2024/482

7.2.2024 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2024/482 НА КОМИСИЯТА

от 31 януари 2024 година

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)

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид 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) ([1]), и по-специално член 49, параграф 7 от него,

като има предвид, че:

(1) С настоящия регламент се определят ролите, правилата и задълженията, както и структурата на европейската схема за сертифициране на киберсигурността, основана на общи критерии (ЕССК), в съответствие с европейската рамка за сертифициране на киберсигурността, установена в Регламент (ЕС) 2019/881. ЕССК се основава на Споразумението за взаимно признаване (СВП) на удостоверенията за оценка на сигурността на информационните технологии на Групата на висшите служители по сигурността на информационните системи ([2]) („SOG-IS“), използваща общите критерии, включително процедурите и документите на групата.

(2) Схемата следва да се основава на установени международни стандарти. „Общите критерии“ представляват международен стандарт за оценяване на информационната сигурност, публикуван например като ISO/IEC 15408 „Сигурност на информацията, киберсигурност и защита на неприкосновеността. Критерии за оценяване на сигурността на информационните технологии“. Той се основава на оценка от трета страна и предвижда седем нива на увереност при оценяване (EAL). „Общите критерии“ са придружени от „обща методология за оценяване“, публикувана например като ISO/IEC 18045 „Сигурност на информацията, киберсигурност и защита на неприкосновеността. Критерии за оценяване на сигурността на информационните технологии. Методология за оценяване на сигурността на информационните технологии“. Спецификациите и документите, с които се прилагат разпоредбите на настоящия регламент, може да се отнасят до публично достъпен стандарт, който отразява стандарта, използван при сертифицирането съгласно настоящия регламент, например „Общи критерии за оценяване на сигурността на информационните технологии“ и „Обща методология за оценяване на сигурността на информационните технологии“.

(3) В ЕССК се използва групата за оценка на уязвимостта на общите критерии (AVA_VAN), компоненти от 1 до 5. В петте компонента са представени всички основни определящи фактори и зависимости за анализ на уязвимостта на ИКТ продуктите. Тъй като компонентите съответстват на нивата на увереност в настоящия регламент, те позволяват добре информиран избор на увереност въз основа на извършените оценки на изискванията за сигурност и на риска, свързан с предвидената употреба на ИКТ продукта. Заявителят на сертификат по ЕССК следва да предостави документацията, свързана с предвидената употреба на ИКТ продукта, и анализа на нивата на рисковете, свързани с тази употреба, за да може органът за оценяване на съответствието да оцени пригодността на избраното ниво на увереност. Когато оценяването и сертифицирането се извършва от един и същ орган за оценяване на съответствието, изискваната информация следва да се подава от заявителя само веднъж.

(4) Техническата област е референтна рамка, която обхваща група ИКТ продукти със специфична и сходна функционалност по отношение на сигурността, с която се намаляват атаките, когато характеристиките са общи за дадено ниво на увереност. За всяка техническа област в актуални технически документи се описват специфичните изисквания за сигурност, както и допълнителните методи, техники и инструменти за оценка, които се прилагат при сертифицирането на ИКТ продукти, обхванати от тази техническа област. Поради това наличието на техническа област също така допринася за хармонизирането на оценката на обхванатите ИКТ продукти. Понастоящем две

([1]) ОВ L 151, 7.6.2019 г., стр. 15.

([2]) Споразумение за взаимно признаване на удостоверенията за оценка на сигурността на информационните технологии, версия 3.0 от януари 2010 г., достъпно на sogis.eu, одобрено от Групата на висшите служители по сигурността на информационните системи на Европейската комисия в отговор на точка 3 от Препоръка 95/144/ЕО на Съвета от 7 април 1995 г. относно общите критерии за оценка на сигурността на информационните технологии (ОВ L 93, 26.4.1995 г., стр. 27).

технически области се използват широко за сертифициране на нива AVA_VAN.4 и AVA_VAN.5. Първата техническа област е „Смарт карти и подобни устройства“, в която значителна част от изискваната функционалност за сигурност зависи от специфични, адаптирани и често разделящи се хардуерни елементи (напр. хардуер за смарт карти, интегрални схеми, съставни продукти за смарт карти, Trusted Platform Modules (модули за надеждна платформа), използвани в Trusted Computing (надеждни изчисления), или карти за цифрови тахографи). Втората техническа област е „Хардуерни устройства с кутии за сигурност“, в която значителна част от изискваната функционалност за сигурност зависи от хардуерна физическа обвивка (наричана „кутия за сигурност“), която е проектирана така, че да устоява на преки атаки, напр. терминални устройства ПОС, тахографски бордови устройства, интелигентни измервателни уреди, терминали за контрол на достъпа и хардуерни модули за сигурност).

(5) Когато подава заявление за сертифициране, заявителят следва да обвърже мотивите си за избор на ниво на увереност с целите, определени в член 51 от Регламент (ЕС) 2019/881, и с избора на компоненти от каталога на функционалните изисквания за сигурност и изискванията за гаранции за сигурност, съдържащи се в общите критерии. Сертифициращите органи следва да оценят целесъобразността на избраното ниво на увереност и да гарантират, че то е съизмеримо с нивото на риска, свързан с предвидената употреба на ИКТ продукта.

(6) Съгласно общите критерии сертифицирането се извършва въз основа на целево ниво на сигурност, което включва определение на проблема със сигурността на ИКТ продукта, както и целите за сигурност, чието постигане би решило този проблем. При формулирането на проблема със сигурността се предоставя подробна информация за предвидената употреба на ИКТ продукта и за свързаните с нея рискове. Избраният набор от изисквания за сигурност отговаря както на проблема със сигурността, така и на целите за сигурност на даден ИКТ продукт.

(7) Защитните профили са ефективно средство за предварително определяне на общите критерии, които са приложими към дадена категория ИКТ продукти, и следователно са и съществен елемент в процеса на сертифициране на ИКТ продуктите, обхванати от защитния профил. Защитният профил се използва за оценяване на бъдещите целеви нива на сигурност, които отговарят на дадената категория ИКТ продукти, обхванати от този защитен профил. Той допълнително рационализира и повишава ефективността на процеса на сертифициране на ИКТ продуктите и помага на ползвателите да определят правилно и ефективно функционалността на даден ИКТ продукт. Затова защитните профили следва да се разглеждат като неразделна част от ИКТ процеса, водещ до сертифициране на ИКТ продукти.

(8) За да могат да изиграят ролята си в ИКТ процеса, подпомагащ разработването и предоставянето на даден сертифициран ИКТ продукт, защитните профили следва да могат да бъдат сертифицирани независимо от сертифицирането на конкретния ИКТ продукт, който попада в обхвата на съответния защитен профил. Ето защо е от съществено значение да се прилага поне същото ниво на контрол към защитните профили, както и към целевите нива на сигурност, за да се гарантира високо ниво на киберсигурност. Защитните профили следва да бъдат оценявани и сертифицирани отделно от свързания ИКТ продукт и единствено чрез прилагане на класа на увереност от общите критерии и общата методика за оценка за защитни профили (APE) и, когато е приложимо, за конфигурации на защитни профили (ACE). Поради важната и деликатна роля, която имат като еталон при сертифицирането на ИКТ продукти, те следва да бъдат сертифицирани само от публични органи или сертифициращ орган, получил предварително одобрение за конкретен защитен профил от националния орган за сертифициране на киберсигурността. Поради основната им роля за сертифициране с ниво на увереност „високо“, особено извън техническите области, защитните профили следва да бъдат разработени под формата на актуални технически документи, които следва да бъдат одобрени от Европейската група за сертифициране на киберсигурността.

(9) Сертифицираните защитни профили следва да бъдат включени в мониторинга на съответствието и спазването на изискванията на ЕССК от страна на националните органи за сертифициране на киберсигурността. Когато за конкретни сертифицирани защитни профили са налице методология, инструменти и умения, прилагани към подходите за оценка на ИКТ продукти, техническите области могат да се основават на тези специфични защитни профили.

(10) За да се постигне високо ниво на доверие и увереност в сертифицираните ИКТ продукти, самооценяването не следва да се разрешава съгласно настоящия регламент. Следва да бъде разрешено само оценяване на съответствието от трета страна, извършвано от ITSEF и от сертифициращи органи.

(11) Общността на SOG-IS предостави съвместни интерпретации и подходи за прилагането на общите критерии и общата методика за оценка при сертифицирането, по-специално за ниво на увереност „високо“, което се изисква по отношение на техническите области „Смарт карти и подобни устройства“ и „Хардуерни устройства с кутии за сигурност“. Повторното използване на такива подкрепящи документи в ЕССК осигурява плавен преход от национално прилаганите схеми на SOG-IS към хармонизираната ЕССК. Поради това в настоящия регламент следва да се включат общовалидни хармонизирани методики за оценка за всички дейности по сертифициране. Освен това Комисията следва да може да поиска от Европейската група за сертифициране на киберсигурността да приеме становище, с което да одобри и препоръча прилагането на методиките за оценка, посочени в актуалните технически документи, за сертифициране на ИКТ продукт или защитен профил по ЕССК. Поради това в приложение I към настоящия регламент са изброени актуалните технически документи за дейностите по оценяване, извършвани от органите за оценяване на съответствието. Европейската група за сертифициране на киберсигурността следва да одобрява и поддържа актуалните технически документи. При сертифицирането следва да се използват актуалните технически документи. Органът за оценяване на съответствието може да не използва тези документи само в изключителни и надлежно обосновани случаи и при специфични условия, по-специално при наличието на одобрение от националния орган за сертифициране на киберсигурността.

(12) Сертифицирането на ИКТ продукти на ниво 4 или 5 на AVA_VAN следва да бъде възможно само при определени условия и когато е налична конкретна методика за оценка. Специфичната методика за оценка може да бъде заложена в актуалните технически документи, които са от значение за техническата област, или в конкретни защитни профили, приети като актуален технически документ, които са от значение за съответната категория продукти. Сертифициране при тези нива на увереност следва да е възможно само в изключителни и надлежно обосновани случаи и при специфични условия, по-специално при наличието на одобрение от националния орган за сертифициране на киберсигурността, включително наличие на приложима методика за оценка. Такива изключителни и надлежно обосновани случаи могат да са налице, когато законодателството на Съюза или националното законодателство изискват сертифициране на ИКТ продукт при ниво 4 или 5 на AVA_VAN. Също така, в изключителни и надлежно обосновани случаи и при специфични условия, по-специално при наличие на одобрение от националния орган за сертифициране на киберсигурността, включително наличие на приложима методика за оценка, може да се извършва сертифициране на защитни профили, без да се прилагат съответните актуални технически документи.

(13) Маркировките и етикетите, използвани в рамките на ЕССК, имат за цел видимо да се покаже на ползвателите надеждността на сертифицирания ИКТ продукт и да им се даде възможност да направят информиран избор при закупуването на ИКТ продукти. Използването на маркировки и етикети също следва да подлежи на правилата и условията, посочени в ISO/IEC 17065 и, когато е приложимо, в ISO/IEC 17030 с приложимите насоки.

(14) Сертифициращите органи следва да вземат решение относно срока на валидност на сертификатите, като отчетат жизнения цикъл на съответния ИКТ продукт. Срокът на валидност не следва да надвишава 5 години. Националните органи за сертифициране на киберсигурността следва да работят за хармонизиране на срока на валидност в Съюза.

(15) Когато обхватът на съществуващ сертификат по ЕССК е намален, сертификатът се оттегля и следва да се издаде нов сертификат с новия обхват, за да се гарантира, че ползвателите са ясно информирани за текущия обхват и нивото на увереност на сертификата за даден ИКТ продукт.

(16) Сертифицирането на защитни профили се различава от това на ИКТ продукти, тъй като се отнася до ИКТ процес. Тъй като защитният профил обхваща категория ИКТ продукти, неговата оценка и сертифицирането му не могат да се извършват въз основа на един-единствен ИКТ продукт. Тъй като защитният профил обединява общите изисквания за сигурност по отношение на категория ИКТ продукти и е независим от представянето на ИКТ продукта от неговия доставчик, срокът на валидност на сертификата по ЕССК за защитен профил следва по принцип да обхваща най-малко 5 години и може да бъде удължен до целия жизнен цикъл на защитния профил.

(17) Органът за оценяване на съответствието се определя като орган, осъществяващ дейности по оценяване на съответствието, включително еталониране, изпитване, сертифициране и контрол. За да се гарантира високо качество на услугите, в настоящия регламент се посочва, че дейностите по изпитване, от една страна, и дейностите по сертифициране и инспекция, от друга страна, следва да се извършват от субекти, които работят независимо един от друг, а именно съответно от центрове за оценка на сигурността на информационните технологии (ITSEF) и от сертифициращи органи. И двата вида органи за оценяване на съответствието следва да бъдат акредитирани, а в определени ситуации — упълномощени.

(18) Сертифициращият орган следва да бъде акредитиран в съответствие със стандарт ISO/IEC 17065 от националния орган по акредитация за ниво на увереност „значително“ и „високо“. В допълнение към акредитацията в съответствие с Регламент (ЕС) 2019/881, разглеждан съвместно с Регламент (ЕО) № 765/2008, органите за оценяване на съответствието следва да отговарят на специфични изисквания, за да се гарантира техническата им компетентност за оценяване на изискванията за киберсигурност при ниво на увереност „високо“ по ЕССК, което се потвърждава с „упълномощаване“. С цел подпомагане на процеса на упълномощаване следва да се разработят съответни актуални технически документи, които да се публикуват от ENISA, след одобрение от Европейската група за сертифициране на киберсигурността.

(19) Техническата компетентност на ITSEF следва да бъде оценена чрез акредитация на лабораторията за изпитване в съответствие с ISO/IEC 17025 и допълнително с ISO/IEC 23532-1 за пълния набор от дейности по оценяване, които са от значение за нивото на увереност и са посочени в ISO/IEC 18045 във връзка с ISO/IEC 15408. Както сертифициращият орган, така и ITSEF следва да създадат и поддържат подходяща система за управление на компетентността на персонала, която се основава на ISO/IEC 19896-1 за елементите и нивата на компетентност и за оценката на компетентността. По отношение на нивото на знанията, уменията, опита и образованието приложимите изисквания към оценителите следва да се вземат от ISO/IEC 19896-3. Следва да се докаже изпълнението на еквивалентни разпоредби и мерки за справяне с отклоненията от такива системи за управление на компетентността в съответствие с целите на системата.

