РЕГЛАМЕНТ (ЕС) 2019/881 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

от 17 април 2019 година

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)

(текст от значение за ЕИП)

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз, и по-специално член 114 от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейския икономически и социален комитет ([1]),

като взеха предвид становището на Комитета на регионите ([2]),

в съответствие с обикновената законодателна процедура ([3]),

като имат предвид, че:

(1) Мрежите и информационните системи и съобщителните мрежи и услуги играят жизненоважна роля за обществото и са се превърнали в основата на икономическия растеж. Информационните и комуникационните технологии (ИКТ) са в основата на сложните системи, които поддържат ежедневната обществена активност, правят възможно функционирането на нашите икономики в основни сектори като здравеопазване, енергетика, финанси и транспорт, и по-специално поддържат функционирането на вътрешния пазар.

(2) Използването на мрежите и информационните системи от гражданите, организациите и предприятията в целия Европейски съюз е вече повсеместно. Цифровизацията и свързаността се превръщат в основни характеристики на все по-голям брой продукти и услуги и с навлизането на „интернет на нещата“ се очаква на територията на Съюза през следващото десетилетие да има изключително голям брой свързани цифрови устройства. Въпреки нарастващия брой на устройствата, свързани към интернет, вграждането на сигурност и устойчивост в тях „още при проектирането“ все още не се извършва в задоволителен мащаб, което води до недостатъчно ниво на киберсигурност. В този контекст, ограниченото използване на сертифицирането води до недостиг на информация за ползвателите физически лица, организации и предприятия относно характеристиките на ИКТ продукти, ИКТ услуги и ИКТ процеси в областта на киберсигурността, като подкопава доверието в цифровите решения. Мрежите и информационните системи могат да улеснят всички аспекти на нашия живот и да стимулират икономическия растеж на Съюза. Те са основата за постигането на цифровия единен пазар.

(3) Нарастването на цифровизацията и свързаността увеличава на рисковете, свързани с киберсигурността, като по този начин обществото като цяло стана по-уязвимо за киберзаплахи и се изостриха опасностите за физически лица, включително уязвими лица, като например деца. С цел да се смекчат тези рискове за обществото, трябва да бъдат предприети всички необходими действия за подобряване на киберсигурността в Съюза, така че да бъде осигурена подобра защита срещу киберзаплахи на мрежите и информационните системи, съобщителните мрежи, цифровите продукти, услугите и устройствата, използвани от гражданите, организациите и предприятията — от малките и средни предприятия (МСП), по смисъла на Препоръка 2003/361/ЕО на Комисията ([4]), до операторите на критична инфраструктура.

([1]) ОВ C 227, 28.6.2018 г., стр. 86.
([2]) ОВ C 176, 23.5.2018 г., стр. 29.
([3]) Позиция на Европейския парламент от 12 март 2019 г. (все още непубликувана в Официален вестник) и решение на Съвета от 9 април 2019.
([4]) Препоръка на Комисията от 6 май 2003 г. относно определението за микро-, малки и средни предприятия (ОВ L 124, 20.5.2003 г., стр. 36).

(4) С предоставянето на относима информация на обществеността Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA), създадена с Регламент (ЕС) № 526/2013 на Европейския парламент и на Съвета ([5]) допринася за развитието на сектора на киберсигурността в Съюза, по-специално на МСП и стартиращите предприятия. ENISA следва да се стреми към по-тясно сътрудничество с университетите и научноизследователските звена, за да допринесе за намаляване на зависимостта от продукти и услуги в областта на киберсигурността с произход извън Съюза и за да подсили веригите за доставки в рамките на Съюза.

(5) Броят на кибератаките нараства, а икономиката и обществото, които са свързани с интернет, са по-уязвими за киберзаплахи и кибератаки и имат нужда от засилени защитни механизми. Независимо от факта обаче, че кибератаките често са трансгранични, правомощията и политическият отговор на органите по киберсигурността и на правоприлагащите органи са основно национални. Широкомащабните инциденти могат да нарушат предоставянето на важни услуги в целия Съюз. Това изисква ефективен и координиран отговор и ефективно управление на кризи на равнището на Съюза, които да се основават на специални политики и по-широкообхватни инструменти за европейска солидарност и взаимопомощ. Освен това редовното оценяване на състоянието на киберсигурността и устойчивостта в Съюза въз основа на надеждни данни на Съюза, както и систематичното прогнозиране на бъдещи развития, предизвикателства и заплахи на равнището на Съюза и на световно равнище, са важни за създателите на политики, за промишлеността и ползвателите.

(6) В светлината на предизвикателствата, пред които е изправен Съюзът в областта на киберсигурността, е необходим всеобхватен набор от мерки, който ще се основава на предходни действия на Съюза и ще насърчава взаимно подкрепящите се цели. Тези цели включват необходимостта от допълнително подобряване на способностите и подготвеността на държавите членки и на предприятията, както и от подобряване на сътрудничеството, обмена на информация и координацията между държавите членки и институциите, органите, службите и агенциите на Съюза. Освен това, предвид трансграничния характер на киберзаплахите, е необходимо да се доразвият способностите на равнището на Съюза, чрез които могат да се допълват действията на държавите членки, по-специално в случаите на мащабни трансгранични инциденти и кризи, като същевременно се вземе предвид значението на поддържането и допълнителното засилване на националните способности за реакция спрямо киберзаплахи от всякакъв мащаб.

(7) Също така са необходими допълнителни усилия, за да се повиши информираността на гражданите, на организациите и на предприятията по въпроси, свързани с киберсигурността. Освен това, като се има предвид, че киберинцидентите накърняват доверието в доставчиците на цифрови услуги и в самия цифров единен пазар, особено сред потребителите, доверието следва да бъде допълнително укрепено, като по прозрачен начин се предоставя информация за нивото на сигурност на ИКТ продуктите, ИКТ услугите и ИКТ процесите, в която се подчертава, че дори и високото равнище на сертифициране на киберсигурността не може да гарантира пълната сигурност на ИКТ продукт, ИКТ услуга или ИКТ процес. Повишаването на доверието може да бъде улеснено чрез сертифициране на равнището на Съюза, като се предоставят общи изисквания за киберсигурност и общи критерии за оценка, независещи от националните пазари и секторите.

(8) Киберсигурността не е само въпрос, свързан с технологията, но и такъв, при който и човешкото поведение е също толкова важно. Поради това „киберхигиената“, а именно обикновените рутинни мерки, които — когато се прилагат и извършват редовно от граждани, организации и предприятия — сведат до минимум излагането им на рискове от киберзаплахи, следва да бъде активно насърчавана.

(9) За целите на укрепването на структурите за киберсигурност на Съюза е важно да се поддържат и развиват способностите на държавите членки за всеобхватен отговор на киберзаплахи, включително трансгранични инциденти.

(10) Предприятията и отделните потребители следва да разполагат с точна информация за това с какво ниво на гарантиране на сигурността са сертифицирани техните ИКТ продукти, ИКТ услуги и ИКТ процеси. Същевременно трябва да се разбира, че никой ИКТ продукт или ИКТ услуга не е напълно сигурен по отношение на киберзаплахите и че основните правила на киберхигиената трябва да се насърчават и да бъдат приоритет. Предвид нарастващата наличност на устройства за „интернет на нещата“ има редица доброволни мерки, които частният сектор следва да вземе, за да укрепи доверието в сигурността на ИКТ продуктите, ИКТ услугите и ИКТ процесите.

(11) Съвременните ИКТ продукти и системи често включват или разчитат на технологии и компоненти на една или повече трети страни, като софтуерни модули, библиотеки или приложно-програмни интерфейси. Подобно разчитане, което се нарича „зависимост“, може да породи допълнителни рискове, свързани с киберсигурността, тъй като открити уязвимости в компонентите на трета страна могат да повлияят на сигурността на ИКТ продуктите, ИКТ услугите и ИКТ процесите. В много случаи установяването и документирането на такива зависимости дава възможност на крайните ползватели на ИКТ продуктите, ИКТ услугите и ИКТ процесите да подобрят своите дейности по управление на риска, свързан с киберсигурността, като усъвършенстват например процедурите на ползвателите за управление и отстраняване на уязвимостта, свързана с киберсигурността.

