. Операционни системи	Софтуерни продукти с цифрови елементи, които предоставят абстрактен интерфейс на основния хардуер и управляват изпълнението на софтуера, и които могат да предоставят услуги като управление и конфигуриране на изчислителни ресурси, планиране на задачи, контрол на входно-изходни операции, управление на данни и осигуряване на интерфейс, чрез който приложенията взаимодействат със системните ресурси и периферните устройства. Тази категория включва, но не се ограничава само до операционни системи в реално време, операционни системи с общо предназначение и специализирани операционни системи.
12. Маршрутизатори, модеми, предназначени за връзка с интернет, и комутатори	Маршрутизаторите са продукти с цифрови елементи, които установяват и контролират потока от данни между различни мрежи, като избират пътища или маршрути, използвайки механизми и алгоритми на протоколи за маршрутизиране, които обикновено функционират на мрежово ниво. Тази категория включва, но не се ограничава само до кабелни и безжични маршрутизатори, виртуални маршрутизатори и маршрутизатори с модеми или без модеми.
	Модемите, предназначени за свързване с интернет, са хардуерни продукти с цифрови елементи, които използват техники за цифрова модулация и демодулация за преобразуване на аналогови сигнали в цифрови и обратно с цел комуникация, базирана на IP протокол. Тази категория включва, но не се ограничава само до оптични модеми, модеми по цифрова абонатна линия (DSL), кабелни модеми (DOCSIS), сателитни модеми и клетъчни модеми.
	Комутаторите са продукти с цифрови елементи, които осигуряват свързаност между мрежови устройства чрез механизми за препращане на пакети и притежават равнина за управление, която обикновено е реализирана на канално или мрежово ниво. Тази категория включва, но не се ограничава само до управляеми комутатори, интелигентни комутатори, многослойни комутатори, виртуални комутатори за сигурност, програмируеми комутатори за софтуерно дефинирани мрежи и мостове, като например безжични точки за достъп.

ELI: http://data.europa.eu/eli/reg_impl/2025/2392/oj

Категория на продуктите	Техническо описание
13. Микропроцесори с функционални възможности, свързани със сигурността	Продукти с цифрови елементи, които представляват интегрални схеми, изпълняващи функции на централен процесор, разчитащи на външна памет и периферни устройства, включително микрокод и друго микропрограмно осигуряване на ниско ниво. Те допълнително осигуряват функции, свързани със сигурността, като криптиране, автентификация, сигурно съхранение на ключове, генериране на случайни числа, надеждна среда за изпълнение или други хардуерни механизми за защита, които имат за цел да осигурят сигурността на други продукти, мрежи или услуги извън самия микропроцесор, като сигурно зареждане, виртуализация или сигурен комуникационен интерфейс.
14. Микроконтролери с функционални възможности, свързани със сигурността	Продукти с цифрови елементи, които представляват интегрални схеми, изпълняващи функции на централен процесор, интегриращи памет, която позволява на микроконтролера да бъде програмируем, а обикновено също и други периферни устройства, включително микрокод и друго микропрограмно осигуряване на ниско ниво. Те допълнително осигуряват функционални възможности, свързани със сигурността, като криптиране, удостоверяване на автентичността, сигурно съхранение на ключове, генериране на случайни числа, надеждна среда за изпълнение или други хардуерни механизми за защита, които имат за цел да осигурят сигурността на други продукти, мрежи или услуги извън самия микроконтролер, като сигурно зареждане, виртуализация или сигурен комуникационен интерфейс.
15. Интегрални схеми, специфични за приложенията (ASIC), и програмируеми логически матрици (FPGA) с функционални възможности, свързани със сигурността	Интегралните схеми, специфични за приложенията (ASIC), с функционални възможности, свързани със сигурността, са продукти с цифрови елементи, които са интегрални схеми, изцяло или частично проектирани по поръчка, за да изпълняват конкретна функция или да реализират конкретно приложение, включително микрокод и друго микропрограмно осигуряване на ниско ниво. Те допълнително осигуряват функционални възможности, свързани със сигурността, като криптиране, удостоверяване на автентичността, сигурно съхранение на ключове, генериране на случайни числа, надеждна среда за изпълнение или други хардуерни механизми за защита, които имат за цел да осигурят сигурността на други продукти, мрежи или услуги извън самата ASIC, като сигурно зареждане, виртуализация или сигурен комуникационен интерфейс.
	Програмируемите логически матрици (FPGA) с функционални възможности, свързани със сигурността, са продукти с цифрови елементи, които са интегрални схеми, характеризиращи се с матрица от конфигурируеми логически блокове, проектирани да бъдат препрограмирани след производството, за да изпълняват конкретна функция или да реализират конкретно приложение, включително микрокод и друго микропрограмно осигуряване на ниско ниво. Те допълнително осигуряват функционални възможности, свързани със сигурността, като криптиране, удостоверяване на автентичността, сигурно съхранение на ключове, генериране на случайни числа, надеждна среда за изпълнение или други хардуерни механизми за защита, които имат за цел да осигурят сигурността на други продукти, мрежи или услуги извън самата FPGA, като сигурно зареждане, виртуализация или сигурен комуникационен интерфейс.
16. Виртуални асистенти с общо предназначение за интелигентни домове	Продукти с цифрови елементи, които комуникират пряко или чрез друго оборудване в публичната интернет мрежа, които обработват заявки, задачи или въпроси въз основа на команди на естествен език, например чрез аудио или писмено въвеждане, и които въз основа на тези заявки, задачи или въпроси осигуряват достъп до други услуги или контролират функциите на свързани устройства в жилищни помещения. Тази категория включва, но не се ограничава само до интелигентни високоговорители с вграден виртуален асистент и отделни виртуални асистенти, които отговарят на това описание.