(20) За да бъде упълномощен, ITSEF следва да докаже способността си да определя липсата на известни уязвимости, правилното и последователно прилагане на актуалните функционалности за сигурност за конкретната технология и устойчивостта на целевия ИКТ продукт спрямо опитни лица, извършващи кибератаки. Освен това за упълномощаването в техническата област „Смарт карти и подобни устройства“ ITSEF следва да докаже и техническите способности, необходими за дейностите по оценяване и свързаните с тях задачи, както е определено в „Минимални изисквания на ITSEF за оценяване на сигурността на смарт карти и подобни устройства“ ([3]), подкрепящ документ съгласно общите критерии. За упълномощаването в техническата област „Хардуерни устройства с кутии за сигурност“ ITSEF следва също така да докаже изпълнението на минималните технически изисквания, необходими за извършване на дейностите по оценяване и свързаните с тях задачи на хардуерни устройства с кутии за сигурност, както е препоръчано от Европейската група за сертифициране на киберсигурността. В контекста на минималните изисквания ITSEF следва да може да извършва различните видове кибератаки, посочени в „Прилагане на потенциала за кибератака към хардуерни устройства с кутии за сигурност“), подкрепящ документ съгласно общите критерии. Тези способности обхващат знанията и уменията на оценителя, както и оборудването и методите за оценка, необходими за определянето и оценяването на различните видове кибератаки.

(21) Националният орган за сертифициране на киберсигурността следва да наблюдава спазването на изискванията от страна на сертифициращите органи, ITSEF и титулярите на сертификати на техните задължения, произтичащи от настоящия регламент и от Регламент (ЕС) 2019/881. За тази цел националният орган за сертифициране на киберсигурността следва да използва всички подходящи източници на информация, включително информация, получена от участниците в процеса на сертифициране и от собствени разследвания.

(22) Сертифициращите органи следва да си сътрудничат със съответните органи за надзор на пазара и да вземат предвид всяка информация за уязвимост, която би могла да има отношение към ИКТ продуктите, за които са издали сертификати. Сертифициращите органи следва да наблюдават сертифицираните от тях защитни профили и да следят дали изискванията за сигурност, определени за дадена категория ИКТ продукти, продължават да отразяват последните промени в обстановката по отношение на заплахите.

(23) В подкрепа на наблюдението на спазването на изискванията от националните органи за сертифициране на киберсигурността следва да си сътрудничат със съответните органи за надзор на пазара в съответствие с член 58 от Регламент (ЕС) 2019/881 и Регламент (ЕС) 2019/1020 на Европейския парламент и на Съвета ([4]). Икономическите оператори в Съюза са задължени да обменят информация и да си сътрудничат с органите за надзор на пазара съгласно член 4, параграф 3 от Регламент (ЕС) 2019/1020.

([3]) Библиотека на Съвместната работна група за тълкуване: „Минимални изисквания на ITSEF за оценяване на сигурността на смарт карти и подобни устройства“, версия 2.1 от февруари 2020 г., на разположение на sogis.eu.

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

(24) Сертифициращите органи следва да наблюдават спазването на изискванията от страна на титулярите на сертификат и съответствието на всички сертификати, издадени по ЕССК. Наблюдението следва да гарантира, че всички доклади за оценка, предоставени от даден ITSEF, и направените в тях заключения, както и критериите и методите за оценка се прилагат последователно и правилно във всички дейности по сертифициране.

(25) Когато се открият потенциални проблеми с несъответствието, които засягат сертифициран ИКТ продукт, е важно да се осигури пропорционална реакция. Поради това действието на сертификатите може да бъде спряно. Спирането на действието следва да води до определени ограничения по отношение на представянето и използването на въпросния ИКТ продукт, но не и да засяга валидността на сертификата. Титулярят на сертификата на ЕС следва да уведоми купувачите на засегнатите ИКТ продукти за спирането на действието на сертификата, а съответният национален орган за сертифициране на киберсигурността следва да уведоми съответните органи за надзор на пазара. За да информира обществеността, ENISA следва да публикува информация за спирането на действието на даден сертификат на специален уебсайт.

(26) Титулярят на сертификат по ЕССК следва да приложи необходимите процедури за управление на уязвимостта и да гарантира, че тези процедури са внедрени в неговата организация. Когато узнае за потенциална уязвимост, титулярят на сертификата по ЕССК следва да извърши анализ на въздействието на уязвимостта. В случай че от анализа на въздействието на уязвимостта се потвърди, че уязвимостта може да се използва, титулярят на сертификата следва да изпрати доклад за оценката на сертифициращия орган, който от своя страна следва да информира националния орган за сертифициране на киберсигурността. Докладът следва да съдържа информация за въздействието на уязвимостта, необходимите промени или корективни мерки, включително възможните по-широки последици от уязвимостта, както и корективни мерки за други продукти. Когато е необходимо, стандартът EN ISO/IEC 29147 следва да допълни процедурата за оповестяване на уязвимостта.

(27) За целите на сертифицирането органите за оценяване на съответствието и националните органи за сертифициране на киберсигурността получават поверителни и чувствителни данни и търговски тайни, включително свързани с интелектуална собственост или с мониторинга за спазване на изискванията, които изискват адекватна защита. Поради това те следва да разполагат с необходимата техническа компетентност и знания и да въведат системи за защита на информацията. Изискванията и условията за защита на информацията следва да бъдат изпълнени както при акредитация, така и при упълномощаване.

(28) ENISA следва да предостави списъка на сертифицираните защитни профили на своя уебсайт за сертифициране на киберсигурността и да посочи техния статус в съответствие с Регламент (ЕС) 2019/881.

(29) В настоящия регламент се определят условията за сключване на споразумения за взаимно признаване с трети държави. Тези споразумения за взаимно признаване могат да бъдат двустранни или многостранни и следва да заменят подобни споразумения, които понастоящем са в сила. За да се улесни плавният преход към такива споразумения за взаимно признаване, се допуска държавите членки да продължават съществуващите договорености за сътрудничество с трети държави за ограничен период от време.

(30) Сертифициращите органи, които издават сертификати по ЕССК с ниво на увереност „високо“, както и съответните свързани ITSEF, следва да се подлагат на партньорски оценки. Целта на партньорските оценки следва да бъде да се определи дали структурата и процедурите на даден сертифициращ орган, подложен на партньорска оценка, продължават да отговарят на изискванията на схемата ЕССК. Партньорските оценки се различават от партньорските проверки на националните органи за сертифициране на киберсигурността, предвидени в член 59 от Регламент (ЕС) 2019/881. Партньорските оценки следва да гарантират, че сертифициращите органи работят по хармонизиран начин и изготвят сертификати с еднакво качество, и в тях следва да бъдат посочени всички потенциални силни или слаби страни в работата на сертифициращите органи, включително с оглед на обмена на най-добри практики. Тъй като съществуват различни видове сертифициращи органи, следва да са допустими различни типове партньорски оценки. В по-сложни случаи, например когато сертифициращи органи издават сертификати за различни нива на AVA_VAN, могат да се използват различни типове партньорски оценки, при условие, че са изпълнени всички изисквания.

(31) Европейската група за сертифициране на киберсигурността следва да играе важна роля в поддържането на схемата. Това следва, наред с другото, да се осъществява чрез сътрудничество с частния сектор, създаване на специализирани подгрупи и подходяща подготвителна работа и помощ, поискана от Комисията. Европейската група за сертифициране на киберсигурността играе важна роля в одобряването на актуалните технически документи. При одобряването и приемането на актуалните технически документи следва надлежно да се вземат предвид елементите, посочени в член 54, параграф 1, буква в) от Регламент (ЕС) 2019/881. Техническите области и актуалните технически

документи следва да се публикуват в приложение I към настоящия регламент. Защитни профили, които са били приети под формата на актуални технически документи, следва да се публикуват в приложение II. За да се гарантира, че тези приложения са динамични, Комисията може да ги изменя в съответствие с процедурата, посочена в член 66, параграф 2 от Регламент (ЕС) 2019/881, като взема предвид становището на Европейската група за сертифициране на киберсигурността. Приложение III съдържа препоръчителни защитни профили, които към момента на влизане в сила на настоящия регламент не са актуални технически документи. Те следва да се публикуват на уебсайта на ENISA, посочен в член 50, параграф 1 от Регламент (ЕС) 2019/881.

(32) Настоящият регламент следва да започне да се прилага 12 месеца след влизането му в сила. Изискванията на глава IV и приложение V не се нуждаят от преходен период и поради това следва да се прилагат от датата на влизане в сила на настоящия регламент.

(33) Мерките, предвидени в настоящия регламент, са в съответствие със становището на Европейския комитет за сертифициране на киберсигурността, създаден с член 66 от Регламент (ЕС) 2019/881,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

ГЛАВА I

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет и приложно поле

С настоящия регламент се установява европейската схема за сертифициране на киберсигурността, основана на общи критерии (ЕССК).

Настоящият регламент се прилага за всички продукти на информационните и комуникационните технологии („ИКТ продукти“), включително тяхната документация, които са представени за сертифициране по ЕССК, както и за всички защитни профили, които са представени за сертифициране като част от ИКТ процеса, водещ до сертифициране на ИКТ продукти.

Член 2

Определения

За целите на настоящия регламент се прилагат следните определения:

1) „общи критерии“ означава общите критерии за оценка на сигурността на информационните технологии, както е посочено в стандарта на ISO/IEC 15408;

2) „обща методика за оценка“ означава общата методика за оценка на сигурността на информационните технологии, както е посочено в стандарта на ISO/IEC ISO/IEC 18045;

3) „обект на оценка“ означава ИКТ продукт или част от него, или защитен профил като част от ИКТ процес, който се подлага на оценка на киберсигурността, за да получи сертификат по ЕССК;

4) „целево ниво на сигурност“ означава заявени и зависими от изпълнението изисквания за сигурност за конкретен ИКТ продукт;

5) „защитен профил“ означава ИКТ процес, чрез който се определят изискванията за сигурност за конкретна категория ИКТ продукти, отговарящи на независещи от конкретно изпълнение нужди относно сигурността, и който може да се използва за оценяване на ИКТ продукти, попадащи в тази конкретна категория, с цел тяхното сертифициране;

6) „технически доклад за оценка“ означава документ, изготвен от даден ITSEF за представяне на констатациите, решенията и обосновките, получени по време на оценката на ИКТ продукт или на защитен профил в съответствие с правилата и задълженията, определени в настоящия регламент;

7) „ITSEF“ означава център за оценка на сигурността на информационните технологии, който е орган за оценяване на съответствието съгласно определението в член 2, точка 13 от Регламент (ЕО) № 765/2008 и който извършва дейности по оценяване;

8) „ниво AVA_VAN“ означава ниво на анализ на уязвимостта, което показва степента на извършените дейности по оценка на киберсигурността, за да се определи нивото на устойчивост срещу потенциална възможност за използване на недостатъци или слабости в обекта на оценка в неговата оперативна среда, както е посочено в общите критерии;

9) „сертификат по ЕССК“ означава сертификат за киберсигурност, издаден съгласно ЕССК за ИКТ продукти или за защитни профили, които могат да се използват изключително в процеса на сертифициране на ИКТ продукти;

10) „съставен продукт“ означава ИКТ продукт, който се оценява заедно с друг базов ИКТ продукт, който вече е получил сертификат по ЕССК и от чиято функционалност по отношение на сигурността зависи съставният ИКТ продукт;

11) „национален орган за сертифициране на киберсигурността“ означава орган, определен от държава членка в съответствие с член 58, параграф 1 от Регламент (ЕС) 2019/881;

12) „сертифициращ орган“ означава орган за оценяване на съответствието съгласно определението в член 2, точка 13 от Регламент (ЕО) № 765/2008, който извършва дейности по сертифициране;

13) „техническа област“ означава обща техническа рамка, свързана с конкретна технология за хармонизирано сертифициране с набор от характерни изисквания за сигурност;

14) „актуален технически документ“ означава документ, в който се определят методите, техниките и инструментите за оценяване, приложими към сертифицирането на ИКТ продукти, или изисквания за сигурност на обща категория ИКТ продукти, или всякакви други изисквания относно сертифицирането, с цел хармонизиране на оценяването по-специално при техническите области или защитните профили;

15) „орган за надзор на пазара“ означава орган съгласно определението в член 3, параграф 4 от Регламент (ЕС) 2019/1020.

Член 3

Стандарти за оценка

За оценките, извършвани по ЕССК, се прилагат следните стандарти:

а) общите критерии;

б) общата методика за оценка.

Член 4

Нива на увереност

1. Сертифициращите органи издават сертификати по ЕССК с ниво на увереност „значително“ или „високо“.

2. Сертификатите по ЕССК с ниво на увереност „значително“ съответстват на сертификати, които покриват ниво 1 или 2 на AVA_VAN.

3. Сертификатите по ЕССК с ниво на увереност „високо“ съответстват на сертификати, които покриват ниво 3, 4 или 5 на AVA_VAN.

4. В нивото на увереност, потвърдено в сертификата по ЕССК, трябва да се разграничава съответстващото и разширеното използване на компонентите за увереност, както е посочено в общите критерии съгласно приложение VIII.

5. Органите за оценяване на съответствието прилагат компонентите за увереност, от които зависи избраното ниво AVA_VAN, в съответствие със стандартите, посочени в член 3.

Член 5

Методи за сертифициране на ИКТ продукти

1. Сертифицирането на даден ИКТ продукт се извършва спрямо неговото целево ниво на сигурност:

а) както е определено от заявителя; или

б) чрез включване на сертифициран защитен профил като част от ИКТ процеса, когато ИКТ продуктът попада в категорията ИКТ продукти, обхванатa от този защитен профил.

2. Защитните профили се сертифицират единствено за целите на сертифицирането на ИКТ продукти, попадащи в конкретната категория ИКТ продукти, обхванатa от защитния профил.

Член 6

Самооценяване на съответствието

Самооценяване на съответствието по смисъла на член 53 от Регламент (ЕС) 2019/881 не се разрешава.

ГЛАВА II

СЕРТИФИЦИРАНЕ НА ИКТ ПРОДУКТИ

РАЗДЕЛ I

СПЕЦИФИЧНИ СТАНДАРТИ И ИЗИСКВАНИЯ ЗА ОЦЕНКА

Член 7

Критерии и методи за оценка на ИКТ продукти

1. ИКТ продукт, представен за сертифициране, се оценява най-малко в съответствие със следното:

а) приложимите елементи на стандартите, посочени в член 3;

б) класовете изисквания за гаранциите за сигурност при анализ на уязвимостта и независимо функционално изпитване, както е определено в стандартите за оценка, посочени в член 3;

в) нивото на риска, свързан с предвидената употреба на съответните ИКТ продукти съгласно член 52 от Регламент (ЕС) 2019/881, и техните функции за сигурност, които подкрепят целите за сигурност, определени в член 51 от Регламент (ЕС) 2019/881;

г) приложимите актуални технически документи, изброени в приложение I. и

д) приложимите сертифицирани защитни профили, изброени в приложение II.

2. В изключителни и надлежно обосновани случаи органът за оценяване на съответствието може да поиска да се въздържи от прилагането на съответния актуален технически документ. В такива случаи органът за оценяване на съответствието информира националния орган за сертифициране на киберсигурността с надлежно мотивирана обосновка за своето искане. Националният орган за сертифициране на киберсигурността оценява обосновката за дадено изключение и го одобрява, когато то е обосновано. До вземането на решение от националния орган за сертифициране на киберсигурността

органът за оценяване на съответствието не издава сертификат. Националният орган за сертифициране на киберсигурността уведомява без ненужно забавяне за одобреното изключение Европейската група за сертифициране на киберсигурността, която може да издаде становище. Националният орган за сертифициране на киберсигурността взема под внимание в най-голяма степен становището на Европейската група за сертифициране на киберсигурността.