([5]) Регламент (ЕС) № 526/2013 на Европейския парламент и на Съвета от 21 май 2013 г. относно Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) и за отмяна на Регламент (ЕО) № 460/2004 (ОВ L 165, 18.6.2013 г., стр. 41).

(12) Организациите, производителите или доставчиците, участващи в проектирането и разработването на ИКТ продукти, ИКТ услуги или ИКТ процеси, следва да бъдат насърчавани да прилагат мерки на най-ранните етапи по такъв начин, че сигурността на тези продукти, услуги и процеси да бъде защитена във възможно най-голяма степен от самото начало, понасянето на кибератаки да се предполага и тяхното въздействие да бъде предвидимо и сведено до минимум („сигурност още при проектирането“). Сигурността следва да бъде осигурена през целия жизнен цикъл на ИКТ продукта, ИКТ услугата и ИКТ процеса чрез процеси на проектиране и разработване, които се развиват постоянно с цел намаляване на вредите от злонамерена експлоатация.

(13) Предприятията, организациите и публичният сектор следва да конфигурират проектираните от тях ИКТ продукти, ИКТ услуги или ИКТ процеси по начин, който осигурява по-висока степен на сигурност, което следва да даде възможност на първия ползвател да получи конфигурация с възможно най-сигурни настройки („сигурност по подразбиране“) като така се намалява тежестта за ползвателите, които трябва да конфигурират даден ИКТ продукт, ИКТ услуга или ИКТ процес по подходящия начин. Сигурността по подразбиране не следва да изисква подробна работна конфигурация, нито конкретни технически познания или необичайно поведение от страна на потребителя и следва да работи надеждно, когато се внедрява. Ако за всеки отделен случай анализ на риска и използваемостта доведе до заключението, че такава настройка по подразбиране не е осъществима, ползвателите следва да бъдат приканени да изберат най-сигурната настройка.

(14) С Регламент (ЕО) № 460/2004 на Европейския парламент и на Съвета ([6]) беше създадена ENISA, предназначена да подпомогне целите за осигуряване на високо и ефективно ниво на мрежова и информационна сигурност в рамките на Съюза и създаване на култура на мрежова и информационна сигурност в полза на гражданите, потребителите, предприятията и държавните администрации. С Регламент (ЕО) № 1007/2008 на Европейския парламент и на Съвета ([7]) беше удължен мандатът на ENISA до март 2012 г. С Регламент (ЕС) № 580/2011 на Европейския парламент и на Съвета ([8]) мандатът на ENISA беше удължен допълнително до 13 септември 2013 г. С Регламент (ЕС) № 526/2013 беше удължен мандатът на ENISA до 19 юни 2020 г.

(15) Съюзът вече предприе важни стъпки за гарантиране на киберсигурността и за повишаване на доверието в цифровите технологии. През 2013 г. беше приета стратегия на Европейския съюз за киберсигурност, която да направлява политиката на Съюза в отговор на заплахите и рисковете в областта на киберсигурността. В усилията си да защити по-добре гражданите в онлайн средата, през 2016 г. Съюзът прие първия законодателен акт в областта на киберсигурността под формата на Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета ([9]). С Директива (ЕС) 2016/1148 бяха въведени изисквания по отношение на националните способности в областта на киберсигурността, бяха създадени първите механизми за засилване на стратегическото и оперативното сътрудничество между държавите членки и бяха въведени задължения относно мерките за сигурност и уведомяването за инциденти отвъд границите на отделните сектори, които са жизненоважни за икономиката и обществото, като енергетиката, транспорта, доставката и снабдяването с питейна вода, банковото дело, инфраструктурите на финансовия пазар, здравеопазването, цифровата инфраструктура, както и доставчиците на основни цифрови услуги (интернет търсачки, услуги за изчисления в облак и платформи за онлайн търговия).

ENISA получи основна роля в подпомагането на изпълнението на посочената директива. В допълнение, ефективната борба срещу киберпрестъпността е важен приоритет в Европейската програма за сигурност, с което се допринася за общата цел за постигане на високо равнище на киберсигурността. Други правни актове, като Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([10]) и директиви 2002/58/ЕО ([11]) и (ЕС) 2018/1972 ([12]) на Европейския парламент и на Съвета също допринасят за високото равнище на киберсигурността на цифровия единен пазар.

([6]) Регламент (ЕО) № 460/2004 на Европейския парламент и на Съвета от 10 март 2004 г. относно създаване на Европейската агенция за мрежова и информационна сигурност (ОВ L 77, 13.3.2004 г., стр. 1).

([7]) Регламент (ЕО) № 1007/2008 на Европейския парламент и на Съвета от 24 септември 2008 г. за изменение на Регламент (ЕО) № 460/2004 относно създаване на Европейска агенция за мрежова и информационна сигурност по отношение на срока на съществуване на агенцията (ОВ L 293, 31.10.2008 г., стр. 1).

([8]) Регламент (ЕС) № 580/2011 на Европейския парламент и на Съвета от 8 юни 2011 г. за изменение на Регламент (ЕО) № 460/2004 относно създаване на Европейската агенция за мрежова и информационна сигурност по отношение на срока на съществуване на агенцията (ОВ L 165, 24.6.2011 г., стр. 3).

([9]) Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194, 19.7.2016 г., стр. 1).

([10]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

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

([12]) Директива (ЕС) 2018/1972 на Европейския парламент и на Съвета от 11 декември 2018 г. за установяване на Европейски кодекс за електронни съобщения (преработена) (ОВ L 321, 17.12.2018 г., стр. 36).

(16) След приемането на Стратегията на Европейския съюз за киберсигурност от 2013 г. и след последното преразглеждане на мандата на ENISA общият контекст на политиката се промени значително, тъй като глобалната среда стана по-нестабилна и по-несигурна. В този смисъл и в контекста на положителното развитие на ролята на ENISA като референтно звено за становища и експертен опит, като помощник в сътрудничеството и изграждането на капацитет, както и в рамките на новата политика за киберсигурност в Съюза, е необходимо да се направи преглед на мандата на ENISA, за да се определи нейната роля в променената екосистема на киберсигурността и да се гарантира нейният ефективен принос в европейския отговор в борбата с предизвикателствата за киберсигурността, произтичащи от коренно променената картина на киберзаплахи, за които настоящият мандат не е достатъчен, както беше констатирано в оценката на ENISA.

(17) ENISA, която се създава с настоящия регламент, следва да бъде правоприемник на ENISA, създадена с Регламент (ЕС) № 526/2013. ENISA следва да изпълнява задачите, възложени ѝ с настоящия регламент и други правни актове на Съюза в областта на киберсигурността, като, наред с другото, предоставя консултации и експертен опит и действа като център на Съюза за информация и знания. Тя следва да насърчава обмена на добри практики между държавите членки и заинтересованите страни от частния сектор, да предоставя предложения за политики на Комисията и държавите членки, да действа като отправна точка за секторни политически инициативи на Съюза по въпросите на киберсигурността и да насърчава оперативното сътрудничество между държавите членки, както и между тях и институциите, органите, службите и агенциите на Съюза.

(18) В рамките на Решение 2004/97/ЕО, Евратом, взето с общо съгласие от представителите на държавите членки, заседаващи на равнище държавни или правителствени ръководители ([13]), представителите на държавите членки решиха, че седалището на ENISA ще бъде в град в Гърция, който ще бъде определен от гръцкото правителство. Приемащата ENISA държава членка следва да осигури възможно най-добрите условия за безпроблемното и ефективно функциониране на ENISA. За правилното и ефикасно изпълнение на задачите на ENISA, за целите на набирането на персонал и задържането му и за подобряване на ефикасността на дейностите за осъществяване на връзки е наложително ENISA да се установи в подходящо местоположение, което наред с другото да предоставя подходящи транспортни връзки и съоръжения за съпрузите и децата, придружаващи членовете на персонала на ENISA. Необходимите разпоредби следва да бъдат определени в споразумение между ENISA и приемащата държава членка, което се сключва след получаване на одобрението на управителния съвет на ENISA.