Категория на продуктите	Техническо описание
17. Продукти за интелигентни домове с функции за сигурност, включително интелигентни ключалки за врати, камери за сигурност, системи за наблюдение на бебето и алармени системи	Продукти с цифрови елементи, които защитават физическата сигурност на потребителите в жилищна среда и които могат да се контролират или управляват дистанционно от други системи, както и хардуер и софтуер, които централизирано контролират такива продукти. Тази категория включва, но не се ограничава само до интелигентни устройства за заключване на врати, системи за наблюдение на бебета, алармени системи и камери за домашна сигурност.
18. Свързани с интернет играчки, обхванати от Директива 2009/48/ЕО на Европейския парламент и на Съвета ([1]), които имат социални интерактивни характеристики (напр. говорене или заснемане) или които имат функции за проследяване на местоположението	Свързаните с интернет играчки, които имат социални интерактивни характеристики, са продукти с цифрови елементи, които са обхванати от Директива 2009/48/ЕО, които пряко или чрез друго оборудване комуникират в публичния интернет и които имат вградени технологии, позволяващи входяща и изходяща комуникация, като клавиатура, микрофон, високоговорител или камера.
	Свързаните с интернет играчки, които имат функции за проследяване на местоположението, са продукти с цифрови елементи, които са обхванати от Директива 2009/48/ЕО, които пряко или чрез друго оборудване комуникират в публичния интернет и които разполагат с технологии, позволяващи проследяване или определяне на географското местоположение на играчката или нейния потребител. Когато играчката просто засича намиращите се в близост потребител или други играчки чрез използване на сензорни технологии, тя не се счита за играчка с функции за проследяване на местоположението.
19. Лични устройства за прикрепване към тялото, предназначени да се носят или поставят върху човешкото тяло с цел наблюдение на здравето (например проследяване) и за които не се прилага нито Регламент (ЕС) 2017/745 ([2]), нито Регламент (ЕС) 2017/746 на Европейския парламент и на Съвета ([3]), или лични устройства за прикрепване към тялото, предназначени за употреба от и за деца	Личните продукти за прикрепване към тялото, които се носят или поставят върху човешкото тяло и имат за цел наблюдение на здравето, са продукти с цифрови елементи, които се носят директно върху тялото или чрез облекло или аксесоари и които могат редовно или непрекъснато да възприемат и обработват информация, включително телесни показатели, свързани със здравето на потребителя, с изключение на продуктите, които попадат в обхвата на Регламент (ЕС) 2017/745 или на Регламент (ЕС) 2017/746. Тази категория включва, но не се ограничава само до фитнес тракери, смарт часовници, смарт бижута, смарт облекло и спортни дрехи, които отговарят на това описание.
	Личните продукти за прикрепване към тялото, предназначени за употреба от и за деца, са продукти с цифрови елементи, които могат да се носят или поставят върху тялото, директно или чрез облекло или аксесоари, на лица на възраст под 14 години. Тази категория включва, но не се ограничава само до устройства за прикрепване към тялото с цел безопасност на децата.