3. Сертифицирането на ИКТ продукти на ниво 4 или 5 на AVA_VAN е възможно само в следните случаи:

а) когато ИКТ продуктът е обхванат от някоя от техническите области, изброени в приложение I, той се оценява в съответствие с приложимите актуални технически документи за тези технически области,

б) когато ИКТ продуктът, попада в категория ИКТ продукти, обхванатa от сертифициран защитен профил, който включва ниво 4 или 5 на AVA_VAN и е посочен като актуален защитен профил в приложение II, той се оценява в съответствие с методиката за оценка, определена за този защитен профил.

в) когато букви а) и б) от настоящия параграф не са приложими и когато включването на техническа област в приложение I или на сертифициран защитен профил в приложение II е малко вероятно в обозримо бъдеще, и само в изключителни и надлежно обосновани случаи, като се спазват условията, посочени в параграф 4.

4. Когато орган за оценяване на съответствието счита, че е налице изключителен и надлежно обоснован случай съгласно посоченото в параграф 3, буква в), той уведомява за планираното сертифициране националния орган за сертифициране на киберсигурността, като предоставя обосновка и предлага методика за оценка. Националният орган за сертифициране на киберсигурността оценява обосновката за дадено изключение и, когато е обосновано, одобрява или изменя методиката за оценка, която се прилага от органа за оценяване на съответствието. До вземането на решение от националния орган за сертифициране на киберсигурността органът за оценяване на съответствието не издава сертификат. Националният орган за сертифициране на киберсигурността докладва без ненужно забавяне за плануваното сертифициране на Европейската група за сертифициране на киберсигурността, която може да издаде становище. Националният орган за сертифициране на киберсигурността взема под внимание в най-голяма степен становището на Европейската група за сертифициране на киберсигурността.

5. В случай на ИКТ продукт, който се подлага на оценяване за съставен продукт в съответствие с приложимите актуални технически документи, ITSEF, който е извършил оценяването на базовия ИКТ продукт, споделя съответната информация с ITSEF, който извършва оценяването на съставния ИКТ продукт.

РАЗДЕЛ II

ИЗДАВАНЕ, ПОДНОВЯВАНЕ И ОТТЕГЛЯНЕ НА СЕРТИФИКАТИ ПО ЕССК

Член 8

Информация, необходима за сертифицирането

1. Заявителят за сертифициране по ЕССК предоставя или по друг начин осигурява на разположение на сертифициращия орган и на ITSEF цялата информация, необходима за дейностите по сертифициране.

2. Информацията, посочена в параграф 1, включва всички относими доказателства в съответствие с разделите „Елементи на действията на разработчика“ в подходящ формат, както е посочено в разделите „Съдържание и представяне на елемента на доказателствата“ от общите критерии и общата методика за оценка за избраното ниво на увереност и свързаните с него изисквания за гаранциите за сигурност. Доказателствата включват, когато е необходимо, подробности за ИКТ продукта и неговия изходен код в съответствие с настоящия регламент, при спазването на гаранции срещу неразрешено разкриване.

3. Заявителите за сертифициране могат да предоставят на сертифициращия орган и на ITSEF подходящи резултати от оценка за предишно сертифициране по силата на:

а) настоящия регламент;

б) друга европейска схема за сертифициране на киберсигурността, приета съгласно член 49 от Регламент (ЕС) 2019/881;

в) национална схема, посочена в член 49 от настоящия регламент.

4. Когато резултатите от оценката са свързани с неговите задачи, ITSEF може да използва повторно тези резултати, при условие че те отговарят на приложимите изисквания и тяхната автентичност е потвърдена.

5. Когато сертифициращият орган разреши продуктът да бъде подложен на сертифициране като част от съставен продукт, заявителят за сертифициране предоставя на сертифициращия орган и на ITSEF всички необходими елементи, когато е приложимо, в съответствие с актуалния технически документ.

6. Заявителите за сертифициране също така предоставят на сертифициращия орган и на ITSEF следната информация:

а) връзка към техния уебсайт, съдържащ допълнителната информация за киберсигурността, посочена в член 55 от Регламент (ЕС) 2019/881;

б) описание на процедурите на заявителя за управление на уязвимости и оповестяване на уязвимости.

7. Цялата съответна документация, посочена в настоящия член, се съхранява от сертифициращия орган, ITSEF и заявителя за период от 5 години след изтичането на срока на валидност на сертификата.

Член 9

Условия за издаване на сертификат по ЕССК

1. Сертифициращите органи издават сертификат по ЕССК, когато са изпълнени всички изброени по-долу условия:

а) категорията на ИКТ продукта попада в обхвата на акредитацията и, когато е приложимо, на упълномощаването на сертифициращия орган и на ITSEF, участващи в сертифицирането;

б) заявителят за сертифициране е подписал декларация, с която поема всички ангажименти, изброени в параграф 2;

в) ITSEF е приключил оценката без възражения в съответствие със стандартите, критериите и методите за оценка, посочени в членове 3 и 7;

г) сертифициращият орган е приключил прегледа на резултатите от оценката без възражения;

д) сертифициращият орган е проверил дали техническите доклади за оценка, предоставени от ITSEF, съответстват на предоставените доказателства и дали стандартите, критериите и методите за оценка, посочени в членове 3 и 7, са правилно приложени.

2. Заявителят за сертифициране поема следните ангажименти:

а) да предостави на сертифициращия орган и на ITSEF цялата необходима пълна и вярна информация, както и да предостави необходимата допълнителна информация при поискване;

б) да не представя ИКТ продукта като сертифициран по ЕССК преди издаването на сертификата по ЕССК;

в) да представя ИКТ продукта като сертифициран само по отношение на обхвата, посочен в сертификата по ЕССК;

г) да преустанови незабавно представянето на ИКТ продукта като сертифициран в случай на спиране на действието, оттегляне или изтичане на валидността на сертификата по ЕССК;

д) да гарантира, че ИКТ продуктите, продавани с позоваване на сертификата по ЕССК, са напълно идентични с ИКТ продукта, подлежащ на сертифициране;

е) да спазва правилата за използване на маркировката и етикета, установени за сертификата по ЕССК в съответствие с член 11.

3. В случай на ИКТ продукт, който се подлага на сертифициране като част от съставен продукт, в съответствие с приложимите актуални технически документи сертифициращият орган, който е извършил сертифицирането на базовия ИКТ продукт, споделя съответната информация със сертифициращия орган, който извършва сертифицирането на съставния ИКТ продукт.

Член 10

Съдържание и формат на сертификата по ЕССК

1. Сертификатът по ЕССК включва най-малко информацията, посочена в приложение VII.

2. Обхватът и границите на сертифицирания ИКТ продукт се посочват недвусмислено в сертификата по ЕССК или в сертификационния доклад, като се посочва дали е бил сертифициран целият ИКТ продукт или само части от него.

3. Сертифициращият орган предоставя сертификата по ЕССК на заявителя най-малко в електронен вид.

4. Сертифициращият орган изготвя сертификационен доклад в съответствие с приложение V за всеки издаден от него сертификат по ЕССК. Сертификационният доклад се основава на техническия доклад за оценка, издаден от съответния ITSEF. В техническия доклад за оценка и в сертификационния доклад се посочват специфичните критерии и методи за оценка, посочени в член 7, използвани за оценката.

5. Сертифициращият орган предоставя на националния орган за сертифициране на киберсигурността и на ENISA всеки сертификат по ЕССК и всеки сертификационен доклад в електронен вид.

Член 11

Маркировка и етикет

1. Титулярят на сертификата може да поставя маркировка и етикет върху сертифицирания ИКТ продукт. Маркировката и етикетът показват, че ИКТ продуктът е сертифициран в съответствие с настоящия регламент. Маркировката и етикетът се поставят в съответствие с настоящия член и с приложение IX.

2. Маркировката и етикетът се поставят върху сертифицирания ИКТ продукт или върху неговата табелка с данни така, че да бъдат видими, четливи и незаличими. Когато това не е възможно или не може да бъде гарантирано поради естеството на продукта, те се поставят върху опаковката и в придружаващите документи. Когато сертифицираният ИКТ продукт се доставя под формата на софтуер, маркировката и етикетът трябва да фигурират по видим, четлив и неизличим начин в придружаващата го документация или тази документация трябва да е лесно и пряко достъпна за ползвателите посредством уебсайт.

3. Маркировката и етикетът се изготвят, както е посочено в приложение IX, и съдържат:

а) нивото на увереност и нивото на AVA_VAN на сертифицирания ИКТ продукт;

б) уникалната идентификация на сертификата, състояща се от:

1) наименованието на схемата;

2) уникалния идентификационен номер на сертифициращия орган, който е издал сертификата.

3) годината и месеца на издаване;

4) идентификационния номер, определен от сертифициращия орган, издал сертификата.

4. Маркировката и етикетът се придружават от QR код с връзка към уебсайт, съдържащ най-малко:

а) информация за валидността на сертификата;

б) необходимата информация относно сертифицирането, както е посочено в приложения V и VII;

в) информацията, която титулярят на сертификата трябва да оповести публично в съответствие с член 55 от Регламент (ЕС) 2019/881; и

г) когато е приложимо, информация от минали периоди, свързана с конкретното сертифициране или с предходни сертифицирания на ИКТ продукта, за да се даде възможност за проследяване.

Член 12

Срок на валидност на сертификатите по ЕССК

1. Сертифициращият орган определя срока на валидност на всеки издаден сертификат по ЕССК, като взема предвид характеристиките на сертифицирания ИКТ продукт.

2. Срокът на валидност на сертификата по ЕССК не може да надвишава 5 години.

3. Чрез дерогация от параграф 2 този срок може да надвиши 5 години, при условие че това бъде предварително одобрено от националния орган за сертифициране на киберсигурността. Националният орган за сертифициране на киберсигурността уведомява Европейската група за сертифициране на киберсигурността за предоставеното одобрение без неоправдано забавяне.

Член 13

Преглед на сертификатите по ЕССК

1. По искане на титуляря на сертификата или по други основателни причини сертифициращият орган може да реши да извърши преглед на сертификата по ЕССК за даден ИКТ продукт. Прегледът се извършва в съответствие с приложение IV. Сертифициращият орган определя обхвата на прегледа. В случай че е необходимо за прегледа, сертифициращият орган отправя искане до ITSEF за извършване на повторна оценка на сертифицирания ИКТ продукт.

2. След резултатите от прегледа и, когато е приложимо, от повторната оценка, сертифициращият орган:

а) потвърждава сертификата по ЕССК;

б) оттегля сертификата по ЕССК в съответствие с член 14;

в) оттегля сертификата по ЕССК в съответствие с член 14 и издава нов сертификат по ЕССК с идентичен обхват и удължен срок на валидност; или

г) оттегля сертификата по ЕССК в съответствие с член 14 и издава нов сертификат по ЕССК с различен обхват.

3. Сертифициращият орган може да реши да спре действието на сертификата по ЕССК без неоправдано забавяне в съответствие с член 30 до предприемането на корективни действия от страна на титуляря на сертификата по ЕССК.

Член 14

Оттегляне на сертификат по ЕССК

1. Без да се засяга член 58, параграф 8, буква д) от Регламент (ЕС) 2019/881, сертификатът по ЕССК се оттегля от сертифициращия орган, който го е издал.

2. Сертифициращият орган, посочен в параграф 1, уведомява националния орган за сертифициране на киберсигурността за оттеглянето на сертификата. Той също така уведомява ENISA за оттеглянето с оглед улесняване на изпълнението на задачата ѝ по член 50 от Регламент (ЕС) 2019/881. Националният орган за сертифициране на киберсигурността уведомява другите съответни органи за надзор на пазара.

3. Титулярят на сертификат по ЕССК може да поиска неговото оттегляне.

ГЛАВА III

СЕРТИФИЦИРАНЕ НА ЗАЩИТНИ ПРОФИЛИ

РАЗДЕЛ I

Специфични стандарти и изисквания за оценка

Член 15

Критерии и методи за оценка

1. Защитният профил се оценява най-малко в съответствие със следното:

а) приложимите елементи на стандартите, посочени в член 3;

б) нивото на риска, свързан с предвидената употреба на съответните ИКТ продукти съгласно член 52 от Регламент (ЕС) 2019/881, и техните функции за сигурност, които подкрепят целите за сигурност, определени в член 51 от същия регламент; и

в) приложимите актуални технически документи, изброени в приложение I. Защитен профил, обхванат от дадена техническа област, се сертифицира спрямо изискванията, определени в тази техническа област.

2. В изключителни и надлежно обосновани случаи органът за оценяване на съответствието може да сертифицира защитен профил, без да прилага съответните актуални технически документи. В такива случаи той информира компетентния национален орган за сертифициране на киберсигурността и представя обосновка за планираното сертифициране без прилагане на съответните актуални технически документи, както и предложената методика за оценка. Националният орган за сертифициране на киберсигурността оценява обосновката и, когато е обосновано, одобрява неприлагането на съответните актуални технически документи, а също така одобрява или изменя, когато е целесъобразно, методиката за оценка, която се прилага от органа за оценяване на съответствието. До вземането на решение от националния орган за сертифициране на киберсигурността органът за оценяване на съответствието не издава сертификат за защитния профил. Националният орган за сертифициране на киберсигурността уведомява без ненужно забавяне за разрешеното неприлагане на съответните актуални технически документи на Европейската група за сертифициране на киберсигурността, която може да издаде становище. Националният орган за сертифициране на киберсигурността взема под внимание в най-голяма степен становището на Европейската група за сертифициране на киберсигурността.

РАЗДЕЛ II

Издаване, подновяване и оттегляне на сертификати по есск за защитни профили

Член 16

Информация, необходима за сертифицирането на защитни профили

Заявителят за сертифициране на защитен профил предоставя или по друг начин осигурява на разположение на сертифициращия орган и на ITSEF цялата информация, необходима за дейностите по сертифициране. Разпоредбите на член 8, параграфи 2, 3 и 4 и 7 се прилагат *mutatis mutandis*.

Член 17

Издаване на сертификати по ЕССК за защитни профили

1. Заявителят за сертифициране предоставя на сертифициращия орган и на ITSEF цялата необходима пълна и вярна информация.

2. Разпоредбите на членове 9 и 10 се прилагат *mutatis mutandis*.

3. ITSEF оценява дали даден защитен профил е пълен, последователен, технически обоснован и ефективен за предвидената употреба и за целите на сигурността на категорията ИКТ продукти, обхванати от този защитен профил.

4. Защитният профил се сертифицира единствено от:

а) национален орган за сертифициране на киберсигурността или друг публичен орган, акредитиран като сертифициращ орган; или

б) сертифициращ орган, след предварително одобрение от националния орган за сертифициране на киберсигурността за всеки отделен защитен профил.

Член 18

Срок на валидност на сертификатите по ЕССК за защитни профили

1. Сертифициращият орган определя срок на валидност за всеки сертификат по ЕССК.