(19) Като се има предвид нарастващият брой на рисковете и предизвикателствата в областта на киберсигурността, пред които е изправен Съюзът, предоставените на ENISA финансови и човешки ресурси следва да бъдат увеличени, така че да отразяват нейната разширена роля и задачи, както и нейната ключова позиция в екосистемата на организациите, защитаващи цифровата екосистема на Съюза, с което на ENISA да се даде възможност ефективно да изпълнява възложените ѝ с настоящия регламент задачи.

(20) ENISA следва да постигне и запази високо равнище на експертен опит и да функционира като отправна точка, създавайки условия за увереност и доверие в единния пазар благодарение на своята независимост, качеството на предоставяните от нея консултации и разпространяваната от нея информация, прозрачността на своите процедури и прозрачността на своите методи на работа, както и добросъвестното изпълнение на възложените ѝ задачи. ENISA следва активно да подпомага усилията на национално равнище и да дава активен принос към усилията на Съюза, като същевременно изпълнява своите задачи в пълно сътрудничество с институциите, органите, службите и агенциите на Съюза, както и с държавите членки, като се избягва всяко дублиране на работата и се насърчават синергиите. Освен това работата на ENISA следва да се основава на приноса и на сътрудничеството с частния сектор и с други заинтересовани страни. В набор от задачи следва да се формулира как ENISA трябва да постига своите цели и същевременно да ѝ се предоставя възможност за гъвкаво функциониране.

(21) С цел осигуряване на адекватна подкрепа за оперативното сътрудничество между държавите членки ENISA следва допълнително да укрепи своите технически и човешки способности и умения. ENISA следва да увеличи своя ноу-хау и капацитет. ENISA и държавите членки биха могли на доброволна основа да разработят програми за командироване на национални експерти в ENISA, за създаване на експертни групи и обмен на служители.

(22) ENISA следва да подпомага Комисията чрез консултации, становища и анализи по всички въпроси на Съюза, свързани с разработването, актуализирането и преразглеждането на политиката и правото в областта на киберсигурността и специфичните за сектора аспекти с цел засилване на значението на политиките и правото на Съюза, свързани с киберсигурността, и осигуряване на последователност при прилагането на тези политики и право на национално равнище. ENISA следва да служи като отправна точка за консултации и експертен опит за специфичните секторни политики и правни инициативи на Съюза, когато те включват въпроси, свързани с киберсигурността. ENISA следва редовно да информира Европейския парламент относно своите дейности.

([13]) Решение 2004/97/ЕО, Евратом, взето по общо съгласие между представителите на държавите-членки на среща на равнище държавен глава или правителствен ръководител от 13 декември 2003 година относно местоположението на някои служби и агенции на Европейския съюз (ОВ L 29, 3.2.2004 г., стр. 15).

(23) Обществената ядро на отворения интернет, а именно неговите основни протоколи и инфраструктура, които са всеобщо обществено благо, осигурява основната функционалност на интернет като цяло и лежи в основата на неговото нормално функциониране. ENISA следва да допринася за сигурността на обществената ядро на отворения интернет и стабилността на неговото функциониране, включително, но не само — ключовите протоколи (по-специално DNS, BGP и IPv6), за експлоатацията на системата за имена на домейни (като тези на всички домейни от първо ниво), и за функционирането на кореновата зона.

(24) Основната задача на ENISA е да насърчава последователното прилагане на съответната правна рамка, по-конкретно ефективното изпълнение на Директива (ЕС) 2016/1148 и други съответни правни инструменти, съдържащи елементи, свързани с киберсигурността, което е от съществено значение за повишаване на киберустойчивостта. С оглед на бързо развиващата се картина на киберзаплахите е ясно, че държавите членки трябва да бъдат подкрепяни чрез по-широкообхватен подход, надхвърлящ границите на отделните политики, за изграждането на киберустойчивост.

(25) ENISA следва да подпомага държавите членки и институциите, органите, службите и агенциите на Съюза в усилията им да изградят и подобрят способностите си и подготвеността си за предотвратяване, откриване и реагиране на заплахи и инциденти в областта на киберсигурността, както и във връзка със сигурността на мрежите и информационните системи. По-специално, ENISA следва да подкрепя развитието и укрепването на националните екипи и екипите на Съюза за реагиране при инциденти с компютърната сигурност (CSIRTs), предвидени в Директива (ЕС) 2016/1148, с оглед на постигането на високо общо равнище на зрелост в рамките на Съюза. Осъществяваните от ENISA дейности, свързани с оперативния капацитет на държавите членки, следва активно да подкрепят действията на държавите членки с цел изпълнение на задълженията им съгласно Директива (ЕС) 2016/1148 и поради това не следва да ги заместват.

(26) ENISA следва също да съдейства за разработването и актуализирането на стратегии на равнището на Съюза, а при поискване — стратегии на държавите членки във връзка със сигурността на мрежите и информационните системи, по-специално в областта на киберсигурността и следва да насърчава разпространението на тези стратегии и да следи хода на тяхното изпълнение. Освен това ENISA следва да допринася за покриване на необходимостта от обучения и учебни материали, включително потребностите на публичните органи, и ако е целесъобразно до голяма степен да „обучава обучаващите“ въз основа на Рамката за цифрова компетентност на гражданите с оглед на помощта за държавите членки и институциите, органите и агенциите на Съюза в разработването на техни собствени способности за обучение.

(27) ENISA следва да подкрепя държавите членки във връзка с повишаването на осведомеността в областта на киберсигурността и образованието, като улеснява по-тясната координация и обмена на добри практики между държавите членки. Тази подкрепа би могла да се изразява, наред с другото, в развитието на мрежа от национални образователни звена за контакт и развитието на платформа за обучение в областта на киберсигурността. Мрежата от национални образователни звена за контакт би могла да развива дейност в рамките на мрежата на националните служители за връзка и да постави началото на бъдеща координация в рамките на държавите членки.

(28) ENISA следва да подпомага групата за сътрудничество, създадена с Директива (ЕС) 2016/1148, в изпълнението на нейните задачи, по-специално чрез предоставяне на експертен опит и консултации и чрез улесняване на обмена на най-добри практики, *inter alia* по отношение на определянето на операторите на основни услуги от държавите членки, както и по отношение на трансграничната зависимост във връзка с рисковете и инцидентите.

(29) С оглед на насърчаването на сътрудничеството между обществения и частния сектор и в рамките на частния сектор, по-специално в подкрепа на защитата на критичните инфраструктури, ENISA следва да подпомага обмена на информация в секторите и между тях, по-специално в секторите, изброени в приложение II към Директива (ЕС) 2016/1148, като им предоставя добри практики и насоки относно наличните инструменти, процедури, както и насоки относно решаването на нормативните проблеми във връзка с обмена на информация, например чрез улесняване създаването на секторни центрове за обмен и анализ на информация.

(30) Доколкото потенциалното отрицателно въздействие на уязвимостите на ИКТ продуктите, ИКТ услугите и ИКТ процесите постоянно се увеличава, тяхното установяване и отстраняване играе важна роля за намаляване на цялостния риск, свързан с киберсигурността. Установено е, че сътрудничеството между организациите, производителите на уязвими ИКТ продукти или доставчиците на уязвими ИКТ продукти, ИКТ услуги и ИКТ процеси и членовете на научноизследователската общност в областта на киберсигурността и правителствата, които откриват подобна уязвимост, значително повишава процента на откриване и отстраняване на уязвимостите на ИКТ продуктите, ИКТ услугите и ИКТ процесите. Координираното оповестяване на уязвимостта представлява структуриран процес на сътрудничество, при който уязвимостите се докладват на собственика на информационната система, което дава възможност на организацията да ги установи и отстрани преди подробна информация за тях да бъде предоставена на трети страни или на обществеността. Освен това процесът дава възможност за координация между страната, установила уязвимостта, и организацията по отношение на публикуването на посочените уязвимости. Политиките за координираното оповестяване на уязвимостта могат да играят важна роля в усилията на държавите членки за укрепване на киберсигурността.

