2024/3144

19.12.2024 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2024/3144 НА КОМИСИЯТА

от 18 декември 2024 година

за изменение на Регламент за изпълнение (ЕС) 2024/482 по отношение на приложимите международни стандарти и за поправка на посочения регламент за изпълнение

(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 Регламент за изпълнение (ЕС) 2024/482 на Комисията ([2]) 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.

(2) Регламент за изпълнение (ЕС) 2024/482 се основава на установени международни стандарти, които представляват общите критерии и общата методика за оценка, поддържани от Международната организация по стандартизация (ISO) и Международната електротехническа комисия (IEC). В Регламент за изпълнение (ЕС) 2024/482 се прави позоваване на стандартите ISO/IEC, но в него не се уточнява приложимата версия на тези стандарти. Поради това следва да се уточни коя версия на стандартите се прилага за сертификатите, издавани съгласно ЕССК.

(3) Правителствените организации, които допринесоха за разработването на общите критерии и общата методика за оценка чрез Споразумението за признаване на основани на общи критерии сертификати в областта на ИТ сигурността (CCRA), са съпритежатели заедно с ISO/IEC на авторските им права. Тези правителствени организации си запазват правото да ги използват. С оглед на значението на тези документи, произхождащи от CCRA, те следва също така да бъдат основа за сертифициране съгласно ЕССК.

(4) Стандартите за общите критерии и общата методика за оценка подлежат на тълкувания, изготвяни от CCRA, които улесняват тяхното прилагане и които могат да бъдат взети предвид от центровете за оценка на сигурността на информационните технологии (ITSEF) и сертифициращите органи.

(5) Международните стандарти, свързани с общите критерии, могат да бъдат актуализирани. За да се гарантира организиран и навременен преход, е целесъобразно да се определят преходни правила, за да се даде достатъчно време за необходимите корекции на доставчиците, ITSEF и сертифициращите органи, както и на другите съответни участници. Тези преходни правила следва да се приведат в съответствие в подходяща степен с глобалните практики, като например онези, определени от CCRA.

([1]) ОВ L 151, 7.6.2019 г., стр. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

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

(6) В Регламент за изпълнение (ЕС) 2024/482 не се уточнява докога сертифицирането на ИКТ продукт може да се основава на предишните версии на стандартите за общите критерии и общата методика за оценка. Техническите области и защитните профили, изброени в приложения I, II и III към посочения регламент за изпълнение, се основават на предишни версии на стандартите ISO/IEC 15408 и 18045. Поради това в Регламент за изпълнение (ЕС) 2024/482 следва да се уточни при какви обстоятелства продължава да се прилага предишната версия на общите критерии и общата методика за оценка и как ще бъде осъществен преходът към последната версия на международните стандарти.

(7) По време на преходния период актуализирането на съответните технически области и защитни профили следва да бъде приоритет за съответните заинтересовани страни. В Регламент за изпълнение (ЕС) 2024/482 следва да се предвиди, че целевите нива на сигурност, основани на предишна версия на стандартите, ще бъдат приемани до 31 декември 2027 г. в съответствие с политиката за преход, приета от CCRA. Трябва обаче да се отбележи, че политиката за преход на CCRA обхваща първоначалните оценки на продуктите и защитните профили, започнали не по-късно от 30 юни 2024 г. — датата, на която ЕСКК все още не беше приложима. Освен това, в съответствие с политиката за преход на CCRA, в Регламент за изпълнение (ЕС) 2024/482 следва да се предвиди, че съответстващите на посочения регламент за изпълнение целеви нива на сигурност, за които е декларирано съответствие със защитни профили, основани на предишна версия на стандартите, ще бъдат приемани до 31 декември 2027 г. Освен това, когато се издава нов сертификат съгласно Регламент за изпълнение (ЕС) 2024/482 в контекста на процес на преглед на национален сертификат, който започва в рамките на две години от първоначалния сертификат, следва да е възможно да се използва предишна версия на стандартите. Това не е от значение за процес на преглед, при който не се изисква издаването на нов сертификат съгласно Регламент за изпълнение (ЕС) 2024/482 и когато сертификатът остава валиден.