2. Срокът на валидност може да бъде до края на жизнения цикъл на съответния защитен профил.

Член 19

Преглед на сертификатите по ЕССК за защитни профили

1. По искане на титуляря на сертификата или по други основателни причини сертифициращият орган може да реши да извърши преглед на сертификата по ЕССК за даден защитен профил. Прегледът се извършва, като се прилагат условията, посочени в член 15. Сертифициращият орган определя обхвата на прегледа. В случай че е необходимо за прегледа, сертифициращият орган отправя искане до ITSEF за извършване на повторна оценка на сертифицирания защитен профил.

2. След резултатите от прегледа и, когато е приложимо от повторната оценка, сертифициращият орган извършва едно от следните действия:

а) потвърждава сертификата по ЕССК;

б) оттегля сертификата по ЕССК в съответствие с член 20;

в) оттегля сертификата по ЕССК в съответствие с член 20 и издава нов сертификат по ЕССК с идентичен обхват и удължен срок на валидност;

г) оттегля сертификата по ЕССК в съответствие с член 20 и издава нов сертификат по ЕССК с различен обхват.

Член 20

Оттегляне на сертификат по ЕССК за защитен профил

1. Без да се засяга член 58, параграф 8, буква д) от Регламент (ЕС) 2019/881, сертификатът по ЕССК за защитен профил се оттегля от сертифициращия орган, който го е издал. Разпоредбите на член 14 се прилагат *mutatis mutandis*.

2. Един сертификат за защитен профил, издаден в съответствие с член 17, параграф 4, буква б), се оттегля от националния орган за сертифициране на киберсигурността, който го е одобрил.

ГЛАВА IV

ОРГАНИ ЗА ОЦЕНЯВАНЕ НА СЪОТВЕТСТВИЕТО

Член 21

Допълнителни или специфични изисквания към сертифициращия орган

1. Националният орган за сертифициране на киберсигурността упълномощава даден сертифициращ орган да издава сертификати по ЕССК с ниво на увереност „високо“, когато този орган докаже, че отговаря на изискванията, определени в член 60, параграф 1 и приложението към Регламент (ЕС) 2019/881 относно акредитацията на органите за оценяване на съответствието, както и на следните изисквания:

а) разполага с необходимите експертен опит и компетентност за вземане на решение за сертифициране на ниво на увереност „високо“;

б) извършва своите дейности по сертифициране в сътрудничество с ITSEF, упълномощен в съответствие с член 22; и

в) разполага с необходимата компетентност и е въвел подходящи технически и оперативни мерки за ефективна защита на поверителна и чувствителна информация за ниво на увереност „високо“, в допълнение към изискванията, посочени в член 43.

2. Националният орган за сертифициране на киберсигурността преценява дали даден сертифициращ орган отговаря на всички изисквания, посочени в параграф 1. Тази оценка включва най-малко структурирани интервюта и преглед на поне едно пилотно сертифициране, извършено от сертифициращия орган в съответствие с настоящия регламент.

В своето становище националният орган за сертифициране на киберсигурността може да използва повторно всяко подходящо доказателство от предишно разрешение или други подобни дейности, издадено в съответствие с:

а) настоящия регламент;

б) друга европейска схема за сертифициране на киберсигурността, приета съгласно член 49 от Регламент (ЕС) 2019/881;

в) национална схема, посочена в член 49 от настоящия регламент.

3. Националният орган за сертифициране на киберсигурността изготвя доклад за упълномощаване, който подлежи на партньорска проверка в съответствие с член 59, параграф 3, буква г) от Регламент (ЕС) 2019/881.

4. Националният орган за сертифициране на киберсигурността определя категориите ИКТ продукти и защитните профили, за които се отнася упълномощаването. Упълномощаването е валидно за срок, не по-дълъг от срока на валидност на акредитацията. То може да бъде подновено при поискване, при условие че сертифициращият орган продължава да отговаря на изискванията, посочени в настоящия член. За подновяване на разрешението не се изискват пилотни оценявания.

5. Националният орган за сертифициране на киберсигурността прекратява упълномощаването на сертифициращия орган, когато той вече не отговаря на условията, посочени в настоящия член. При прекратяване на упълномощаването сертифициращият орган незабавно спира да се представя като упълномощен сертифициращ орган.

Член 22

Допълнителни или специфични изисквания за ITSEF

1. Националният орган за сертифициране на киберсигурността упълномощава даден ITSEF да извършва оценка на ИКТ продукти, които подлежат на сертифициране при ниво на увереност „високо“, когато ITSEF докаже, че отговаря на изискванията, определени в член 60, параграф 1 и приложението към Регламент (ЕС) 2019/881 относно акредитацията на органите за оценяване на съответствието, както и на всички посочени по-долу условия:

а) разполага с необходимия експертен опит за извършване на дейностите по оценяване с цел определяне на устойчивостта срещу актуални кибератаки, осъществявани от лица със значителни умения и ресурси;

б) по отношение на техническите области и защитните профили, които са част от ИКТ процеса за тези ИКТ продукти, той разполага със:

1) експертни познания за извършване на конкретните дейности по оценяване, необходими за методичното определяне на устойчивостта на обекта на оценка срещу извършвани от опитни лица кибератаки, в неговата оперативна среда при допускане на потенциал за кибератака „умерен“ или „висок“, както е определено в стандартите, посочени в член 3;

2) техническата компетентност, посочена в актуалните технически документи, изброени в приложение I;

в) разполага с необходимата компетентност и е въвел подходящи технически и оперативни мерки за ефективна защита на поверителна и чувствителна информация за ниво на увереност „високо“, в допълнение към изискванията, посочени в член 43.

2. Националният орган за сертифициране на киберсигурността преценява дали даден ITSEF отговаря на всички изисквания, посочени в параграф 1. Тази оценка включва най-малко структурирани интервюта и преглед на поне едно пилотно оценяване, извършено от ITSEF в съответствие с настоящия регламент.

3. В своето становище националният орган за сертифициране на киберсигурността може да използва повторно всяко подходящо доказателство от предишно разрешение или други подобни дейности, издадено в съответствие с:

а) настоящия регламент;

б) друга европейска схема за сертифициране на киберсигурността, приета съгласно член 49 от Регламент (ЕС) 2019/881;

в) национална схема, посочена в член 49 от настоящия регламент.

4. Националният орган за сертифициране на киберсигурността изготвя доклад за упълномощаване, който подлежи на партньорска проверка в съответствие с член 59, параграф 3, буква г) от Регламент (ЕС) 2019/881.

5. Националният орган за сертифициране на киберсигурността определя категориите ИКТ продукти и защитните профили, за които се отнася упълномощаването. Упълномощаването е валидно за срок, не по-дълъг от срока на валидност на акредитацията. То може да бъде подновено при поискване, при условие че ITSEF продължава да отговаря на изискванията, посочени в настоящия член. За подновяване на разрешението не следва да се изискват пилотни оценявания.

6. Националният орган за сертифициране на киберсигурността прекратява упълномощаването на ITSEF, когато той вече не отговаря на условията, посочени в настоящия член. При прекратяване на упълномощаването ITSEF незабавно спира да се представя като упълномощен ITSEF.

Член 23

Уведомление относно сертифициращите органи

1. Националният орган за сертифициране на киберсигурността изпраща уведомление до Комисията относно сертифициращите органи на негова територия, които са компетентни да сертифицират за ниво на увереност „значително“ въз основа на своята акредитация.

2. Националният орган за сертифициране на киберсигурността изпраща уведомление до Комисията относно сертифициращите органи на негова територия, които са компетентни да сертифицират за ниво на увереност „високо“ въз основа на своята акредитация и решението за упълномощаването им.

3. Националният орган за сертифициране на киберсигурността предоставя най-малко следната информация, когато изпраща уведомление до Комисията относно сертифициращите органи:

а) нивото или нивата на увереност, за които сертифициращият орган е компетентен да издава сертификати по ЕССК;

б) следната информация относно акредитацията:

1) датата на акредитацията;

2) наименование и адрес на сертифициращия орган;

3) държавата на регистрация на сертифициращия орган;

4) референтния номер на акредитацията;

5) обхват и срок на валидност на акредитацията;

6) адреса, местоположението и връзка към съответния уебсайт на националния орган по акредитация; и

в) следната информация относно упълномощаването за ниво „високо“:

1) датата на решението за упълномощаване;

2) референтния номер на решението за упълномощаване;

3) срок на валидност на упълномощаването;

4) обхват на упълномощаването, включително най-високото ниво на AVA_VAN и, когато е приложимо, обхванатата техническа област.

4. Националният орган за сертифициране на киберсигурността изпраща копие от уведомлението, посочено в параграфи 1 и 2, на ENISA с оглед публикуването на точна информация относно допустимостта на сертифициращите органи на уебсайта за сертифициране на киберсигурността.

5. Националният орган по сертифициране на киберсигурността разглежда без неоправдано забавяне всяка информация относно промяна в статуса на акредитацията, предоставена от националния орган по акредитация. В случай на прекратяване на акредитацията или на упълномощаването националният орган за сертифициране на киберсигурността информира Комисията за това и може да подаде до нея искане в съответствие с член 61, параграф 4 от Регламент (ЕС) 2019/881.

Член 24

Уведомление относно ITSEF

Задълженията за уведомление от страна на националните органи за сертифициране на киберсигурността, посочени в член 23, се прилагат и за ITSEF. Уведомлението включва адреса на ITSEF, валидната акредитация и, когато е приложимо, валидното упълномощаване на съответния ITSEF.

ГЛАВА V

МОНИТОРИНГ, НЕСЪОТВЕТСТВИЕ И НЕСПАЗВАНЕ НА ИЗИСКВАНИЯ

РАЗДЕЛ I

Мониторинг за спазване на изисквания

Член 25

Дейности по мониторинг, извършвани от националния орган за сертифициране на киберсигурността

1. Без да се засяга член 58, параграф 7 от Регламент (ЕС) 2019/881, националният орган за сертифициране на киберсигурността следи за спазването на:

а) изискванията от страна на сертифициращия орган и ITSEF съгласно настоящия регламент и съгласно Регламент (ЕС) 2019/881;

б) изискванията от страна на титулярите на сертификати по ЕССК съгласно настоящия регламент и съгласно Регламент (ЕС) 2019/881;

в) посочените в ЕССК изисквания по отношение на сертифицираните ИКТ продукти;

г) увереността, посочена в сертификата по ЕССК, за справяне с променящата се обстановка по отношение на заплахите.

2. Националният орган за сертифициране на киберсигурността извършва своите дейности по мониторинг по-специално въз основа на:

а) информация, получена от сертифициращи органи, национални органи по акредитация и съответните органи за надзор на пазара;

б) информация, получена в резултат на собствени одити и разследвания или одити и разследвания на други органи;

в) проверка на извадки в съответствие с параграф 3;

г) получени жалби.

3. Националният орган за сертифициране на киберсигурността, в сътрудничество с други органи за надзор на пазара, ежегодно проверява извадка от най-малко 4 % от сертификатите по ЕСКС, определена чрез оценка на риска. При поискване и като действат от името на компетентния национален орган за сертифициране на киберсигурността, сертифициращите органи и, ако е необходимо, ITSEF подпомагат този орган при мониторинга на спазването на изискванията.

4. Националният орган за сертифициране на киберсигурността подбира извадката от сертифицирани ИКТ продукти за проверка, като използва обективни критерии, включително:

а) категория продукти;

б) нива на увереност на продуктите;

в) титуляр на сертификата;

г) сертифициращ орган и, когато е приложимо, ITSEF, действащ като подизпълнител;

д) всяка друга информация, предоставена на вниманието на органа.

5. Националният орган за сертифициране на киберсигурността информира титулярите на сертификатите по ЕССК за избраните ИКТ продукти и за критериите за подбор.

6. По искане на националния орган за сертифициране на киберсигурността и със съдействието на съответния ITSEF сертифициращият орган, който е сертифицирал ИКТ продукта, включен в извадката, извършва допълнителен преглед в съответствие с процедурата, определена в раздел IV.2 от приложение IV, и информира националния орган за сертифициране на киберсигурността за резултатите.

7. Когато националният орган за сертифициране на киберсигурността има достатъчно основания да смята, че сертифициран ИКТ продукт вече не отговаря на изискванията на настоящия регламент или на Регламент (ЕС) 2019/881, той може да провежда разследвания или да използва всички други правомощия за мониторинг, посочени в член 58, параграф 8 от Регламент (ЕС) 2019/881.

8. Националният орган за сертифициране на киберсигурността информира съответния сертифициращ орган и ITSEF за текущите разследвания по отношение на избрани ИКТ продукти.

9. Когато националният орган за сертифициране на киберсигурността установи, че текущо разследване засяга ИКТ продукти, които са сертифицирани от органи за сертифициране, установени в други държави членки, той информира за това националните органи за сертифициране на киберсигурността на съответните държави членки, за да си сътрудничат при разследванията, когато е уместно. Този национален орган за сертифициране на киберсигурността също така уведомява Европейската група за сертифициране на киберсигурността за трансграничните разследвания и последващите резултати.

Член 26

Дейности по мониторинг, извършвани от сертифициращия орган

1. Сертифициращият орган следи за:

а) спазването на изискванията от страна на титулярите на сертификати съгласно настоящия регламент и Регламент (ЕС) 2019/881 по отношение на сертификатите по ЕССК, издадени от сертифициращия орган;

б) съответствието на сертифицираните от него ИКТ продукти с приложимите спрямо тях изисквания за сигурност;

в) увереността, посочена в сертифицираните защитни профили.

2. Сертифициращият орган извършва своите дейности по мониторинг въз основа на:

а) информацията, предоставена по силата на ангажиментите на заявителя за сертифициране, посочени в член 9, параграф 2;

б) информацията, произтичаща от дейностите на други съответни органи за надзор на пазара;

в) получени жалби;

г) информация за уязвимости, които биха могли да засегнат сертифицираните от него ИКТ продукти.

3. Националният орган за сертифициране на киберсигурността може да изготви правила за периодичен диалог между сертифициращите органи и титулярите на сертификати по ЕССК, с цел да се проверява и докладва за спазването на ангажиментите, поети съгласно член 9, параграф 2, без да се засягат дейностите, свързани с други съответни органи за надзор на пазара.

Член 27

Дейности по мониторинг, извършвани от титуляря на сертификат

1. Титулярят на сертификат по ЕССК изпълнява следните задачи, за да следи за съответствието на сертифицирания ИКТ продукт със съответните изисквания за сигурност:

а) следи информацията за уязвимостта на сертифицирания ИКТ продукт, включително известните зависимости, със собствени средства, но и като взема предвид:

1) публикация или информация за уязвимост, подадена от ползвател или изследовател в областта на сигурността, посочени в член 55, параграф 1, буква в) от Регламент (ЕС) 2019/881;

2) информация от друг източник;

б) следи за увереността, посочена в сертификата по ЕССК.