(31) ENISA следва да обобщава и анализира доброволно подадените национални доклади от CSIRT и междуинституционалния екип за незабавно реагиране при компютърни инциденти, създаден с договореност между Европейския парламент, Европейския съвет, Съвета на Европейския съюз, Европейската комисия, Съда на Европейския съюз, Европейската централна банка, Европейската сметна палата, Европейската служба за външна дейност, Европейския икономически и социален комитет, Европейския комитет на регионите и Европейската инвестиционна банка относно организацията и функционирането на екип за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на Съюза (CERT-EU) ([14]) с цел осигуряване на принос за създаването на общи процедури, език и терминология за обмен на информация. В този контекст ENISA следва също така да включи частния сектор, в рамките на Директива (ЕС) 2016/1148, с която бяха положени основите за доброволен обмен на техническа информация на оперативно равнище в мрежата от екипи за реагиране при инциденти с компютърната сигурност („мрежа на CSIRT“), създадена с посочената директива.

(32) ENISA следва да допринася за реакцията на равнището на Съюза в случай на мащабни трансгранични инциденти и кризи, свързани с киберсигурността. Тази задача следва да бъде изпълнявана в съответствие с мандата на ENISA съгласно настоящия регламент и подход, който да бъде съгласуван от държавите членки в контекста на Препоръка (ЕС) 2017/1584 ([15]) на Комисията и заключенията на Съвета от 26 юни 2018 г. относно координирана реакция на мащабни киберинциденти и кризи. Тази задача би могла да включва събирането на съответна информация и поемането на ролята на посредник между мрежата на CSIRT, техническата общност и вземащите решения, отговарящи за управлението на кризи. Освен това ENISA би могла да подпомогне оперативното сътрудничество между държавите членки по искане на една или повече държави членки в справянето с инциденти в технически аспект посредством улесняването на съответния технически обмен на решения между държавите членки и приноса за публичното осведомяване. ENISA следва да подкрепя оперативното сътрудничество, като проверява как функционират договореностите на това сътрудничество чрез редовни учения в областта на киберсигурността.

(33) При подпомагане на оперативното сътрудничество ENISA следва да използва наличния технически и оперативен експертен опит на CERT-EU чрез структурирано сътрудничество. Структурираното сътрудничество може да се развива въз основа на експертния опит на ENISA. Когато е целесъобразно, следва да бъдат сключени специални договорености между двете организации, за да се определи практическото изражение на това сътрудничество и да се избегне дублирането на дейности.

(34) В съответствие със задачите си за подпомагане на оперативното сътрудничество в рамките на мрежата CSIRT ENISA следва да е в състояние да оказва подкрепа на държавите членки по тяхно искане, например като предоставя консултации относно начините за подобряване на техния капацитет за предотвратяване, откриване и реагиране на инциденти, като улеснява справянето в технически аспект с инциденти със значително или съществено въздействие или като осигурява анализи на киберзаплахите и инцидентите. ENISA следва да спомага за справянето в технически аспект с инциденти със значително или съществено въздействие, по-специално като подкрепя доброволния обмен на технически решения между държавите членки или като изготвя комбинирана техническа информация, например технически решения, обменяни доброволно от държавите членки. В препоръка (ЕС) 2017/1584 се препоръчва държавите членки да си сътрудничат добросъвестно и да обменят информация помежду си и с ENISA относно мащабни инциденти и кризи, свързани с киберсигурността без излишно забавяне. Тази информация допълнително ще помогне на ENISA при изпълнението на нейните задачи за подпомагане на оперативното сътрудничество.

(35) Като част от редовното сътрудничество на техническо равнище за подпомагане на ситуационната осведоменост на Съюза, ENISA следва редовно и в тясно сътрудничество с държавите членки да изготвя задълбочени технически доклади за състоянието на киберсигурността в ЕС във връзка с инциденти и киберзаплахи въз основа на публично достъпна информация, свои собствени анализи, както и доклади, подадени от CSIRT на държавите членки или от единните звена за контакт по сигурността на мрежите и информационните системи (наричани по-долу „единните звена за контакт“), предвидени в Директива (ЕС) 2016/1148, и двете на доброволна основа, Европейския център за борба с киберпрестъпността (EC3) към Европол, CERT-EU, и когато е целесъобразно — от Центъра на ЕС за анализ на информация (EU INTCEN) към Европейската служба за външна дейност. Докладите следва да се предоставят на Съвета, Комисията, върховния представител на Съюза по въпросите на външните работи и политиката на сигурност и мрежата на CSIRT.

(36) Подкрепата на ENISA по отношение на последващите технически разследвания на инциденти със значително или съществено въздействие, предприети по искане на засегнатите държави членки, следва да се съсредоточи върху предотвратяването на бъдещи инциденти. Засегнатите държави членки следва да предоставят необходимата информация и помощ, за да може ENISA ефективно да подпомага последващото техническо разследване.

([14]) ОВ C 12, 13.1.2018 г., стр. 1.
([15]) Препоръка (ЕС) 2017/1584 на Комисията от 13 септември 2017 г. относно координирана реакция на мащабни киберинциденти и кризи (ОВ L 239, 19.9.2017 г., стр. 36).

(37) Държавите членки могат да приканят засегнати от инцидента предприятия да сътрудничат, като предоставят необходимата информация и съдействие на ENISA, без да се накърнява правото им на защита на поверителната търговска информация и информацията от значение за обществената сигурност.

(38) С оглед да се разберат по-добре предизвикателствата в областта на киберсигурността и да се предоставят стратегически дългосрочни препоръки на държавите членки и институциите, органите, службите и агенциите на Съюза, ENISA трябва да анализира текущите и нововъзникващи рискове, свързани с киберсигурността. За тази цел ENISA, в сътрудничество с държавите членки и, по целесъобразност, със статистически органи и други органи, следва да събира съответната публично достъпна или доброволно подадена информация, да извършва анализи на нововъзникващите технологии и да предоставя тематично ориентирани оценки на очакваните социални, правни, икономически и регулаторни въздействия на дадени технологични иновации в областта на мрежовата и информационната сигурност, по-специално в областта на киберсигурността. Освен това ENISA следва да подпомага държавите членки и институциите, органите, службите и агенциите на Съюза при установяването на възникващите рискове, свързани с киберсигурността и предотвратяването на инциденти, като извършва анализи на киберзаплахите, уязвимостта и инцидентите.

(39) С цел да се повиши устойчивостта на Съюза, ENISA следва да развие капацитет в областта на киберсигурността на инфраструктурите, по-специално за да подпомогне секторите, изброени в приложение II към Директива (ЕС) 2016/1148, и инфраструктурите, използвани от доставчици на цифровите услуги, изброени в приложение III към същата директива, като предоставя съвети, дава насоки и обменя добри практики. С оглед да се осигури по-лесен достъп до по-добре структурирана информация относно рисковете, свързани с киберсигурността и възможните средства за защита, ENISA следва да разработи и поддържа „информационен център“ на Съюза — портал за „обслужване на едно гише“, който осигурява на обществеността информация относно киберсигурността, получена от институциите, органите, службите и агенциите на Съюза и от националните институции, органи, служби и агенции. Улесняването на достъпа до по-добре структурирана информация относно рисковете, свързани с киберсигурността и възможните средства за защита може също да помогне на държавите членки да подобрят своя капацитет и да приведат в съответствие своите практики, с което да увеличат цялостната си устойчивост на кибератаки.

(40) ENISA следва да допринася за повишаването на обществената осведоменост, включително посредством кампании за повишаване на осведомеността в ЕС, чрез насърчаване на образованието относно рисковете, свързани с киберсигурността, и за предлагането на насоки относно добри практики за отделните ползватели, насочени към гражданите, организациите и предприятията. ENISA следва също така да допринася за насърчаването на добрите практики и решения, включително киберхигиената и киберграмотността, на равнище граждани, организации и предприятия, като събира и анализира обществено достъпна информация относно значителни инциденти, и като изготвя и публикува доклади и насоки за гражданите, организациите и предприятията, както и за подобряването на цялостното ниво на подготвеност и устойчивост. ENISA следва да се стреми също така да предоставя на потребителите подходяща информация относно приложимите схеми за сертифициране, като например предоставя насоки и препоръки. Освен това ENISA следва да организира, в съответствие с Плана за действие в областта на цифровото образование, съдържащ се в съобщение на Комисията от 17 януари 2018 г., и в сътрудничество с институциите, органите, службите и агенциите на Съюза и държавите членки, редовни разяснителни и обществени образователни кампании за крайните ползватели, насочени към насърчаването на по-безопасно поведение онлайн на физическите лица, цифровата грамотност и повишаването на осведомеността за потенциалните киберзаплахи, включително престъпни действия онлайн като фишинг, ботмрежи, финансови и данъчни измами, инциденти, свързани с измамите с данни, а също така насочени към разпространението на основни съвети относно многофакторната автентификация, коригирането на грешките, криптирането, анонимизирането и защитата на данните.