(8) С цел да се осигури организиран преход към последната версия на стандартите, в Регламент за изпълнение (ЕС) 2024/482 следва да се предвидят специфични преходни правила и да продължи да се дава възможност за издаване на сертификати съгласно посочения регламент за изпълнение, за които е декларирано съответствие със защитни профили, основани на предишни версии на стандартите, публикувани от CCRA, когато използването на такива защитни профили се изисква съгласно законодателството на Съюза. Такъв е случаят с Регламент за изпълнение (ЕС) 2016/799 на Комисията ([3]), както и с Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета ([4]) и Решение за изпълнение (ЕС) 2016/650 на Комисията ([5]).

(9) В приложение I към Регламент за изпълнение (ЕС) 2024/482 са изброени приложимите актуални технически документи за оценка на ИКТ продукти и защитни профили. В него обаче не се уточнява версията на документите. Поради това следва да се уточни коя версия на документите се прилага за сертификатите, издавани съгласно ЕССК. Тези версии се основават на документи, одобрени от Европейската група за сертифициране на киберсигурността, като същевременно са преминали допълнителен преглед за включването им в ЕССК. Освен това приложение I следва да бъде изменено, за да включи осъвременени и нови актуални технически документи след одобряването им от Европейската група за сертифициране на киберсигурността, като по този начин се гарантира единна акредитация на органите за оценяване на съответствието съгласно ЕССК. Изискванията за акредитация, свързани с акредитацията на ITSEF, следва да бъдат актуализирани, за да се изясни прилагането на критериите за независимост и безпристрастност, и следва да бъде създаден нов актуален технически документ за акредитацията на сертифициращите органи.

(10) Актуалните технически документи могат да бъдат добавени към ЕССК или да подлежат на актуализиране в контекста на дейностите ѝ по поддържане. Може да се наложи да бъдат установени подходящи преходни правила за новите или осъвременените актуални технически документи, за да се даде възможност на доставчиците, ITSEF, сертифициращите органи и другите заинтересовани страни да направят необходимите корекции. За осъвременяването на актуалния технически документ, свързан с акредитацията на ITSEF, осъвременеият документ следва да се прилага за акредитации, издадени преди 8 юли 2025 г. само когато са преразгледани, например в контекста на процедура за оценка или повторна оценка. Освен това осъвременеият документ следва да се прилага за всички акредитации за ITSEF, издадени след 8 юли 2025 г.

([3]) 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 по отношение на определянето на изискванията за конструкцията, изпитването, монтирането, експлоатацията и ремонта на тахографите и техните компоненти (ОВ L 139, 26.5.2016 г., стр. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

([4]) Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ L 257, 28.8.2014 г., стр. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([5]) Решение за изпълнение (ЕС) 2016/650 на Комисията от 25 април 2016 г. за определяне на стандарти за оценка на сигурността на устройствата за създаване на квалифициран електронен подпис и печат съгласно член 30, параграф 3 и член 39, параграф 2 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар (ОВ L 109, 26.4.2016 г., стр. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

(11) Допълнителните корекции на членове 5, 8, 16, 29 и 44 и на приложение IV към Регламент за изпълнение (ЕС) 2024/482 допринасят за осигуряването на единна формулировка и ясно правно тълкуване.

(12) Правилата за нотифициране на органите за оценяване на съответствието следва да бъдат установени хоризонтално за всички схеми съгласно европейската рамка за сертифициране на киберсигурността. Регламент за изпълнение (ЕС) 2024/3143 на Комисията ([6]) обхваща такива правила за нотифициране. Следователно членове 23 и 24 от Регламент за изпълнение (ЕС) 2024/482 следва да се заличат от датата, на която започва да се прилага Регламент за изпълнение (ЕС) 2024/3143.

(13) Поради това Регламент за изпълнение (ЕС) 2024/482 следва да бъде съответно изменен и поправен.