2. Титулярят на сертификат по ЕССК работи в сътрудничество със сертифициращия орган, с ITSEF и, когато е приложимо, с националния орган за сертифициране на киберсигурността, за да подпомага техните дейности по мониторинг.

РАЗДЕЛ II

Съответствие и спазване на изисквания

Член 28

Последици при несъответствие на сертифициран ИКТ продукт или на защитен профил

1. Когато сертифициран ИКТ продукт или защитен профил не отговаря на изискванията, определени в настоящия регламент и в Регламент (ЕС) 2019/881, сертифициращият орган информира титуляря на сертификата по ЕССК за установеното несъответствие и изисква да бъдат предприети корективни действия.

2. Когато даден случай на несъответствие с разпоредбите на настоящия регламент може да засегне съответствието с друг приложим законодателен акт на Съюза, в който се предвижда възможност за доказване на презумпцията за съответствие с изискванията на този правен акт чрез използване на сертификата по ЕССК, сертифициращият орган незабавно информира националния орган за сертифициране на киберсигурността. Националният орган за сертифициране на киберсигурността незабавно уведомява органа за надзор на пазара, отговарящ за такъв друг съответен законодателен акт на Съюза, за установения случай на несъответствие.

3. При получаване на информацията, посочена в параграф 1, титулярят на сертификата по ЕССК в рамките на определения от сертифициращия орган срок, който не надвишава 30 дни, предлага на сертифициращия орган коригиращото действие, необходимо за отстраняване на несъответствието.

4. Сертифициращият орган може да спре действието на сертификата по ЕССК без неоправдано забавяне в съответствие с член 30 в случай на спешност или в случай че титулярят на сертификата по ЕССК не оказва надлежно сътрудничество на сертифициращия орган.

5. Сертифициращият орган извършва преглед в съответствие с членове 13 и 19, като преценява дали коригиращото действие води до отстраняване на несъответствието.

6. Когато титулярят на сертификата по ЕССК не предложи подходящи коригиращи действия в срока, посочен в параграф 3, действието на сертификата се спира в съответствие с член 30 или сертификатът се оттегля в съответствие с членове 14 или 20.

7. Настоящият член не се прилага за случаи на уязвимости, засягащи сертифициран ИКТ продукт, които се разглеждат в съответствие с глава VI.

Член 29

Последици от неспазване на изискванията от страна на титуляря на сертификат

1. Когато сертифициращият орган установи, че:

а) титулярят на сертификат по ЕССК или заявителят за сертифициране не спазва своите ангажименти и задължения, посочени в член 9, параграф 2, член 17, параграф 2, член 27 и член 41; или

б) титулярят на сертификат по ЕССК не спазва член 56, параграф 8 от Регламент (ЕС) 2019/881 или глава VI от настоящия регламент;

той определя срок не по-дълъг от 30 дни, в който титулярят на сертификат по ЕССК предприема коригиращи действия.

2. Когато титулярят на сертификата по ЕССК не предложи подходящи коригиращи действия в срока, посочен в параграф 1, действието на сертификата се спира в съответствие с член 30 или сертификатът се оттегля в съответствие с член 14 и член 20.

3. Продължаващо или многократно нарушение от страна на титуляря на сертификата по ЕССК на задълженията, посочени в параграф 1, води до оттегляне на сертификата по ЕССК в съответствие с член 14 или член 20.

4. Сертифициращият орган информира националния орган за сертифициране на киберсигурността за констатациите, посочени в параграф 1. Когато случаят на неспазване на изискванията засяга спазването на друг приложим законодателен акт на Съюза, националният орган за сертифициране на киберсигурността незабавно уведомява органа за надзор на пазара, отговарящ за другия приложим законодателен акт на Съюза, за установения случай на неспазване.

Член 30

Спиране на действието на сертификата по ЕССК

1. Когато в настоящия регламент се предвижда спиране на действието на сертификат по ЕССК, сертифициращият орган спира действието на съответния сертификат по ЕССК за срок, съобразен с обстоятелствата, довели до спирането, който не надвишава 42 дни. Срокът на спиране на действието започва да тече от деня, следващ деня на решението на сертифициращия орган. Спирането на действието не засяга валидността на сертификата.

2. Сертифициращият орган уведомява титуляря на сертификата и националния орган за сертифициране на киберсигурността за спирането без неоправдано забавяне и посочва причините за спирането, изискваните действия, които трябва да бъдат предприети, и срока на спиране на действието.

3. Титулярят на сертификата уведомява купувачите на съответните ИКТ продукти за спирането на действието му и за причините, посочени от сертифициращия орган за това спиране, с изключение на онези части от причините, чието споделяне би представлявало риск за сигурността или които съдържат чувствителна информация. Тази информация се оповестява публично от титуляря на сертификата.

4. В случай че в друг приложим законодателен акт на Съюза се предвижда презумпция за съответствие въз основа на сертификати, издадени съгласно разпоредбите на настоящия регламент, националният орган за сертифициране на киберсигурността информира органа за надзор на пазара, отговарящ за другия приложим законодателен акт на Съюза, за спирането на действието.

5. Спирането на действието на даден сертификат се съобщава на ENISA в съответствие с член 42, параграф 3.

6. В надлежно обосновани случаи националният орган за сертифициране на киберсигурността може да разреши удължаване на срока на спиране на действието на сертификат по ЕССК. Общият срок на спиране на действието не може да надвишава 1 година.

Член 31

Последици от неспазване на изискванията от страна на органа за оценяване на съответствието

1. В случай че даден сертифициращ орган не спазва задълженията си или в случай че ITSEF установи, че съответният сертифициращ орган не спазва изискванията, националният орган за сертифициране на киберсигурността без неоправдано забавяне:

а) установява, с подкрепата на съответния ITSEF, потенциално засегнатите сертификати по ЕССК;

б) ако е необходимо, изисква да бъдат извършени дейности по оценяване на един или повече ИКТ продукти или защитни профили или от ITSEF, който е извършил оценката, или от друг акредитиран и, когато е приложимо, упълномощен ITSEF, който може да е в по-добра позиция в техническо отношение да подпомогне това установяване;

в) анализира въздействието на неспазването на изискванията;

г) уведомява титуляря на сертификата по ЕССК, засегнат от неспазването на изискванията.

2. Въз основа на мерките, посочени в параграф 1, сертифициращият орган приема едно от следните решения по отношение на всеки засегнат сертификат по ЕССК:

а) сертификатът по ЕССК се запазва в непроменен вид;

б) сертификатът по ЕССК се оттегля в съответствие с член 14 или член 20 и, когато е целесъобразно, се издава нов сертификат по ЕССК.

3. Въз основа на мерките, посочени в параграф 1, националният орган за сертифициране на киберсигурността:

а) докладва, ако е необходимо, на националния орган по акредитация за неспазването на изискванията от страна на сертифициращия орган или на свързания с него ITSEF;

б) оценява, ако е приложимо, потенциалното въздействие върху упълномощаването.

ГЛАВА VI

УПРАВЛЕНИЕ И ОПОВЕСТЯВАНЕ НА УЯЗВИМОСТИТЕ

Член 32

Обхват на управлението на уязвимостите

Настоящата глава се прилага за ИКТ продукти, за които е издаден сертификат по ЕССК.

РАЗДЕЛ I

УПРАВЛЕНИЕ НА УЯЗВИМОСТИТЕ

Член 33

Процедури за управление на уязвимостите

1. Титулярят на сертификат по ЕССК установява и поддържа всички необходими процедури за управление на уязвимостите в съответствие с правилата, установени в настоящия раздел, и когато е необходимо, допълнени от процедурите, установени в EN ISO/IEC 30111.

2. Титулярят на сертификат по ЕССК поддържа и публикува подходящи методи за получаване на информация за уязвимости, свързани с неговите продукти, от външни източници, включително от ползватели, сертифициращи органи и изследователи в областта на сигурността.

3. Когато титуляр на сертификат по ЕССК открие или получи информация за потенциална уязвимост, засягаща сертифициран ИКТ продукт, той я регистрира и извършва анализ на въздействието на уязвимостта.

4. Когато потенциална уязвимост оказва въздействие върху съставен продукт, титулярят на сертификата по ЕССК информира титуляря на зависимите сертификати по ЕССК за потенциалната уязвимост.

5. В отговор на обосновано искане от сертифициращия орган, издал сертификата, титулярят на сертификат по ЕССК предава на този сертифициращ орган цялата съответна информация за потенциални уязвимости.

Член 34

Анализ на въздействието на уязвимостта

1. Анализът на въздействието на уязвимостта се позовава на целта на оценката и на декларациите за достоверност, съдържащи се в сертификата. Анализът на въздействието на уязвимостта се извършва в срок, съобразен с риска от експлоатиране и критичността на потенциалната уязвимост на сертифицирания ИКТ продукт.

2. Когато е приложимо, се извършва изчисление на потенциала за кибератака съгласно съответната методика, включена в стандартите, посочени в член 3, и съответните актуални технически документи, изброени в приложение I, за да се определи възможността за използване на уязвимостта. Взема се предвид нивото на AVA_VAN на сертификата по ЕССК.

Член 35

Доклад за анализ на въздействието на уязвимостта

1. Титулярят на сертификата изготвя доклад за анализ на въздействието на уязвимостта, когато анализът на въздействието показва, че уязвимостта има вероятно въздействие върху съответствието на ИКТ продукта със сертификата му.

2. Докладът за анализ на въздействието на уязвимостта съдържа оценка на следните елементи:

а) въздействието на уязвимостта върху сертифицирания ИКТ продукт;

б) възможни рискове, свързани с близостта или наличието на кибератака;

в) дали уязвимостта може да бъде коригирана;

г) в случаите, в които уязвимостта може да бъде коригирана, възможни решения за нейното отстраняване.

3. Докладът за анализ на въздействието на уязвимостта съдържа, когато е приложимо, подробна информация за възможните начини за използване на уязвимостта. Информацията, отнасяща се до възможните начини за използване на уязвимостта, се обработва в съответствие с подходящи мерки за сигурност, за да се защити нейната поверителност и да се обезпечи, ако е необходимо, ограниченото ѝ разпространение.

4. Титулярят на сертификата по ЕССК предава без ненужно забавяне доклад от анализ на въздействието на уязвимостта на сертифициращия орган или на националния орган за сертифициране на киберсигурността в съответствие с член 56, параграф 8 от Регламент (ЕС) 2019/881.

5. Когато в доклада за анализ на въздействието на уязвимостта се констатира, че уязвимостта не е остатъчна по смисъла на стандартите, посочени в член 3, и че тя може да бъде отстранена, се прилага член 36.

6. Когато в доклада за анализ на въздействието на уязвимостта се констатира, че уязвимостта не е остатъчна и че тя не може да бъде коригирана, сертификатът по ЕССК се оттегля в съответствие с член 14.

7. Титулярят на сертификат по ЕССК наблюдава всички остатъчни уязвимости, за да гарантира, че те не могат да бъдат експлоатирани в случай на промени в оперативната среда.

Член 36

Коригиране на уязвимости

Титулярят на сертификата по ЕССК представя на сертифициращия орган предложение за подходящо коригиращо действие. Сертифициращият орган извършва преглед на сертификата по ЕССК в съответствие с член 13. Обхватът на прегледа се определя от предложените мерки за отстраняване на уязвимостта.

РАЗДЕЛ II

ОПОВЕСТЯВАНЕ НА УЯЗВИМОСТ

Член 37

Информация, споделяна с националния орган за сертифициране на киберсигурността

1. Информацията, предоставяна от сертифициращия орган на националния орган за сертифициране на киберсигурността, включва всички елементи, необходими на националния орган за сертифициране на киберсигурността, за да разбере въздействието на уязвимостта, промените, които трябва да бъдат направени в ИКТ продукта, и, когато е налична, всякаква информация от сертифициращия орган относно по-широките последици от уязвимостта за други сертифицирани ИКТ продукти.

2. Информацията, предоставена в съответствие с параграф 1, не съдържа подробности за начините за използване на уязвимостта. Настоящата разпоредба не засяга правомощията за разследване на националния орган за сертифициране на киберсигурността.

Член 38

Сътрудничество с други национални органи за сертифициране на киберсигурността

1. Националният орган за сертифициране на киберсигурността споделя важната информация, получена в съответствие с член 37, с други национални органи за сертифициране на киберсигурността, както и с ENISA.

2. Другите национални органи за сертифициране на киберсигурността могат да решат да направят допълнителен анализ на уязвимостта или, след като информират титуляря на сертификата по ЕССК, да поискат от съответните органи за сертифициране да преценят дали уязвимостта може да засегне други сертифицирани ИКТ продукти.

Член 39

Публикуване на уязвимостта

След оттегляне на даден сертификат титулярят на сертификата по ЕССК оповестява и регистрира всяка публично известна и коригирана уязвимост в ИКТ продукта в европейската база данни за уязвимости, създадена в съответствие с член 12 от

Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета ([5]), или в други онлайн хранилища, посочени в член 55, параграф 1, буква г) от Регламент (ЕС) 2019/881.

ГЛАВА VII

СЪХРАНЕНИЕ, ОПОВЕСТЯВАНЕ И ЗАЩИТА НА ИНФОРМАЦИЯТА

Член 40

Съхранение на деловодни записи от сертифициращите органи и ITSEF

1. ITSEF и сертифициращите органи поддържат деловодна система, която съдържа всички документи, изготвени във връзка с всяка извършена от тях оценка и сертифициране.

2. Сертифициращите органи и ITSEF съхраняват деловодните записи по сигурен начин и ги пазят за периода, необходим за целите на настоящия регламент, и най-малко 5 години след оттеглянето на съответния сертификат по ЕССК. Когато сертифициращият орган е издал нов сертификат по ЕССК в съответствие с член 13, параграф 2, буква в), той съхранява документацията за оттегления сертификат по ЕССК заедно с тази за новия сертификат по ЕССК и за същия период от време като тази за новия сертификат по ЕССК.

Член 41

Информация, предоставяна от титуляря на сертификата

1. Информацията, посочена в член 55 от Регламент (ЕС) 2019/881, се предоставя на език, който е лесно достъпен за ползвателите.

2. Титулярят на сертификат по ЕССК съхранява на сигурно място следните данни за периода, необходим за целите на настоящия регламент, и най-малко 5 години след оттеглянето на съответния сертификат по ЕССК:

а) деловодни записи на информацията, предоставена на сертифициращия орган и на ITSEF по време на процеса на сертифициране;

б) образец на сертифицирания ИКТ продукт.

3. Когато сертифициращият орган е издал нов сертификат по ЕССК в съответствие с член 13, параграф 2, буква в), титулярят на сертификата съхранява документацията за оттегления сертификат по ЕССК заедно с тази за новия сертификат по ЕССК и за същия период от време като тази за новия сертификат по ЕССК.

4. При поискване от страна на сертифициращия орган или на националния орган за сертифициране на киберсигурността титулярят на сертификат по ЕССК предоставя деловодните записи и копията, посочени в параграф 2.