(41) ENISA следва да играе централна роля за по-бързото осведомяване на крайните ползватели относно сигурността на изделията и сигурното използване на услуги и да популяризира на равнището на Съюза „сигурността още при проектирането“ и „защитата на личните данни още при проектирането“. За да постигне тази цел, ENISA следва да се възползва максимално от наличните добри практики и опит, особено добрите практики и опит на академичните институции и изследователите в сферата на ИТ сигурността.

(42) За да се подпомогнат предприятията, извършващи дейност в сектора на киберсигурността, както и ползвателите на решения в областта на киберсигурността, ENISA следва да разработи и поддържа „обсерватория на пазара“, като извършва редовни анализи и разпространява информация за основните тенденции на пазара на киберсигурността, както по отношение на търсенето, така и по отношение на предлагането.

(43) ENISA следва да допринася към усилията на Съюза за сътрудничество с международни организации, както и в контекста на подходящи международни рамки за сътрудничество в областта на киберсигурността. По-специално ENISA следва да допринася, когато е необходимо, за сътрудничеството с организации като ОИСР, ОССЕ и НАТО. Това сътрудничество може да включва съвместни учения в областта на киберсигурността и съвместна координация на реакцията при инциденти. Тези дейности трябва да се осъществяват при пълно зачитане на принципите на приобщаване, реципрочност и автономност на вземането на решения на Съюза, без да се засяга специфичният характер на политиката за сигурност и отбрана на която и да е държава членка.

(44) За да се гарантира, че ENISA ще постигне изцяло своите цели, тя следва да си сътрудничи със съответните надзорни и други компетентни органи в Съюза, с институциите, органите, службите и агенциите на Съюза, в това число CERT-EU, EC3, Европейската агенция по отбрана (EDA), Европейската глобална навигационна спътникова система (Европейската агенция за ГНСС), Органа на европейските регулатори в областта на електронните съобщения (ОЕРЕС), Европейската агенция за оперативното управление на широкомащабни информационни системи в областта на свободата, сигурността и правосъдието (eu-LISA), Европейската централна банка (ЕЦБ), Европейския банков орган (ЕБО), Европейския комитет по защита на данните, Агенцията на ЕС за сътрудничество между регулаторите на енергия (ACER), Агенцията за авиационна безопасност на Европейския съюз (ЕААБ) и всяка друга агенция на Съюза, която действа в областта на киберсигурността. ENISA следва също така да поддържа връзка с органите, които работят в областта на защитата на данните, с цел да обменя с тях ноу-хау и най-добри практики и следва да предоставя консултации относно въпроси на киберсигурността, които биха могли да окажат влияние върху тяхната работа. Правоприлагащите органи на национално равнище и на равнището на Съюза и органите за защита на данните следва да имат правото да бъдат представлявани в консултативната група на ENISA. При сътрудничеството си с правоприлагащите органи по въпроси на мрежовата и информационната сигурност, които биха могли да окажат влияние върху тяхната работа, ENISA следва да спазва съществуващите информационни канали и изградени мрежи.

(45) Биха могли да бъдат установени партньорства с академични институции, които имат научноизследователски инициативи в съответните области, като следва да съществуват съответни пътища за принос на организациите на потребителите и на други организации, който да бъде вземан под внимание.

(46) ENISA, в ролята си на секретариат на мрежата на CSIRT, следва да подкрепя екипите CSIRT на държавите членки и екипите CERT-EU при оперативното сътрудничество във връзка със съответните задачи на мрежата на CSIRT, както е посочено в Директива (ЕС) 2016/1148. Наред с това ENISA следва да насърчава и подкрепя сътрудничеството между съответните екипи CSIRT в случай на инциденти, атаки или нарушения в работата на мрежите или инфраструктурата, управлявани или защитавани от екипите CSIRT, които включват или са в състояние да включват най-малко два екипа CSIRT, като същевременно взема предвид надлежно стандартните оперативни процедури на мрежата на CSIRT.

(47) С оглед на повишаването на подготвеността на Съюза за реагиране на инциденти, ENISA следва редовно да организира учения в областта на киберсигурността на равнището на Съюза и да помага на държавите членки и на институциите, органите, службите и агенциите на Съюза, по тяхно искане, при организирането на такива учения. Веднъж на всеки две години следва да се организира широкомащабно всеобхватно учение, което да включва технически, оперативни и стратегически елементи. Освен това ENISA може да организира редовно по-ограничени по мащаб учения със същата цел — повишаване на подготвеността на Съюза за реагиране на инциденти.

(48) ENISA следва да продължава да развива и поддържа своя експертен опит в областта на сертифицирането на киберсигурността, с цел да подпомага политиките на Съюза в тази област. ENISA следва да развива дейността си, като надгражда на основата на съществуващите добри практики, и следва да насърчава внедряването на сертифицирането на киберсигурността в рамките на Съюза, включително като допринася за създаването и поддържането на рамка за сертифициране на киберсигурността на равнище на Съюза (Европейска рамка за сертифициране на киберсигурността), с цел повишаване на прозрачността на увереността в киберсигурността на ИКТ продуктите, ИКТ услугите и ИКТ процесите и, в крайна сметка, укрепване на доверието в цифровия вътрешен пазар и неговата конкурентоспособност.

(49) Ефективните политики за киберсигурност следва да се основават на добре разработени методи за оценяване на риска както в публичния, така и в частния сектор. Методите за оценка на риска се използват на различни нива, без да има обща практика относно най-добрия начин за тяхното ефикасно прилагане. Популяризирането и развитието на най-добри практики за оценяване на риска и за оперативно съвместими решения за управление на риска в организациите от публичния и частния сектор ще повиши нивото на киберсигурността в Съюза. За целта ENISA следва да подкрепя сътрудничеството между заинтересовани страни на равнището на Съюза и да ги подпомага в техните усилия, свързани с въвеждането и използването на европейски и международни стандарти за управление на риска и за измерима сигурност на електронните продукти, системи, мрежи и услуги, които заедно със софтуера са елементите, образуващи мрежите и информационните системи.

(50) ENISA следва да насърчава държавите членки, производителите или доставчиците на ИКТ продукти, ИКТ услуги и ИКТ процеси да повишават общите си стандарти за сигурност, така че всички ползватели на интернет да вземат необходимите мерки за гарантиране на собствената си киберсигурност и следва да проявява инициативност в това отношение. По-специално, производителите и доставчиците на ИКТ продукти, ИКТ услуги и ИКТ процеси следва да осигуряват необходимите актуализации и следва да изземат, изтеглят от пазара или рециклират ИКТ продукти, ИКТ услуги или ИКТ процеси, които не отговарят на нормите за киберсигурност, а вносителите и дистрибуторите следва да са сигурни, че ИКТ продуктите, ИКТ услугите и ИКТ процесите, които пускат на пазара на Съюза, отговарят на приложимите изисквания и не представляват риск за потребителите на Съюза.

(51) В сътрудничество с компетентните органи, ENISA следва да може да разпространява информация относно равнището на киберсигурността на ИКТ продуктите, ИКТ услугите и ИКТ процесите, предлагани на вътрешния пазар, и следва да отправя предупреждения по отношение на производителите или доставчиците на ИКТ продукти, ИКТ услуги или ИКТ процеси и да изисква от тях да подобрят сигурността на своите ИКТ продукти, ИКТ услуги или ИКТ процеси, включително киберсигурността.

(52) ENISA следва да взема под внимание в пълна степен текущата научноизследователска и развойна дейност и дейностите за оценка на технологиите, по-специално тези дейности, провеждани от различните научноизследователски инициативи на Съюза, за да съветва институциите, органите, службите и агенциите на Съюза и, когато е необходимо, държавите членки, по тяхно искане, относно необходимостта от научни изследвания и приоритети в областта на киберсигурността. С цел определяне на научноизследователските нужди и приоритети ENISA следва също така да се консултира със съответните групи ползватели. По-конкретно, би могло да се установи сътрудничество с Европейския съвет за научни изследвания, Европейския институт за иновации и технологии и Европейския институт за изследване на сигурността.