(14) Мерките, предвидени в настоящия регламент, са в съответствие със становището на комитета, създаден съгласно член 66 от Регламент (ЕС) 2019/881,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Регламент за изпълнение (ЕС) 2024/482 се изменя, както следва:

1) В член 2 точки 1 и 2 се заменят със следното:

„1) „общи критерии“ означава общите критерии за оценка на сигурността на информационните технологии, както е определено в стандарти ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 или ISO/IEC 15408-5:2022 или в Общите критерии за оценяване на сигурността на информационните технологии, версия CC:2022, части 1—5, публикувани от участниците в Споразумението за признаване на основани на общи критерии сертификати в областта на ИТ сигурността;

2) „обща методика за оценка“ означава общата методика за оценка на сигурността на информационните технологии, както е определено в стандарт ISO/IEC 18045:2022, или Общата методика за оценка на сигурността на информационните технологии, версия CEM:2022, публикувана от участниците в Споразумението за признаване на основани на общи критерии сертификати в областта на ИТ сигурността;“.

2) Член 3 се заменя със следното:

„*Член 3*

Стандарти за оценка

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

а) общите критерии;

б) общата методика за оценка.

2. До 31 декември 2027 г. може да се издава сертификат съгласно ЕССК, като се прилага един от следните стандарти:

а) ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 или ISO/IEC 15408-3:2008;

б) Общи критерии за оценяване на сигурността на информационните технологии, версия 3.1, редакция 5, публикувана от участниците в Споразумението за признаване на основани на общи критерии сертификати в областта на ИТ сигурността;

([6]) Регламент за изпълнение (ЕС) 2024/3143 на Комисията от 18 декември 2024 г. за установяване на обстоятелствата, форматите и процедурите за нотификациите съгласно член 61, параграф 5 от Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии (ОВ L, 2024/3143, 19.12.2024 г., ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

в) ISO/IEC 18045:2008;

г) Обща методика за оценка на сигурността на информационните технологии, редакция 5, версия 3.1, публикувана от участниците в Споразумението за признаване на основани на общи критерии сертификати в областта на ИТ сигурността;

3. До 31 декември 2027 г. съгласно ЕССК може да се издава прилагащ стандартите по параграф 1 сертификат, за който е декларирано съответствие със защитен профил, приложил стандартите, изброени в параграф 2.

4. Сертификат, прилагащ стандартите, посочени в параграф 1, може също да бъде издаден съгласно ЕССК, като декларира съответствие със защитен профил, който е приложил някой от следните стандарти, при условие че използването на такъв защитен профил се изисква съгласно Регламент за изпълнение (ЕС) 2016/799 на Комисията (*), Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета (**)или Решение за изпълнение (ЕС) 2016/650 на Комисията (***):

а) Общи критерии за оценяване на сигурността на информационните технологии, версия 3.1, редакции 1—4, публикувана от участниците в Споразумението за признаване на основани на общи критерии сертификати в областта на ИТ сигурността;

б) Обща методика за оценка на сигурността на информационните технологии, версия 3.1, редакции 1—4, публикувана от участниците в Споразумението за признаване на основани на общи критерии сертификати в областта на ИТ сигурността.

_____

(*) 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 по отношение на определянето на изискванията за конструкцията, изпитването, монтирането, експлоатацията и ремонта на тахографите и техните компоненти (ОВ L 139, 26.5.2016 г., стр. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

(**) Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ L 257, 28.8.2014 г., стр. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(***) Решение за изпълнение (ЕС) 2016/650 на Комисията от 25 април 2016 г. за определяне на стандарти за оценка на сигурността на устройствата за създаване на квалифициран електронен подпис и печат съгласно член 30, параграф 3 и член 39, параграф 2 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар (ОВ L 109, 26.4.2016 г., стр. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).“

3) В глава IV се вмъква следният член 20а:

„*Член 20а*

Спецификация на изискванията за акредитация на органите за оценяване на съответствието

При акредитацията на органите за оценяване на съответствието се взима предвид спецификацията на изискванията за акредитация на сертифициращите органи и ITSEF, определени в приложимите актуални технически документи, изброени в точка 2 от приложение I.“

4) Членове 23 и 24 се заличават.

5) В член 48 се добавя следният параграф 4:

„4. Освен ако не е посочено друго в приложение I или II, актуалните технически документи се прилагат от датата на прилагане на акта за изменение, с който са били включени в приложение I или II.“

6) В член 49 се добавя следният параграф 4:

„4. При извършване на прегледа по параграф 3 в срок от две години от издаването на първоначалния сертификат и когато този преглед води до издаването на нов сертификат в съответствие с настоящия регламент, може да се приложат стандартите, изброени в член 3, параграф 2. Под дата на издаване на първоначалния сертификат се разбира датата на издаване на последния сертификат за ИКТ продукт или защитен профил, на който се основава текущото сертифициране.“

7) Приложение I се заменя с текста в приложение I към настоящия регламент.