([1]) Директива 2009/48/ЕО на Европейския парламент и на Съвета от 18 юни 2009 г. относно безопасността на детските играчки (ОВ L 170, 30.6.2009 г., стр. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Регламент (ЕС) 2017/745 на Европейския парламент и на Съвета от 5 април 2017 г. за медицинските изделия, за изменение на Директива 2001/83/ЕО, Регламент (ЕО) № 178/2002 и Регламент (ЕО) № 1223/2009 и за отмяна на директиви 90/385/ЕИО и 93/42/ЕИО на Съвета (ОВ L 117, 5.5.2017 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Регламент (ЕС) 2017/746 на Европейския парламент и на Съвета от 5 април 2017 г. за медицинските изделия за *инвитро* диагностика и за отмяна на Директива 98/79/ЕО и Решение 2010/227/ЕС на Комисията (ОВ L 117, 5.5.2017 г., стр. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

Клас II

Категория на продуктите	Техническо описание
1. Хипервайзори и системи за изпълнение на контейнери, които поддържат виртуализация на операционни системи и подобни среди	Хипервайзорите са софтуерни продукти с цифрови елементи, които отделят и/или разпределят изчислителни ресурси и позволяват изпълнението, управлението и оркестрирането на виртуални машини, които са логически отделени една от друга и/или от физическия хардуер. Хипервайзорите могат да работят директно върху хардуер, върху операционна система или в рамките на друга виртуална машина (вложени виртуализации). В контекста на тази категория продукти виртуална машина е софтуерно дефинирана логическа сегментация, която включва виртуализиран набор от хардуерни ресурси (напр. процесор, памет, хранилище, мрежови интерфейси) и обикновено хоства собствена операционна система. Тази категория включва, но не се ограничава само до хипервайзори от тип 1 (хардуер), хипервайзори от тип 2 (хоствани на операционна система) и хибридни хипервайзори.
	Системите за изпълнение на контейнери са софтуерни продукти с цифрови елементи, които управляват изпълнението и жизнения цикъл на контейнери, работещи на една хостваща операционна система като изолирани процеси, като разпределят ресурси и позволяват управлението и оркестрирането на отделни контейнери. В контекста на тази категория продукти, контейнер е софтуерна среда за изпълнение, която капсулира един или повече софтуерни компоненти и техните зависимости в един пакет, което позволява той да работи независимо и последователно.
2. Защитни стени, системи за установяване и/или предотвратяване на проникване	Защитните стени са продукти с цифрови елементи, които защитават от неразрешен достъп дадена свързана мрежа или система, като наблюдават и ограничават трафика на данни към и от тази мрежа. Тази категория включва, но не се ограничава само до мрежови защитни стени и защитни стени за приложения, като защитни стени или филтри за уеб приложения и антиспам шлюзове.
	Системите за установяване на проникване са продукти с цифрови елементи, които наблюдават за подозрителна дейност трафика след навлизането му в мрежовата среда и установяват или идентифицират дали е направен опит за проникване, дали в момента се извършва проникване, или вече е настъпило проникване в свързана мрежа или система. Тази категория включва, но не се ограничава само до мрежови системи за установяване на проникване и хост-базирани системи за установяване на проникване.
	Системите за предотвратяване на проникване са продукти с цифрови елементи, които съдържат система за установяване на проникване, която активно реагира на проникване в свързана мрежа или система. Тази категория включва, но не се ограничава само до мрежови системи за предотвратяване на проникване и хост-базирани системи за предотвратяване на проникване.