(53) При изготвянето на европейските схеми за сертифициране на киберсигурността ENISA следва редовно да се консултира с организациите за стандартизация, по-специално европейските организации за стандартизация.

(54) Киберзаплахите представляват глобален проблем. Необходимо е по-тясно международно сътрудничество с цел подобряване на стандартите за киберсигурност, включително необходимо е определяне на общи норми на поведение, приемане на кодекси за поведение, използване на международни стандарти, обмен на информация, насърчаване на по-бързи форми на международно сътрудничество при реагиране на проблеми на мрежовата и информационната сигурност, както и общ глобален подход към такива проблеми. За тази цел ENISA следва да подкрепя по-задълбоченото ангажиране на Съюза и сътрудничеството с трети държави и международни организации, като предоставя, където е уместно, необходимия експертен опит и анализи на съответните институции, органи, служби и агенции на Съюза.

(55) ENISA следва да бъде в състояние да отговаря на *ad hoc* искания за консултации и помощ от страна на държавите членки и институциите, органите, службите и агенциите на Съюза по въпроси, попадащи в обхвата на мандата на ENISA.

(56) Разумно и препоръчително е да се прилагат определени принципи по отношение на управлението на ENISA, за да се спази съвместното изявление и общия подход, договорени от междуинституционалната работна група за децентрализираните агенции на ЕС през юли 2012 г., чиято цел е усъвършенстването на дейността на агенциите и подобряването на техните резултати. Препоръките на съвместното изявление и на общия подход следва също да се отчитат, когато е уместно, в работните програми на ENISA, оценките на ENISA, както и докладването и административната практика на ENISA.

(57) Управителният съвет, състоящ се от представители на държавите членки и на Комисията, следва да определя общата насока на дейността на ENISA и да гарантира, че тя изпълнява своите задачи в съответствие с настоящия регламент. Управителният съвет следва да получи правомощията, необходими за определяне на бюджета, проверка на изпълнението на бюджета, приемане на подходящи финансови правила, установяване на прозрачни работни процедури за вземане на решения от страна на ENISA, приемане на единния програмен документ на ENISA, приемане на собствен правилник за дейността на ENISA, назначаване на изпълнителния директор и вземане на решения за удължаване или прекратяване на неговия мандат.

(58) С оглед на правилното и ефективно функциониране на ENISA Комисията и държавите членки следва да гарантират, че лицата, назначени в управителния съвет, притежават подходяща професионална компетентност и опит. Държавите членки и Комисията следва също да положат усилия да намалят текучеството на своите съответни представители в управителния съвет, за да се гарантира непрекъснатост на работата му.

(59) Гладкото функциониране на ENISA налага нейният изпълнителен директор да се назначава въз основа на неговите заслуги и документирани административни и управленски умения, както и въз основа на неговите компетентност и опит, свързани с киберсигурността. Задълженията на изпълнителния директор следва да се изпълняват в условия на пълна независимост. Изпълнителният директор следва да изготвя предложение за годишна работна програма на ENISA след предварителни консултации с Комисията и следва да предприема всички необходими стъпки за гарантиране на правилното изпълнение на тази работна програма. Изпълнителният директор следва да изготвя ежегоден доклад, който се изпраща на управителния съвет и който включва изпълнението на годишната работна програма на ENISA, да съставя проект на разчета за предвидените приходи и разходи на ENISA, както и да изпълнява бюджета. Освен това, изпълнителният директор следва да разполага с възможността да сформира *ad hoc* работни групи за решаване на специфични въпроси, по-специално въпроси с научен, технически, правен или социално-икономически характер. Създаването на *ad hoc* работна група се счита за необходимо в частност във връзка с подготовката на конкретен проект за европейска схема за сертифициране на киберсигурността („проект за схема“). Изпълнителният директор следва да гарантира, че членовете на *ad hoc* работните групи се избират съобразно най-високите стандарти за експертни знания, като се стреми да гарантира баланс между половете и подходящ баланс в зависимост от

конкретния въпрос, между държавните администрации на държавите членки, институциите, органите, службите и агенциите на Съюза и частния сектор, включително индустрията, ползвателите и академичните експерти в областта на мрежовата и информационната сигурност.

(60) Изпълнителният съвет следва да допринася за ефективното функциониране на управителния съвет. Като част от подготвителната си работа във връзка с решенията на управителния съвет, изпълнителният съвет следва да разглежда подробно съответната информация, да проучва възможните варианти и да предлага консултации и решения за изготвяне на решенията на управителния съвет.

(61) ENISA следва да разполага с консултативна група на ENISA в ролята на консултативен орган, за да се гарантира редовен диалог с частния сектор, потребителските организации и другите заинтересовани страни. Консултативната група на ENISA, сформирана от управителния съвет по предложение на изпълнителния директор, следва да се съсредоточи върху въпроси, засягащи заинтересованите страни, и следва да насочва вниманието на ENISA към тях. С консултативната група на ENISA следва да се проведат консултации относно проекта на годишна работна програма на ENISA. Съставът на Консултативната група на ENISA и задачите, които ѝ се възлагат, следва да гарантират достатъчна степен на представяне на заинтересованите страни в работата на ENISA.

(62) Следва да се създаде Група на заинтересованите страни в областта на сертифицирането на киберсигурността, която да помага на ENISA и на Комисията в осъществяването на консултациите със съответните заинтересовани страни. Групата на заинтересованите страни в областта на сертифицирането на киберсигурността следва да се състои от членове, представляващи сектора в балансирано съотношение, както от страна на търсенето, така и от страна на предлагането на ИКТ продукти и ИКТ услуги, включително по-специално МСП, доставчиците на цифрови услуги, европейските и международните органи по стандартизация, националните органи по акредитация, надзорните органи по защита на данните и органите за оценяване на съответствието съгласно Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета ([16]), академичните среди и организациите на потребителите.

(63) ENISA следва да има правила за предотвратяването и управлението на конфликти на интереси. ENISA следва също така да прилага съответните разпоредби на Съюза относно публичния достъп до документи, както е посочено в Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета ([17]). ENISA следва да обработва лични данни в съответствие с Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([18]). ENISA следва да съблюдава разпоредбите, приложими за институциите, органите, службите и агенциите на Съюза, както и националното законодателство относно обработката на информация, по-специално на чувствителната некласифицирана информация и на класифицирана информация на Европейския съюз.

(64) За да се гарантира пълната автономност и независимост на ENISA и за да може тя да изпълнява допълнителни задачи, включително непредвидени задачи в спешни случаи, на ENISA следва да бъде предоставен достатъчен и автономен бюджет, чиито приходи следва да се набавят най-вече чрез вноска на Съюза и вноски на трети държави, вземащи участие в работата на ENISA. Подходящият бюджет е от основно значение, за да се гарантира, че ENISA има достатъчно капацитет, за да изпълнява всички свои увеличаващи се задачи и за да постига целите си. Поголямата част от персонала на ENISA следва да е пряко ангажирана с оперативното изпълнение на мандата на ENISA. Приемащата държава членка и всяка друга държава членка следва да могат да правят доброволни вноски към бюджета на ENISA. Бюджетната процедура на Съюза следва да остане приложима по отношение на всякакви субсидии, платими от общия бюджет на Съюза. Освен това Сметната палата следва да одитира финансовите отчети на ENISA, за да се гарантират прозрачност и отчетност.

(65) Сертифицирането на киберсигурността играе важна роля за повишаването на доверието в ИКТ продуктите, ИКТ услугите и ИКТ процесите. Цифровият единен пазар, и по-конкретно основаващата се на данни икономика и „интернет на нещата“, могат да функционират успешно само ако обществото като цяло е уверено, че тези продукти, услуги и процеси предоставят определено ниво на киберсигурността. Свързаните автомобили и автомобилите с автоматично управление, електронните медицински устройства, системите за управление на промишлената автоматизация и интелигентните енергийни мрежи са само някои от примерите за сектори, в които сертифицирането вече широко се използва или е вероятно да бъде използвано в близко бъдеще. Секторите, регулирани от Директива (ЕС) 2016/1148, са също така сектори, в които сертифицирането на киберсигурността е от ключово значение.