8) Приложение IV се изменя в съответствие с приложение II към настоящия регламент.

Член 2

Регламент за изпълнение (ЕС) 2024/482 се поправя, както следва:

1) В член 5, параграф 1 буква б) се заменя със следното:

„б) чрез деклариране на съответствие със сертифициран защитен профил като част от ИКТ процеса, когато ИКТ продуктът попада в категорията ИКТ продукти, обхванати от този защитен профил.“

2) Член 8 се поправя, както следва:

а) заглавието се заменя със следното:

„Информация, необходима за сертифициране и оценяване“;

б) параграф 1 се заменя със следното:

„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 и оценяване.“

3) Член 16 се заменя със следното:

„*Член 16*

Информация, необходима за сертифицирането и оценяването 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 и оценяване, в пълна и точна форма. Разпоредбите на член 8, параграфи 2, 3, 4 и 7 се прилагат *mutatis mutandis*.“

4) В член 17 параграф 1 се заличава.

5) В член 29 параграф 2 се заменя със следното:

„2. Когато титулярят на сертификата по ЕССК не предложи подходящи корективни 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 или член 20.“

Член 3

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

Член 1, параграф 4 се прилага от 8 януари 2025 г.

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

Съставено в Брюксел на 18 декември 2024 година.

За Комисията
Председател
Ursula VON DER LEYEN

ПРИЛОЖЕНИЕ I

„„*ПРИЛОЖЕНИЕ I*

Актуални технически документи в подкрепа на техническите области и други актуални технически документи

1. Актуални технически документи в подкрепа на техническите области на нива 4 или 5 на AVA_VAN:

   а) следните документи, свързани с хармонизираната оценка на техническата област „Смарт карти и подобни устройства“:

      1) „Минимални изисквания на ITSEF за оценяване на сигурността на смарт карти и подобни устройства“, версия 1.1;

      2) „Минимални изисквания за сигурност на обекти“, версия 1.1;

      3) „Прилагане на общи критерии спрямо интегралните схеми“, версия 1.1;

      4) „Изисквания по отношение на архитектурата за информационна сигурност (ADV_ARC) за смарт карти и подобни устройства“, версия 1.1;

      5) „Сертифициране на „отворени“ продукти за смарт карти“, версия 1.1;

      6) „Оценка на съставни продукти за смарт карти и подобни устройства“, версия 1.1;

      7) „Прилагане на потенциала за кибератака спрямо смарт карти и подобни устройства“, версия 1.2.

   б) следните документи, свързани с хармонизираната оценка на техническата област „Хардуерни устройства с кутии за сигурност“:

      1) „Минимални изисквания на ITSEF за оценяване на сигурността на хардуерни устройства с кутии за сигурност“, версия 1.1;

      2) „Минимални изисквания за сигурност на обекти“, версия 1.1;

      3) „Прилагане на потенциала за кибератака спрямо хардуерни устройства с кутии за сигурност“, версия 1.2.

2. Актуални технически документи, свързани с хармонизираната акредитация на органите за оценяване на съответствието:

   а) „Акредитация на ITSEF за ЕССК“, версия 1.1 за акредитации, издадени преди 8 юли 2025 г.

   б) „Акредитация на ITSEF за ЕССК“, версия 1.6c за новоиздадени или подложени на преглед акредитации след 8 юли 2025 г.

   в) „Акредитация на CO за ЕССК“, версия 1.6b.““

ПРИЛОЖЕНИЕ II

В приложение IV към Регламент за изпълнение (ЕС) 2024/482 раздел IV.3 точки 5 и 6 се заменят със следното:

„5. Когато сертифициращият орган потвърди, че промените са несъществени, за изменения ИКТ продукт не се издава нов сертификат, а се изготвя доклад за поддръжка към първоначалния сертификационен доклад.

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

а) въведение;

б) описание на промените;

в) засегнати доказателства на разработчика.

6. Докладът за поддръжката по точка 5 се предоставя на ENISA за публикуване на нейния уебсайт за сертифициране на киберсигурността.“