Категория на продуктите	Техническо описание
3. Защитени от външна намеса микропроцесори	Продукти с цифрови елементи, които са микропроцесори с функционални възможности, свързани със сигурността, посочени в таблица „Клас I“, точка 13 от настоящото приложение, включително индикации, устойчивост или реакция срещу подправяне, и които допълнително са проектирани да осигуряват защита на ниво 2 или 3 на AVA_VAN, както е определено в Общите критерии и Общата методика за оценка.
4. Защитени от външна намеса микроконтролери	Продукти с цифрови елементи, които са микроконтролери с функционални възможности, свързани със сигурността, посочени в таблица „Клас I“, точка 14 от настоящото приложение, включително индикации, устойчивост или реакция срещу подправяне, и които допълнително са проектирани да осигуряват защита на ниво 2 или 3 на AVA_VAN, както е определено в Общите критерии и Общата методика за оценка.

ПРИЛОЖЕНИЕ II

КРИТИЧНИ ПРОДУКТИ С ЦИФРОВИ ЕЛЕМЕНТИ

Категория на продуктите	Техническо описание
1. Хардуерни устройства с кутии за сигурност	Хардуерни продукти с цифрови елементи, които съхраняват, обработват или управляват чувствителни данни по сигурен начин или изпълняват криптографски операции, и които се състоят от множество дискретни компоненти, включващи хардуерна физическа обвивка, осигуряваща индикация, устойчивост или реакция срещу външна намеса като противодействие срещу физически атаки. Тази категория включва, но не се ограничава само до физически терминали за плащане, хардуерни модули за сигурност, които генерират и управляват криптографски елементи, и тахографи, които отговарят на горното описание.
2. Шлюзове за интелигентни измервателни уреди в рамките на интелигентни измервателни системи съгласно определението в член 2, параграф 23 от Директива (ЕС) 2019/944 на Европейския парламент и на Съвета ([1]), и други устройства за целите на усъвършенстваната сигурност, включително за сигурна криптообработка	Шлюзовете за интелигентни измервателни уреди са продукти с цифрови елементи, които контролират комуникацията между компонентите в интелигентни измервателни системи или свързани с такива системи, както е определено в член 2, параграф 23 от Директива (ЕС) 2019/944, и упълномощени трети страни, като доставчици на комунални услуги. Шлюзовете за интелигентни измервателни уреди събират, обработват и съхраняват данни от измервателни уреди или лични данни, защитават потоците от данни и информация, като поддържат специфични криптографски функции, като криптиране и декриптиране на данни, включват функционални възможности на защитна стена и предоставят средства за контрол на други устройства. Тази категория включва, но не се ограничава само до шлюзове за интелигентни измервателни уреди, свързани с интелигентни измервателни системи за измерване на електроенергия, както е определено в член 2, параграф 23 от Директива (ЕС) 2019/944. Тя може да включва и шлюзове за интелигентни измервателни уреди, използвани в други интелигентни измервателни системи, измерващи потреблението на други енергийни източници, като газ или топлина, при условие че шлюзът отговаря на това описание.
3. Смарткарти или подобни устройства, включително защитени елементи	Защитените елементи са микроконтролери или микропроцесори с функционални възможности, свързани със сигурността, включително индикация, устойчивост или реакция срещу външна намеса. Те обикновено съхраняват, обработват или управляват криптографски операции или чувствителни данни, като например свидетелства за самоличност или данни за плащания. Защитените елементи са проектирани да осигуряват защита от най-малко AVA_VAN.4, както е определено в Общите критерии или Общата методика за оценка. Те могат да бъдат дискретни силициеви компоненти или да бъдат интегрирани в системи върху интегрална схема (SoC). Защитените елементи могат да включват приложна среда или операционна система и могат да съдържат едно или повече приложения. Тази категория включва, но не се ограничава само до доверени платформени модули (TPM) и вградени универсални карти с интегрална схема (UICC).
	Смарткартите или подобни устройства са защитни елементи, интегрирани в носител, като пластмаса или дърво, във формата на карта, или защитни елементи, интегрирани в носители с други форми. Тази категория включва, но не се ограничава само до документи за самоличност и пътуване, карти за квалифициран подпис, заменяеми UICC, физически разплащателни карти, физически карти за достъп, цифрови тахографски карти или гривни с вградени защитени елементи за плащане.

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