([16]) Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. за определяне на изискванията за акредитация и надзор на пазара във връзка с предлагането на пазара на продукти и за отмяна на Регламент (ЕИО) № 339/93 (ОВ L 218, 13.8.2008 г., стр. 30).

([17]) Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета от 30 май 2001 г. относно публичния достъп до документи на Европейския парламент, на Съвета и на Комисията (ОВ L 145, 31.5.2001 г., стр. 43).

([18]) Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39).

(66) В съобщението от 2016 г., озаглавено „Укрепване на отбранителната способност на Европа срещу кибератаки и изграждане на конкурентен и иновативен сектор на киберсигурността“, Комисията описа необходимостта от висококачествени, достъпни и оперативно съвместими продукти и решения, свързани с киберсигурността. Предлагането на ИКТ продукти, ИКТ услуги и ИКТ процеси в рамките на единния пазар остава обаче силно разпокъсано географски. Това е така, защото развитието на сектора на киберсигурността в Европа се основава главно на търсене от страна на националните правителства. Освен това, липсата на оперативно съвместими решения (технически стандарти), практики и прилагани в целия Съюз механизми за сертифициране е част от другите пропуски, които оказват влияние върху единния пазар в областта на киберсигурността. Това влошава конкурентоспособността на европейските предприятия в национален, европейски и световен мащаб. То също така ограничава избора на надеждни и приложими технологии за киберсигурност, до които лицата и предприятията имат достъп. Аналогично, в съобщението от 2017 г. относно междинния преглед на изпълнението на стратегията за цифровия единен пазар — свързан с интернет цифров единен пазар за всички, Комисията подчерта необходимостта от безопасни свързани продукти и системи и посочи, че създаването на европейска рамка за ИКТ сигурност, определяща правила относно организацията на сертифицирането на сигурността на ИКТ в ЕС, би могло да помогне както за запазването на доверието в интернет, така и за преодоляването на настоящата разпокъсаност на вътрешния пазар.

(67) Понастоящем сертифицирането на киберсигурността на ИКТ продукти, ИКТ услуги и ИКТ процеси се използва само в ограничена степен. Ако има такова, то се осъществява предимно на равнището на държавите членки или в рамките на секторно обусловени схеми. В тези условия сертификат, издаден от един национален орган за сертифициране на киберсигурността, по принцип не се признава от другите държави членки. Поради това може да се наложи предприятията да сертифицират своите ИКТ продукти, ИКТ услуги и ИКТ процеси в няколко държави членки, в които развиват дейност, например с цел да участват в националните процедури за възлагане на обществени поръчки, като по този начин увеличават разходите си. Освен това, въпреки че се появяват нови схеми, изглежда няма съгласуван и цялостен подход по отношение на хоризонталните въпроси, свързани с киберсигурността, например в сферата на „интернет на нещата“. Действащите схеми проявяват съществени недостатъци и различия по отношение на продуктовия обхват, нивата на увереност, съществените критерии и фактическото използване, което пречи на механизмите за взаимно признаване в Съюза.

(68) Бяха положени известни усилия за постигането на взаимно признаване на сертификати в рамките на Съюза. Те обаче имаха само частичен успех. Най-важният пример в това отношение е споразумението за взаимно признаване (СВП) на Групата на висшите служители по сигурността на информационните системи (SOG-IS). Макар да представлява най-важният модел за сътрудничество и взаимно признаване в областта на сертифицирането на сигурността, SOG-IS включва само част от държавите членки. Това ограничава ефективността на СВП на SOG-IS от гледна точка на вътрешния пазар.

(69) Поради това е необходимо да бъде възприет общ подход и да се въведе европейска рамка на сертифициране на киберсигурността, която определя основните хоризонтални изисквания за европейските схеми за сертифициране на киберсигурността, които ще бъдат разработени, и дава възможност европейските сертификати за киберсигурност и ЕС декларациите за съответствие за ИКТ продукти, ИКТ услуги или ИКТ процеси да бъдат признавани и използвани във всички държави членки. По този начин е от съществено значение да се гради върху съществуващи национални и международни схеми, както и върху системи за взаимно признаване, по-специално SOG-IS, и да се даде възможност за плавен преход от съществуващите схеми по такива системи към схеми по новата европейска рамка на сертифициране на киберсигурността. Европейската рамка на сертифициране на киберсигурността следва да има две цели. Първо тя следва да спомогне за повишаване на доверието в ИКТ продуктите, ИКТ услугите и ИКТ процесите, които са били сертифицирани по европейски схеми за сертифициране на киберсигурността. Второ тя следва да предотврати увеличаването на броя на противоречащи си или припокриващи се национални схеми за сертифициране на киберсигурността и по този начин да намали разходите за предприятията, упражняващи дейност на цифровия единен пазар. Европейските схеми за сертифициране на киберсигурността следва да бъдат недискриминационни и да се основават на европейски или международни стандарти, освен ако тези стандарти са неефективни или неподходящи за изпълнението на легитимните цели на Съюза в това отношение.

(70) Тази европейска рамка на сертифициране на киберсигурността следва да се въведе по еднакъв начин във всички държави членки, за да се избегне практиката да се търси „по-изгодната среда за сертифициране“ поради различия в строгостта на изискванията в различни държави членки.

(71) Европейските схеми за сертифициране на киберсигурността следва да бъдат изградени въз основа на вече съществуващото на международно и национално равнище и ако е необходимо, въз основа на технически спецификации от форуми и консорциуми, като се базират на изводите от сегашните силни страни и оценката и корекцията на слабостите.

(72) Необходими са гъвкави решения за киберсигурност, за да се изпреварват киберзаплахите, и следователно всяка схема за сертифициране следва да се създава по начин, по който се избягва рискът от бързо остаряване.

(73) Комисията следва да бъде оправомощена да приема европейски схеми за сертифициране на киберсигурността за специфични групи ИКТ продукти, ИКТ услуги и ИКТ процеси. Тези схеми следва да се прилагат и контролират от национални органи за сертифициране на киберсигурността, а сертификатите, издадени в рамките на тези схеми, следва да са валидни и да се признават на цялата територия на Съюза. Схемите за сертифициране, управлявани от промишлеността или от други частни организации, следва да не попадат в обхвата на настоящия регламент. Въпреки това, управляващите такива схеми органи следва да могат да предлагат на Комисията да ги разгледа като основа за схеми, които да бъдат одобрени като европейска схема за сертифициране на киберсигурността.

(74) Разпоредбите на настоящия регламент не следва да засягат правото на Съюза, с което се определят специфични правила за сертифициране на ИКТ продукти, ИКТ услуги и ИКТ процеси. По-конкретно с Регламент (ЕС) 2016/679 се установяват разпоредби за създаване на механизми за сертифициране и на печати и маркировки за защита на данните, чрез които се доказва съответствието с посочения регламент на операциите по обработката на данни от страна на контрольорите и обработващите тези данни. Тези механизми за сертифициране и тези печати и маркировки за защита на данните следва да позволяват на субектите, предоставящи своите данни, бързо да оценяват нивото на защита на данните на съответните ИКТ продукти, ИКТ услуги и ИКТ процеси. Настоящият регламент не засяга сертифицирането на операции по обработката на данни съгласно Регламент (ЕС) 2016/679, включително когато тези операции са включени в ИКТ продукти, ИКТ услуги и ИКТ процеси.