Член 42

Информация, която трябва да бъде предоставена от ENISA

1. ENISA публикува следната информация на уебсайта, посочен в член 50, параграф 1 от Регламент (ЕС) 2019/881:

а) всички сертификати по ЕССК;

б) информация за статуса на даден сертификат по ЕССК, а именно дали той е в сила, дали действието му е спряно, дали е оттеглен, или е с изтекъл срок;

в) сертификационните доклади, съответстващи на всеки сертификат по ЕССК;

([5]) 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).

г) списък на акредитираните органи за оценяване на съответствието;

д) списък на упълномощените органи за оценяване на съответствието;

е) актуалните технически документи, изброени в приложение I;

ж) становищата на Европейската група за сертифициране на киберсигурността, посочена в член 62, параграф 4, буква в) от Регламент (ЕС) 2019/881;

з) доклади за партньорска оценка, издадени в съответствие с член 47.

2. Информацията, посочена в параграф 1, се предоставя поне на английски език.

3. Сертифициращите органи и, когато е приложимо, националните органи за сертифициране на киберсигурността информират незабавно ENISA за своите решения, които засягат съдържанието или статуса на даден сертификат по ЕССК, както е посочено в параграф 1, буква б).

4. ENISA гарантира, че в информацията, публикувана в съответствие с параграф 1, букви а), б) и в), ясно се посочват версиите на даден сертифициран ИКТ продукт, които са обхванати от сертификата по ЕССК.

Член 43

Защита на информацията

Органите за оценяване на съответствието, националните органи за сертифициране на киберсигурността, Европейската група за сертифициране на киберсигурността, ENISA, Комисията и всички други страни гарантират сигурността и защитата на търговски тайни и друга поверителна информация, включително от търговски характер, както и запазването на правата върху интелектуалната собственост, и предприемат необходимите и подходящи технически и организационни мерки.

ГЛАВА VIII

СПОРАЗУМЕНИЯ ЗА ВЗАИМНО ПРИЗНАВАНЕ С ТРЕТИ ДЪРЖАВИ

Член 44

Условия

1. Трети държави, които желаят да сертифицират своите продукти в съответствие с настоящия регламент и които искат това сертифициране да бъде признато в рамките на Съюза, сключват споразумение за взаимно признаване със Съюза.

2. Споразумението за взаимно признаване обхваща приложимите нива на увереност за сертифицираните ИКТ продукти и, когато е приложимо, защитните профили.

3. Споразумения за взаимно признаване, посочени в параграф 1, могат да се сключват само с трети държави, които отговарят на следните условия:

а) разполагат с орган, който:

1) е публичен орган, независим от субектите, които наблюдава и контролира, по отношение на организационната и правната структура, финансовото обезпечаване и вземането на решения;

2) разполага с подходящи правомощия за мониторинг и надзор, за да извършва разследвания, и е оправомощен да предприема подходящи коригиращи мерки, за да гарантира спазването на изискванията;

3) разполага с ефективна, пропорционална и възпираща система от санкции, за да гарантира спазването на изискванията;

4) приема да си сътрудничи с Европейската група за сертифициране на киберсигурността и с ENISA за обмен на най-добри практики и важни разработки в областта на сертифицирането на киберсигурността и да работи за уеднаквяване на тълкуването на приложимите понастоящем критерии и методи за оценка, наред с другото, чрез прилагане на хармонизирана документация, която е равностойна на актуалните технически документи, изброени в приложение I;

б) разполагат с независим орган по акредитация, който извършва акредитации по стандарти, равностойни на посочените в Регламент (ЕО) № 765/2008;

в) поемат ангажимента, че процесите и процедурите по оценяване и сертифициране ще се извършват надлежно и професионално, като се отчита спазването на международните стандарти, посочени в настоящия регламент, и по-специално в член 3;

г) разполагат с капацитет за докладване на неоткрити преди това уязвимости и с установена, адекватна процедура за управление и оповестяване на уязвимости;

д) разполагат с установени процедури, които им позволяват ефективно подаване и разглеждане на жалби и обезпечаване на ефективна правна защита на жалбоподателя;

е) създават механизъм за сътрудничество с други органи на Съюза и на държавите членки, имащи отношение към сертифицирането на киберсигурността съгласно настоящия регламент, включително обмен на информация за евентуални несъответствия на сертификатите, мониторинг на значимите промени в областта на сертифицирането и осигуряване на съвместен подход към поддържането и прегледа на сертификатите.

4. В допълнение към условията, изложени в параграф 3, споразумение за взаимно признаване съгласно параграф 1, обхващащо ниво на увереност „високо“, може да бъде сключено с трети държави само ако са изпълнени и следните условия:

а) третата държава разполага с независим и публичен орган за сертифициране на киберсигурността, който извършва или делегира дейности по оценяване, необходими за сертифициране с ниво на увереност „високо“, които са равностойни на изискванията и процедурите, определени за националните органи за киберсигурност в настоящия регламент и в Регламент (ЕС) 2019/881;

б) в споразумението за взаимно признаване се създава съвместен механизъм, равностоен на партньорската оценка за сертифициране по ЕССК, за да се подобри обменът на практики и да се решават съвместно въпроси в областта на оценяването и сертифицирането.

ГЛАВА IX

ПАРТНЬОРСКА ОЦЕНКА НА СЕРТИФИЦИРАЩИТЕ ОРГАНИ

Член 45

Процедура за партньорска оценка

1. Сертифициращият орган, който издава сертификати по ЕССК с ниво на увереност „високо“, се подлага на партньорска оценка редовно и най-малко на всеки пет години. Различните типове партньорски оценки са изброени в приложение VI.

2. Европейската група за сертифициране на киберсигурността изготвя и поддържа график на партньорските оценки, като гарантира спазването на тази периодичност. Освен в надлежно обосновани случаи, партньорските оценки се извършват на място.

3. Партньорската оценка може да се основава на доказателства, събрани в хода на предишни партньорски оценки или равностойни процедури на подложен на партньорска оценка сертифициращ орган или национален орган за сертифициране на киберсигурността, при условие че:

а) резултатите не са по-стари от 5 години;

б) резултатите се придружават от описание на процедурите за партньорска оценка, установени за тази схема, когато те се отнасят за партньорска оценка, извършена по друга схема за сертифициране;

в) в доклада за партньорска оценка, посочен в член 47, се указва кои резултати са използвани повторно със или без допълнителна оценка.

4. Когато партньорската оценка обхваща техническа област, съответният ITSEF също се оценява.

5. Сертифициращият орган, подложен на партньорска оценка, и когато е необходимо, националният орган за сертифициране на киберсигурността гарантират, че цялата информация от значение е на разположение на екипа за партньорската оценка.

6. Партньорската оценка се извършва от екип за партньорска оценка, създаден в съответствие с приложение VI.

Член 46

Етапи на партньорската оценка

1. По време на подготвителния етап членовете на екипа за партньорска оценка преглеждат документацията на сертифициращия орган, обхващаща неговите политики и процедури, включително използването на актуалните технически документи.

2. По време на етапа на посещение на място екипът за партньорска оценка оценява техническата компетентност на органа и, когато е приложимо, компетентността на ITSEF, който е извършил най-малко оценка на един ИКТ продукт, обхванат от партньорската оценка.

3. Продължителността на етапа на посещение на място може да бъде удължена или намалена в зависимост от фактори като възможността за повторно използване на съществуващите доказателства и резултатите от партньорската оценка или броя на ITSEF и техническите области, за които сертифициращият орган издава сертификати.

4. Ако е приложимо, екипът за партньорска оценка определя техническата компетентност на всеки ITSEF, като посещава неговата техническа лаборатория или лаборатории и задава въпроси на неговите оценители относно техническата област и свързаните с нея специфични методи за кибератака.

5. На етапа на докладване екипът за оценка документира своите констатации в доклад за партньорска оценка, включващ решение и, когато е приложимо, списък на констатираните несъответствия, всяко от които е степенувано по ниво на критичност.

6. Докладът за партньорска оценка трябва първо да бъде обсъден със сертифициращия орган, подложен на партньорска оценка. След обсъжданията сертифициращият орган, подложен на партньорска оценка, изготвя график на мерките, които трябва да бъдат предприети за отстраняване на констатираните недостатъци.

Член 47

Доклад за партньорска оценка

1. Екипът за партньорска оценка предоставя на сертифициращия орган, подложен на партньорска оценка, проект на доклада за партньорска оценка.

2. Сертифициращият орган, подложен на партньорска оценка, представя на екипа за партньорска оценка коментари относно констатациите и списък с ангажименти за отстраняване на недостатъците, установени в проекта на доклада за партньорска оценка.

3. Екипът за партньорска оценка представя на Европейската група за сертифициране на киберсигурността окончателен доклад за партньорска оценка, който включва също така коментарите и ангажиментите, поети от сертифициращия орган, подложен на партньорска оценка. Екипът за партньорска оценка включва и своята позиция по коментарите и дали тези ангажименти са достатъчни за отстраняване на установените недостатъци.

4. Когато в доклада за партньорска оценка са установени несъответствия, Европейската група за сертифициране на киберсигурността може да определи подходящ срок за тяхното отстраняване от сертифициращия орган, подложен на партньорска оценка.

5. Европейската група за сертифициране на киберсигурността приема становище по доклада за партньорска оценка:

а) когато в доклада за партньорска оценка не са установени несъответствия или когато несъответствията са отстранени по подходящ начин от сертифициращия орган, подложен на партньорска оценка, Европейската група за сертифициране на киберсигурността може да издаде положително становище и всички съответни документи се публикуват на уебсайта на ENISA за сертифициране;

б) когато сертифициращият орган, подложен на партньорска оценка, не отстрани несъответствията по подходящ начин в определения срок, Европейската група за сертифициране на киберсигурността може да издаде отрицателно становище, което се публикува на уебсайта на ENISA за сертифициране заедно с доклада за партньорска оценка и всички съответни документи.

6. Преди публикуването на становището цялата чувствителна, лична или защитена фирмена информация се премахва от публикуваните документи.

ГЛАВА X

ПОДДЪРЖАНЕ НА СХЕМАТА

Член 48

Поддържане на ЕССК

1. Комисията може да поиска от Европейската група за сертифициране на киберсигурността да приеме становище с оглед на поддържането на ЕССК и да предприеме необходимите подготвителни дейности.

2. Европейската група за сертифициране на киберсигурността може да приеме становище, с което да одобри актуалните технически документи.

3. Актуалните технически документи, които са одобрени от Европейската група за сертифициране на киберсигурността, се публикуват от ENISA.

ГЛАВА XI

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 49

Национални схеми, обхванати от ЕССК

1. В съответствие с член 57, параграф 1 от Регламент (ЕС) 2019/881 и без да се засяга член 57, параграф 3 от посочения регламент, всички национални схеми за сертифициране на киберсигурността и свързаните с тях процедури за ИКТ продукти и ИКТ процеси, които попадат в обхвата на ЕССК, престават да пораждат действие 12 месеца след влизането в сила на настоящия регламент.

2. Чрез дерогация от член 50 процес на сертифициране може да бъде стартиран по национална схема за сертифициране на киберсигурността в рамките на 12 месеца след влизането в сила на настоящия регламент, при условие че процесът на сертифициране бъде завършен не по-късно от 24 месеца след влизането в сила на настоящия регламент.

3. Сертификатите, издадени в рамките на национални схеми за сертифициране на киберсигурността, могат да бъдат подложени на преглед. Нови сертификати, заместващи подложените на преглед сертификати, се издават в съответствие с настоящия регламент.

Член 50

Влизане в сила

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

Той се прилага от 27 февруари 2025 г.

Глава IV и приложение V се прилагат от датата на влизане в сила на настоящия регламент.

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

Съставено в Брюксел на 31 януари 2024 година.

За Комисията
Председател
Ursula VON DER LEYEN

ПРИЛОЖЕНИЕ I

Техническа област и актуални технически документи

1. Технически области на ниво 4 или 5 на AVA_VAN:

   а) документи, свързани с хармонизираната оценка на техническата област „Смарт карти и подобни устройства“, и по-специално следните документи в съответните им версии, които са в сила на [дата на влизане в сила]:

      1) „Минимални изисквания на ITSEF за оценяване на сигурността на смарт карти и подобни устройства“, одобрен първоначално от Европейската група за сертифициране на киберсигурността на 20 октомври 2023 г.;

      2) „Минимални изисквания за сигурност на обекти“, одобрен първоначално от Европейската група за сертифициране на киберсигурността на 20 октомври 2023 г.;

      3) „Прилагане на общи критерии спрямо интегралните схеми“, одобрен първоначално от Европейската група за сертифициране на киберсигурността на 20 октомври 2023 г.;

      4) „Изисквания по отношение на архитектурата за информационна сигурност (ADV_ARC) за смарт карти и подобни устройства“, одобрен първоначално от Европейската група за сертифициране на киберсигурността на 20 октомври 2023 г.;

      5) „Сертифициране на „отворени“ продукти за смарт карти“, одобрен първоначално от Европейската група за сертифициране на киберсигурността на 20 октомври 2023 г.;

      6) „Оценка на съставни продукти за смарт карти и подобни устройства“, одобрен първоначално от Европейската група за сертифициране на киберсигурността на 20 октомври 2023 г.;

      7) „Прилагане на потенциала за кибератака спрямо смарт картите“, одобрен първоначално от Европейската група за сертифициране на киберсигурността на 20 октомври 2023 г.;

   б) документи, свързани с хармонизираната оценка на техническата област „Хардуерни устройства с кутии за сигурност“, и по-специално следните документи в съответните им версии, които са в сила на [дата на влизане в сила]:

      1) „Минимални изисквания на ITSEF за оценяване на сигурността на хардуерни устройства с кутии за сигурност“, одобрен първоначално от Европейската група за сертифициране на киберсигурността на 20 октомври 2023 г.;

      2) „Минимални изисквания за сигурност на обекти“, одобрен първоначално от Европейската група за сертифициране на киберсигурността на 20 октомври 2023 г.;

      3) „Прилагане на потенциала за кибератака спрямо хардуерни устройства с кутии за сигурност“, одобрен първоначално от Европейската група за сертифициране на киберсигурността на 20 октомври 2023 г.;

2. Актуални технически документи в съответните им версии, които са в сила на [дата на влизане в сила]:

   а) документ, свързан с хармонизираната акредитация на органите за оценяване на съответствието: „Акредитация на ITSEF за ЕССК“, одобрен първоначално от Европейската група за сертифициране на киберсигурността на 20 октомври 2023 г.

ПРИЛОЖЕНИЕ II

Защитни профили, сертифицирани на ниво 4 или 5 на AVA_VAN

1. За категорията „Устройства за създаване на квалифициран електронен подпис и печат от разстояние“:

1) EN 419241-2:2019 — Надеждни системи, поддържащи сървърно подписване. Част 2: Защитни профили за QSCD за сървърно подписване;

2) EN 419221-5:2018 — Защитни профили за TSP криптографски модули. Част 5: Криптографски модул за удостоверителни услуги

2. Защитни профили, които са били приети като актуални технически документи:

[ПРАЗНО ПОЛЕ]

ПРИЛОЖЕНИЕ III

Препоръчани защитни профили (илюстриращи техническите области от приложение I)

Защитни профили (ЗП), използвани при сертифицирането на ИКТ продукти, попадащи в посочената по-долу категория ИКТ продукти:

а) за категорията „Машинночетими документи за пътуване“:

1) ЗП за машинночетим документ за пътуване с използване на стандартна процедура за проверка с PACE, BSI-CC-PP-0068-V2-2011-MA-01;

2) ЗП за машинночетим документ за пътуване с разширен контрол на достъпа на „Приложение на ИКАО“, BSI-CC-PP-0056-2009;

3) ЗП за машинночетим документ за пътуване с разширен контрол на достъпа на „Приложение на ИКАО“ с PACE, BSI-CC-PP-0056-V2-2012-MA-02;

4) ЗП за машинночетим документ за пътуване с основен контрол на достъпа на „Приложение на ИКАО“, BSI-CC-PP-0055-2009;

б) за категорията „Устройства за създаване на защитени подписи“:

1) EN 419211-1:2014 — Профил на защита за устройства за създаване на сигурен електронен подпис. Част 1: Преглед

2) EN 419211-2:2013 — Защитни профили за устройство за създаване на защитени подписи. Част 2: Устройство с генериране на ключове;

3) EN 419211-3:2013 — Защитни профили за устройство за създаване на защитени подписи. Част 3: Устройство с внасяне на ключове;

4) EN 419211-4:2013 — Защитни профили за устройство за създаване на защитени подписи. Част 4: Разширение за устройство с генериране на ключове и надежден канал към приложение за генериране на сертификати;

5) EN 419211-5:2013 — Защитни профили за устройство за създаване на защитени подписи. Част 5: Разширение за устройство с генериране на ключове и надежден канал към приложение за създаване на подписи;

6) EN 419211-6:2014 — Защитни профили за устройство за създаване на защитени подписи. Част 6: Разширение за устройство с внасяне на ключове и надежден канал към приложение за създаване на подписи;

в) за категорията „Цифрови тахографи“:

1) цифров тахограф — тахографска карта, както е посочено в Регламент за изпълнение (ЕС) 2016/799 на Комисията от 18 март 2016 г. за прилагане на Регламент (ЕС) № 165/2014 (приложение 1B);

2) цифров тахограф — бордово устройство, както е посочено в приложение IБ към Регламент (ЕО) № 1360/2002 на Комисията, предназначено за монтиране в пътни превозни средства;

3) цифров тахограф — външно устройство за GNSS (ЗП за външно устройство за GNSS), както е посочено в приложение 1B към Регламент за изпълнение (ЕС) 2016/799 на Комисията от 18 март 2016 г. за прилагане на Регламент (ЕС) № 165/2014 на Европейския парламент и на Съвета;

4) цифров тахограф — датчик за движение (ЗП за ДД), както е посочено в приложение 1B към Регламент за изпълнение (ЕС) 2016/799 на Комисията от 18 март 2016 г. за прилагане на Регламент (ЕС) № 165/2014 на Европейския парламент и на Съвета;

г) за категорията „Защитени интегрални схеми, смарт карти и свързани с тях устройства“:

1) ЗП за платформа за сигурност на интегрални схеми, BSI-CC-PP-0084-2014;

2) Java Card System — отворена конфигурация, в. 3.0.5 BSI-CC-PP-0099-2017;

3) Java Card System — затворена конфигурация, BSI-CC-PP-0101-2017;

4) ЗП за настолен компютър за специфичен клиентски доверен платформен модул за група 2.0, ниво 0, версия 1.16, ANSSI-CC-PP-2015/07;

5) универсална SIM карта, PU-2009-RT-79, ANSSI-CC-PP-2010/04;

6) вградена UICC (универсална карта с интегрална схема) (eUICC) за устройства от типа „машина—машина“, BSI-CC-PP-0089-2015;

д) за категорията „Точки за (платежно) взаимодействие и терминални устройства ПОС“:

1) точка за взаимодействие „POI-CHIP-ONLY“, ANSSI-CC-PP-2015/01;

2) точка за взаимодействие „POI-CHIP-ONLY и пакет с отворен протокол“, ANSSI-CC-PP-2015/02;

3) точка за взаимодействие „POI-COMPREHENSIVE“, ANSSI-CC-PP-2015/03;

4) точка за взаимодействие „POI-COMPREHENSIVE и пакет с отворен протокол“, ANSSI-CC-PP-2015/04;

5) точка за взаимодействие „POI-PED-ONLY“, ANSSI-CC-PP-2015/05;

6) точка за взаимодействие „POI-PED-ONLY и пакет с отворен протокол“, ANSSI-CC-PP-2015/06;

е) за категорията „Хардуерни устройства с кутии за сигурност“:

1) криптографски модул за операции по подписване на доставчик на компютърни услуги „в облак“ с резервно копие — ЗП за CMCSOB, ЗП за HSM CMCSOB 14167-2, ANSSI-CC-PP-2015/08;

2) криптографски модул за услуги за генериране на ключове на доставчик на компютърни услуги „в облак“ — ЗП за CMCKG, ЗП за HSM CMCKG 14167-3, ANSSI-CC-PP-2015/09;

3) криптографски модул за операции по подписване на доставчик на компютърни услуги „в облак“ без резервно копие — ЗП за CMCSO, ЗП за HSM CMCKG 14167-4, ANSSI-CC-PP-2015/10.

ПРИЛОЖЕНИЕ IV

Непрекъснатост на увереността и преглед на сертификатите

IV.1 **Непрекъснатост на увереността: обхват**

1. Посочените по-долу изисквания за непрекъснатост на увереността се прилагат към дейностите по поддържане, свързани със следното:

   а) повторно оценяване дали непроменният сертифициран ИКТ продукт все още отговаря на изискванията за сигурност;

   б) оценка на въздействието на промените в сертифициран ИКТ продукт върху неговото сертифициране;

   в) ако е включено в сертифицирането, прилагането на софтуерни поправки в съответствие с оценен процес на управление на софтуерни поправки;

   г) ако е включен, преглед на управлението на жизнения цикъл или производствените процеси при титуляря на сертификата.

2. Титулярят на сертификат по ЕССК може да поиска преглед на сертификата в следните случаи:

   а) срокът на валидност на сертификата по ЕССК изтича в рамките на девет месеца;

   б) настъпила е промяна в сертифицирания ИКТ продукт или в друг фактор, който би могъл да повлияе на неговата функционалност по отношение на сигурността;

   в) титулярят на сертификата иска оценката на уязвимостта да бъде извършена отново, за да се потвърди отново увереността на сертификата по ЕССК, свързана с устойчивостта на ИКТ продукта, срещу настоящи кибератаки.

IV.2 **Повторно оценяване**

1. В случай че е необходимо да се оцени въздействието на промените в средата по отношение на заплахите върху непроменен сертифициран ИКТ продукт, до сертифициращия орган се подава искане за повторно оценяване.

2. Повторното оценяване се извършва от същия ITSEF, който е участвал в предишното оценяване, като се използват отново всички все още приложими резултати от него. При оценяването се набляга на дейностите, свързани с увереността, които са потенциално повлияни от променената среда по отношение на заплахите, на сертифицирания ИКТ продукт, по-специално съответната група AVA_VAN и в допълнение групата на жизнения цикъл на увереност (ALC), където отново се събират достатъчно доказателства за поддържането на средата за разработка.

3. ITSEF описва промените, както и резултатите от повторното оценяване, с актуализация на предишния технически доклад за оценка.

4. Сертифициращият орган извършва преглед на актуализирания технически доклад за оценка и изготвя доклад за повторна оценка. След това статусът на първоначалния сертификат се променя в съответствие с член 13.

5. Докладът за повторна оценка и актуализираният сертификат се предоставят на националния орган за сертифициране на киберсигурността и на ENISA за публикуване на нейния уебсайт за сертифициране на киберсигурността.

IV.3 **Промени в сертифициран ИКТ продукт**

1. Когато сертифициран ИКТ продукт е бил подложен на промени, титулярят на сертификата, който желае да запази сертификата, предоставя на сертифициращия орган доклад за оценка на въздействието.

2. Докладът за оценка на въздействието съдържа следните елементи:

   а) въведение, включващо необходимата информация за установяване на доклада за оценка на въздействието и обекта на оценката, подлежащ на промени;

б) описание на промените в продукта;

в) обозначаване на засегнатите доказателства на разработчика;

г) описание на промените в доказателствата на разработчика;

д) констатациите и заключенията относно въздействието върху увереността за всяка промяна.

3. Сертифициращият орган разглежда промените, описани в доклада за оценка на въздействието, за да потвърди тяхното въздействие върху увереността на сертифицирания обект на оценка, както е предложено в заключенията на доклада за оценка на въздействието.

4. След проверката сертифициращият орган определя мащаба на промяната като несъществен или съществен в съответствие с нейното въздействие.

5. Когато сертифициращият орган потвърди, че промените са несъществени, за изменения ИКТ продукт се издава нов сертификат и се изготвя доклад за поддръжка към първоначалния сертификационен доклад при следните условия:

а) докладът за поддръжката се включва като част от доклада за оценка на въздействието и съдържа следните раздели:

1) въведение;

2) описание на промените;

3) засегнати доказателства на разработчика;

б) датата на валидност на новия сертификат не може да бъде след датата на първоначалния сертификат.

6. Новият сертификат, включително докладът за поддръжка, се предоставя на ENISA за публикуване на нейния уебсайт за сертифициране на киберсигурността.

7. Когато се потвърди, че промените са съществени, се извършва повторно оценяване в контекста на предишното оценяване, като се използват отново всички все още приложими резултати от предишното оценяване.

8. След приключването на оценката на променения обект на оценката ITSEF изготвя нов технически доклад за оценка. Сертифициращият орган преглежда актуализирания технически доклад за оценка и, ако е приложимо, издава нов сертификат с нов сертификационен доклад.

9. Новият сертификат и сертификационният доклад се предоставят на ENISA за публикуване.

IV.4 **Управление на софтуерните поправки**

1. В процедурата за управление на софтуерните поправки е предвиден структуриран процес за актуализиране на сертифициран ИКТ продукт. Процедурата за управление на софтуерните поправки, включително механизмът, внедрен в ИКТ продукта от заявителя за сертифициране, може да се използва след сертифицирането на ИКТ продукта под отговорността на органа за оценяване на съответствието.

2. Заявителят за сертифициране може да включи в сертифицирането на ИКТ продукта механизъм за софтуерни поправки като част от сертифицирана процедура за управление, използвана при ИКТ продукта, при едно от следните условия:

а) функционалностите, засегнати от софтуерната поправка, се намират извън обекта на оценка на сертифицирания ИКТ продукт;

б) софтуерната поправка е свързана с предварително определена несъществена промяна в сертифицирания ИКТ продукт;

в) софтуерната поправка е свързана с потвърдена уязвимост с критично въздействие върху сигурността на сертифицирания ИКТ продукт.

3. Ако софтуерната поправка е свързана със съществена промяна на обекта на оценка на сертифицирания ИКТ продукт във връзка с неоткрита преди това уязвимост, която няма критично въздействие върху сигурността на ИКТ продукта, се прилагат разпоредбите на член 13.

4. Процедурата за управление на софтуерните поправки за даден ИКТ продукт се състои от следните елементи:

   а) процеса на разработване и пускане на софтуерната поправка за ИКТ продукта;

   б) техническия механизъм и функциите за внедряване на софтуерната поправка в ИКТ продукта;

   в) набор от дейности за оценка, свързани с ефективността и изпълнението на техническия механизъм.

5. По време на сертифицирането на ИКТ продукта:

   а) заявителят за сертифициране на ИКТ продукта предоставя описание на процедурата за управление на софтуерните поправки;

   б) ITSEF проверява следните елементи:

      1) разработчикът е внедрил механизмите за софтуерна поправка в ИКТ продукта в съответствие с процедурата за управление на софтуерните поправки, която е била представена за сертифициране;

      2) границите на обекта на оценка са разделени по такъв начин, че промените, направени в разделените процеси, да не засягат сигурността на обекта на оценка;

      3) техническият механизъм за софтуерни поправки функционира в съответствие с разпоредбите на настоящия раздел и твърденията на заявителя;

   в) сертифициращият орган включва в доклада за сертифициране резултата от оценената процедура за управление на софтуерните поправки.

6. Титулярят на сертификата може да пристъпи към прилагане на софтуерната поправка, създадена в съответствие със сертифицираната процедура за управление на софтуерните поправки, към съответния сертифициран ИКТ продукт и предприема посочените по-долу стъпки в рамките на 5 работни дни в следните случаи:

   а) в случая, посочен в точка 2, буква а), докладва за съответната софтуерна поправка на сертифициращия орган, който не променя съответния сертификат по ЕССК;

   б) в случая, посочен в точка 2, буква б), представя съответната софтуерна поправка на ITSEF за преглед. ITSEF информира сертифициращия орган след получаването на софтуерната поправка, след което сертифициращият орган предприема подходящи действия за издаване на нова версия на съответния сертификат по ЕССК и за актуализиране на сертификационния доклад;

   в) в случая, посочен в точка 2, буква в), представя съответната софтуерна поправка на ITSEF за необходимото повторно оценяване, но паралелно може да внедри софтуерната поправка. ITSEF информира сертифициращия орган, след което сертифициращият орган започва съответните дейности по сертифициране.

ПРИЛОЖЕНИЕ V

Съдържание на сертификационния доклад

V.1 **Сертификационен доклад**

1. Въз основа на техническите доклади за оценка, предоставени от ITSEF, сертифициращият орган изготвя сертификационен доклад, който се публикува заедно със съответния сертификат по ЕССК.

2. Сертификационният доклад е източник на подробна и практическа информация за ИКТ продукта или категорията ИКТ продукти и за безопасното внедряване на ИКТ продукта и следователно включва цялата публично достъпна и подлежаща на споделяне информация, която е от значение за ползвателите и заинтересованите страни. В сертификационния доклад може да се съдържат препратки към публично достъпна и подлежаща на споделяне информация.

3. Сертификационният доклад съдържа най-малко следните раздели:

   а) резюме;

   б) обозначаване на ИКТ продукта или на категорията ИКТ продукти за защитни профили;

   в) услуги за сигурност;

   г) допускания и изясняване на обхвата;

   д) информация за архитектурата;

   е) допълнителна информация за киберсигурността, ако е приложимо;

   ж) изпитване на ИКТ продукта, ако е извършено такова;

   з) когато е приложимо, идентифициране на процесите на титуляря на сертификата за управление на жизнения цикъл и на неговите производствени съоръжения;

   и) резултатите от оценката и информация относно сертификата;

   й) резюме на целевото ниво на сигурност на ИКТ продукта, представен за сертифициране;

   к) маркировката или етикета, свързани със схемата, когато има такива;

   л) библиография.

4. Резюмето представлява кратък преглед на целия сертификационен доклад. Резюмето съдържа ясно и кратко обобщение на резултатите от оценката и включва следната информация:

   а) наименование на оценявания ИКТ продукт, изброяване на компонентите на продукта, които са част от оценката, и версия на ИКТ продукта;

   б) наименованието на ITSEF, който е извършил оценката, и, когато е приложимо, списък на подизпълнителите;

   в) дата на приключване на оценката;

   г) данни на техническия доклад за оценка, изготвен от ITSEF;

   д) кратко описание на резултатите от сертификационния доклад, включително:

      1) версията и, ако е приложимо, изданието на общите критерии, приложени към оценката;

      2) пакета за получаване на увереност по общите критерии и компонентите за гаранциите за сигурност, включително нивото на AVA_VAN, приложено по време на оценката, и съответното ниво на увереност, както е посочено в член 52 от Регламент (ЕС) 2019/881, за което се отнася сертификатът по ЕССК;

      3) функционалността за сигурност на оценявания ИКТ продукт;

      4) обобщение на заплахите и политиките за организационна сигурност, на които отговаря оценяваният ИКТ продукт;

5) специални изисквания за конфигурацията;

6) допускания за операционната среда;

7) когато е приложимо, наличието на одобрена процедура за управление на софтуерни поправки в съответствие с раздел IV.4 от приложение IV;

8) отказ(и) от отговорност.

5. Оценяваният ИКТ продукт се обозначава ясно, като се включва следната информация:

а) наименованието на оценявания ИКТ продукт;

б) изброяване на компонентите на ИКТ продукта, които са част от оценката;

в) номерът на версията на компонентите на ИКТ продукта;

г) допълнителни изисквания към операционната среда на сертифицирания ИКТ продукт;

д) име и информация за връзка на титуляря на сертификата по ЕССК;

е) когато е приложимо, процедурата за управление на софтуерните поправки, включена в сертификата;

ж) връзка към уебсайта на титуляря на сертификата по ЕССК, на който се предоставя допълнителна информация за киберсигурността на сертифицирания ИКТ продукт в съответствие с член 55 от Регламент (ЕС) 2019/881.

6. Информацията, включена в този раздел, е възможно най-точна, за да се осигури цялостно и прецизно представяне на ИКТ продукта, което може да се използва повторно при бъдещи оценки.

7. Разделът относно политиката за сигурност съдържа описание на политиката за сигурност на ИКТ продукта и политиките или правилата, които се налагат с оценявания ИКТ продукт или на които той отговаря. В него се включва позоваване и описание на следните политики:

а) политиката за справяне с уязвимости на титуляря на сертификата;

б) политиката за непрекъснатост на увереността на титуляря на сертификата.

8. Когато е приложимо, политиката може да включва условия, свързани с прилагането на процедура за управление на софтуерните поправки по време на срока на валидност на сертификата.

9. Разделът за допусканията и изясняването на обхвата съдържа изчерпателна информация относно обстоятелствата и целите, свързани с предвидената употреба на продукта, както е посочено в член 7, параграф 1, буква в). Информацията включва следното:

а) допускания за използването и внедряването на ИКТ продукта под формата на минимални изисквания, като например правилно инсталиране и конфигуриране и изпълнение на хардуерните изисквания;

б) допускания за оперативната среда с оглед на съвместимата работа на ИКТ продукта.

10. Информацията, посочена в точка 9, е възможно най-разбираема, за да могат ползвателите на сертифицирания ИКТ продукт да вземат информирани решения относно рисковете, свързани с неговата употреба.

11. Разделът с информация за архитектурата включва описание на високо ниво на ИКТ продукта и на неговите основни компоненти в съответствие с проекта на подсистемите ADV_TDS от общите критерии.

12. Пълният списък на допълнителната информация за киберсигурността на ИКТ продукта се предоставя в съответствие с член 55 от Регламент (ЕС) 2019/881. Цялата относима документация се обозначава с номера на версията.

13. Разделът за изпитване на ИКТ продукта включва следната информация:

    а) наименованието и звеното за контакт на органа или субекта, издал сертификата, включително отговорния национален орган за сертифициране на киберсигурността;

    б) наименованието на ITSEF, който е извършил оценката, когато е различен от сертифициращия орган;

    в) обозначаване на използваните компоненти на увереността от стандартите, посочени в член 3;

    г) версията на актуалния технически документ и допълнителните критерии за оценка на сигурността, използвани при оценката;

    д) пълните и точни настройки и конфигурация на ИКТ продукта по време на оценката, включително оперативни бележки и наблюдения, ако има такива;

    е) всеки използван защитен профил, включително следната информация:

        1) автора на защитния профил;

        2) наименованието и идентификатора на защитния профил;

        3) идентификатора на сертификата на защитния профил;

        4) наименованието и данните за връзка на сертифициращия орган и на ITSEF, участващи в оценката на защитния профил;

        5) пакета(ите) за получаване на увереност, изискван(и) за даден продукт, съответстващ на защитния профил.

14. Резултатите от оценката и информацията относно раздела за сертификата включват следната информация:

    а) потвърждение на достигнатото ниво на увереност, както е посочено в член 4 от настоящия регламент и член 52 от Регламент (ЕС) 2019/881;

    б) изискванията за увереност от стандартите, посочени в член 3, на които ИКТ продуктът или защитният профил действително отговаря, включително нивото на AVA_VAN;

    в) подробно описание на изискванията за увереност, както и подробности за това как продуктът отговаря на всяко едно от тях;

    г) дата на издаване и срок на валидност на сертификата;

    д) уникален идентификатор на сертификата;

15. Целевото ниво на сигурност се включва в сертификационния доклад или се посочва и обобщава в него и се предоставя заедно със сертификационния доклад за целите на публикуването му.

16. Целевото ниво на сигурност може да бъде редактирано в съответствие с раздел VI.2.

17. Маркировката или етикетът, свързани с ЕССК, могат да бъдат вмъкнати в сертификационния доклад в съответствие с установените правила и процедури в член 11.

18. Разделът с библиографията включва препратки към всички документи, използвани при изготвянето на сертификационния доклад. Тази информация включва най-малко следното:

    а) критериите за оценка на сигурността, използваните актуални технически документи и други съответни спецификации и тяхната версия;

    б) техническия доклад за оценка;

    в) техническия доклад за оценка на съставен продукт, когато е приложимо;

    г) техническа справочна документация;

    д) документация на разработчика, използвана при оценката.

19. За да се гарантира възпроизводимостта на оценката, цялата документация, на която се прави позоваване, трябва да бъде посочена еднозначно с правилната дата на издаване и правилния номер на версията.

V.2 **Редактиране на целевото ниво на сигурност за публикуване**

1. Целевото ниво на сигурност, което трябва да бъде включено в сертификационния доклад или да бъде посочено в него съгласно раздел VI.1, точка 1, може да бъде редактирано чрез премахване или перифразиране на защитена фирмена информация от технически характер.

2. Редактираната версия на целевото ниво на сигурност представя реалистично неговата пълна оригинална версия. Това означава, че в редактираната версия на целевото ниво на сигурност не може да се пропуска информация, която е необходима, за да се разберат характеристиките на обекта на оценката, свързани със сигурността, и обхватът на оценката.

3. Съдържанието на редактираната версия на целевото ниво на сигурност отговаря на следните минимални изисквания:

   а) въведението не се редактира, тъй като по принцип не съдържа защитена фирмена информация;

   б) редактираната версия на целевото ниво на сигурност трябва да има уникален идентификатор, който се различава от пълната му оригинална версия;

   в) описанието на обекта на оценка може да бъде съкратено, тъй като може да включва защитена фирмена информация и подробности за проекта на обекта на оценка, които не следва да се публикуват;

   г) описанието на средата за сигурност на обекта на оценката (допускания, заплахи, организационни политики за сигурност) не се съкращава, доколкото тази информация е необходима за разбиране на обхвата на оценката;

   д) целите на сигурността не се съкращават, тъй като цялата информация трябва да се оповести публично, за да се разбере замисълът на целевото ниво на сигурност и на обекта на оценката;

   е) всички изисквания по отношение на сигурността се оповестяват публично. В бележките за приложенията може да се предостави информация за това как са използвани функционалните изисквания на общите критерии, посочени в член 3, за да се разбере целевото ниво на сигурност;

   ж) обобщената спецификация на обекта на оценката включва всички функции за сигурност на обекта на оценка, но допълнителната защитена фирмена информация може да бъде редактирана;

   з) включват се препратки към защитните профили, прилагани към обекта на оценка;

   и) обосновката може да бъде редактирана, за да се премахне защитена фирмена информация.

4. Дори ако редактираната версия на целевото ниво на сигурност не е официално оценена в съответствие със стандартите за оценка, посочени в член 3, сертифициращият орган гарантира, че тя съответства на пълната и оценена версия на целевото ниво на сигурност, и включва препратка както към пълната, така и към редактирана версия в сертификационния доклад.

ПРИЛОЖЕНИЕ VI

ОБХВАТ И СЪСТАВ НА ЕКИПА ЗА ПАРТНЬОРСКИ ОЦЕНКИ

VI.1 **Обхват на партньорската оценка**

1. Обхванати са следните типове партньорски оценки:

   а) Тип 1: когато сертифициращият орган извършва дейности по сертифициране на нивото на AVA_VAN.3;

   б) Тип 2: когато сертифициращият орган извършва дейности по сертифициране, свързани с техническа област, включена в списъка на актуалните технически документи в приложение I;

   в) Тип 3: когато сертифициращият орган извършва дейности по сертифициране на ниво над AVA_VAN.3, като използва защитен профил, включен в списъка на актуалните технически документи в приложение II или III.

2. Сертифициращият орган, подложен на партньорска оценка, представя списък на сертифицираните ИКТ продукти, които могат да бъдат кандидати за преглед от екипа за партньорска оценка, в съответствие със следните правила:

   а) продуктите кандидати отговарят на техническия обхват на пълномощията на сертифициращия орган и от този обхват чрез партньорска оценка се анализират най-малко две различни оценки на продукти с ниво на увереност „високо“ и един защитен профил, ако сертифициращият орган е издал сертификат с ниво на увереност „високо“;

   б) за партньорска оценка от тип 2 сертифициращият орган представя поне един продукт за всяка техническа област и за всеки съответен ITSEF;

   в) за партньорска оценка от тип 3 поне един продукт кандидат се оценява в съответствие с приложим и съответстващ защитен профил.

VI.2 **Екип за партньорска оценка**

1. Екипът за оценка се състои от най-малко двама експерти, всеки от които е избран от различен сертифициращ орган от различни държави членки, който издава сертификати с ниво на увереност „високо“. Експертите следва да докажат съответния експертен опит в областта на стандартите, посочени в член 3, и актуалните технически документи, които са в обхвата на партньорската оценка.

2. В случай на делегиране на правомощия за издаване или предварително одобряване на сертификати, както е посочено в член 56, параграф 6 от Регламент (ЕС) 2019/881, експерт от националния орган за сертифициране на киберсигурността, свързан със съответния сертифициращ орган, трябва да участва също в екипа от експерти, избран в съответствие с параграф 1 от настоящия раздел.

3. За партньорска оценка от тип 2 членовете на екипа се избират от сертифициращи органи, упълномощени за съответната техническа област.

4. Всеки член на екипа за оценка има най-малко две години опит в извършването на дейности по сертифициране в сертифициращ орган.

5. За партньорска оценка от тип 2 или тип 3 всеки член на екипа за оценка има най-малко две години опит в извършването на дейности по сертифициране в съответната техническа област или защитен профил и доказан опит и участие в упълномощаването на ITSEF.

6. Националният орган за сертифициране на киберсигурността, който наблюдава и контролира сертифициращия орган, подложен на партньорска оценка, и поне един национален орган за сертифициране на киберсигурността, чийто сертифициращ орган не подлежи на партньорска оценка, участват в партньорската оценка в качеството си на наблюдатели. ENISA може да участва в партньорската оценка и като наблюдател.

7. Съставът на екипа за партньорска оценка се представя на сертифициращия орган, подложен на партньорска оценка. В обосновани случаи последният може да оспори състава на екипа за партньорска оценка и да поиска той да бъде преразгледан.

ПРИЛОЖЕНИЕ VII

Съдържание на сертификата по ЕССК

Сертификатът по ЕССК трябва да съдържа най-малко:

а) уникален идентификатор, определен от сертифициращия орган, който издава сертификата;

б) информация, свързана със сертифицирания ИКТ продукт или защитен профил и с титуляря на сертификата, включително:

1) наименование на ИКТ продукта или на защитния профил, когато е приложимо, на обекта на оценката;

2) вида на ИКТ продукта или на защитния профил, когато е приложимо, на обекта на оценката;

3) версия на ИКТ продукта или на защитния профил;

4) име, адрес и информация за връзка на титуляря на сертификата;

5) връзка към уебсайта на титуляря на сертификата, съдържащ допълнителната информация за киберсигурността, посочена в член 55 от Регламент (ЕС) 2019/881;

в) информация, свързана с оценката и сертифицирането на ИКТ продукта или на защитния профил, включително:

1) наименование, адрес и информация за връзка на сертифициращия орган, който е издал сертификата;

2) когато е различен от сертифициращия орган, наименованието на ITSEF, който е извършил оценката;

3) наименованието на отговорния национален орган за сертифициране на киберсигурността;

4) препратка към настоящия регламент;

5) данни за сертификационния доклад, свързан със сертификата, посочен в приложение V;

6) приложимото ниво на увереност в съответствие с член 4;

7) данни за версията на стандартите, използвани за оценката, посочена в член 3;

8) посочване на определените в стандартите ниво на увереност или пакет за получаване на увереност в съответствие с член 3 и приложение VIII, включително използваните компоненти за увереността и обхванатото ниво на AVA_VAN;

9) когато е приложимо, препратка към един или повече защитни профили, на които съответстват ИКТ продуктът или защитният профил;

10) дата на издаване;

11) срок на валидност на сертификата;

г) маркировката и етикета, свързани със сертификата, в съответствие с член 11.

ПРИЛОЖЕНИЕ VIII

Декларация за пакет за получаване на увереност

1. Обратно на определенията в общите критерии, разширение:

а) не се обозначава със съкращението „+“;

б) описва се подробно със списък на всички засегнати компоненти;

в) описва се подробно в сертификационния доклад.

2. Нивото на увереност, потвърдено в сертификата по ЕССК, може да бъде допълнено от нивото на увереност на оценката, както е посочено в член 3 от настоящия регламент.

3. Ако нивото на увереност, потвърдено в сертификата по ЕССК, не се отнася до разширение, в сертификата по ЕССК се посочва един от следните пакети:

а) „специфичният пакет за получаване на увереност“;

б) „пакетът за получаване на увереност, съответстващ на защитния профил“ в случай на позоваване на защитен профил без ниво на увереност на оценката.

ПРИЛОЖЕНИЕ IX

Маркировка и етикет

1. Форма на маркировката и етикета:

2. Ако размерите на маркировката и етикета се намаляват или увеличават, задължително се спазват пропорциите, посочени в чертежа по-горе.

3. Когато присъстват физически, маркировката и етикетът са с височина най-малко 5 mm.