(75) Целта на европейските схеми за сертифициране на киберсигурността следва да бъде да се гарантира, че ИКТ продуктите, ИКТ услугите и ИКТ процесите, сертифицирани по такава схема, съответстват на специфицираните изисквания с цел да се защити наличността, автентичността, целостта и поверителността на съхраняваните, предавани или обработвани данни, или на свързаните с тях функции или услуги, предлагани от тези продукти, процеси и услуги през целия им жизнен цикъл. Не е възможно в настоящия регламент да се определят подробно изискванията за киберсигурност по отношение на всички ИКТ продукти, ИКТ услуги и ИКТ процеси. ИКТ продуктите, ИКТ услугите и ИКТ процесите и техните потребности във връзка с киберсигурността са толкова разнообразни, че е много трудно да се формулират общи изисквания за киберсигурност, които да са общовалидни. Поради това е необходимо да се приеме широко и общо понятие за киберсигурността за целите на сертифицирането, което следва да се допълва от набор от конкретни цели, свързани с киберсигурността, които трябва да бъдат вземани предвид при разработването на европейските схеми за сертифициране на киберсигурността. Условията, при които тези цели ще бъдат постигани при конкретни ИКТ продукти, ИКТ услуги и ИКТ процеси, следва да бъдат допълнително уточнявани в подробности на нивото на всяка отделна схема за сертифициране, приемана от Комисията, например чрез позоваване на стандарти или технически спецификации, ако не са налице подходящи стандарти.

(76) Техническите спецификации, които трябва да се използват в европейските схеми за сертифициране на киберсигурността, следва да спазват изискванията, установени в приложение II към Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета ([19]). Някои отклонения от тези изисквания биха могли обаче да се счетат за необходими в надлежно обосновани случаи, когато тези технически спецификации трябва да се използват в европейска схема за сертифициране на киберсигурността, отнасяща се до високо ниво на увереност. Следва да бъде осигурен публичен достъп до причините за тези отклонения.

(77) Оценяването на съответствието е процес на оценяване на изпълнението на специфицираните изисквания, свързани с ИКТ продукт, ИКТ услуга или ИКТ процес. Този процес се осъществява от независима трета страна, различна от производителя или доставчика на ИКТ продукта, ИКТ услугата или ИКТ процеса, които са оценявани. Европейски сертификат за киберсигурност следва да се издава след успешна оценка на ИКТ продукт, ИКТ услуга или ИКТ процес. Европейският сертификат за киберсигурност следва да се счита за потвърждение, че съответната оценка е извършена правилно. В зависимост от нивото на увереност, европейската схема за сертифициране на киберсигурността следва да посочва дали европейският сертификат за киберсигурност трябва да се издаде от частен или публичен орган. Оценяването на съответствието и сертифицирането сами по себе си не могат да гарантират, че сертифицираните ИКТ продукти, ИКТ услуги и ИКТ процеси са сигурни по отношение на киберзаплахите. Те представляват само процедури и технически методики за удостоверяване, че ИКТ продуктите, ИКТ услугите и ИКТ процесите са изпитани и отговарят на определени изисквания за киберсигурност, които са определени другаде, например в технически стандарти.

(78) Изборът от страна на ползвателите на европейски сертификати на киберсигурността на подходящото сертифициране и свързаните с него изисквания по отношение на сигурността следва да се основават на анализ на риска, свързан с използването на ИКТ продуктите, ИКТ услугите или ИКТ процесите. Поради това нивото на увереност следва да е съизмеримо със степента на риск, свързан с предвидената употреба на даден ИКТ продукт, ИКТ услуга или ИКТ процес.

([19]) Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета от 25 октомври 2012 г. относно европейската стандартизация, за изменение на директиви 89/686/ЕИО и 93/15/ЕИО на Съвета и на директиви 94/9/ЕО, 94/25/ЕО, 95/16/ЕО, 97/23/ЕО, 98/34/ЕО, 2004/22/ЕО, 2007/23/ЕО, 2009/23/ЕО и 2009/105/ЕО на Европейския парламент и на Съвета и за отмяна на Решение 87/95/ЕИО на Съвета и на Решение № 1673/2006/ЕО на Европейския парламент и на Съвета (ОВ L 316, 14.11.2012 г., стр. 12).

(79) Европейските схеми за сертифициране на киберсигурността може да предвидят оценяване на съответствието под отговорността единствено на производителя или доставчика на ИКТ продукти, ИКТ услуги или ИКТ процеси („самооценяване на съответствието“). В такива случаи следва да е достатъчно производителят или доставчикът на ИКТ продукти, ИКТ услуги или ИКТ процеси сам да извърши всички проверки, за да гарантира съответствието на ИКТ продуктите, ИКТ услугите или ИКТ процесите с европейската схема за сертифициране на киберсигурността. Самооценката на съответствието следва да се счита за подходяща за ИКТ продукти, ИКТ услуги или ИКТ процеси с ниска степен на сложност, които представляват малък риск за обществения интерес като опростени механизми за проектиране и производство. Освен това самооценката на съответствието следва да се разрешава само за ИКТ продукти, ИКТ услуги или ИКТ процеси само при условие че те съответстват на ниво на увереност „базово“.

(80) Европейските схеми за сертифициране на киберсигурността може да дадат възможност както за самооценка, така и за сертифициране на съответствието на ИКТ продукти, ИКТ услуги или ИКТ процеси. В този случай схемата следва да предоставя ясни и разбираеми способи за потребителите или други ползватели да направят разграничение между ИКТ продукти, ИКТ услуги или ИКТ процеси, чието оценяване се прави под отговорността на производителя или доставчика на ИКТ продукти, ИКТ услуги или ИКТ процеси и ИКТ продукти, ИКТ услуги или ИКТ процеси, които са сертифицирани от трета страна.

(81) Производителят или доставчикът на ИКТ продукти, ИКТ услуги или ИКТ процеси, който прави самооценяване на съответствието, следва да може да издаде и подпише ЕС декларация за съответствие като част от процедурата за оценяване на съответствието. ЕС декларацията за съответствие е документ, в който се посочва, че конкретен ИКТ продукт, ИКТ услуга или ИКТ процес отговаря на изискванията на европейската схема за сертифициране на киберсигурността. Чрез издаването и подписването на ЕС декларацията за съответствие производителят или доставчикът на ИКТ продукти, ИКТ услуги или ИКТ процеси поема отговорност за съответствието на ИКТ продукта, ИКТ услугата или ИКТ процеса с правните изисквания на европейската схема за сертифициране на киберсигурността. Копие от ЕС декларацията за съответствие следва да се предостави на националния орган за сертифициране на киберсигурността и на ENISA.

(82) Производителите или доставчиците на ИКТ продукти, ИКТ услуги или ИКТ процеси следва да предоставят ЕС декларацията за съответствие, техническата документация и всякаква друга относима информация във връзка със съответствието на ИКТ продуктите, ИКТ услугите или ИКТ процесите с дадена европейска схема за сертифициране на киберсигурността, на разположение на компетентния национален орган за сертифициране на киберсигурността за срок, определен в съответната европейска схема за сертифициране на киберсигурността. Техническата документация следва да определя приложимите съгласно схемата изисквания и следва да обхваща проектирането, производството и функционирането на ИКТ продукта, ИКТ услугата или ИКТ процеса до степента, необходима за самооценяването. Техническата документация следва да е изготвена така, че да предоставя възможност за оценяване дали даден ИКТ продукт, ИКТ услуга или ИКТ процес отговаря на приложимите съгласно посочената схема изисквания.

(83) В управлението на европейската рамка за сертифициране на киберсигурността се отчита участието на държавите членки, както и подходящото участие на заинтересованите страни, и се определя ролята на Комисията в процеса на планиране и предлагане, поискване, подготовка, приемане и преразглеждане на европейските схеми за сертифициране на киберсигурността.

(84) С помощта на Европейската група за сертифициране на киберсигурността и на Групата на заинтересованите страни в областта на сертифицирането на киберсигурността, както и след открита и широка консултация, Комисията следва да изготви непрекъсната работна програма на Съюза за европейските схеми за сертифициране на киберсигурността и следва да я публикува под формата на инструмент без обвързващ характер. Непрекъснатата работна програма на Съюза следва да бъде стратегически документ, който да позволява по-специално на предприятията, на националните органи и органите по стандартизация, по-специално, да се подготвят предварително за бъдещите европейски схеми за сертифициране на киберсигурността. Непрекъснатата работна програма на Съюза следва да включва многогодишен преглед на проектите за схеми, които Комисията възнамерява да представи на ENISA за подготовка въз основа на конкретни основания. Комисията следва да се съобрази с непрекъснатата работна програма на Съюза при изготвянето на техния непрекъснат план за стандартизация на ИКТ и исканията за стандартизация към европейски организации за стандартизация. С оглед на бързото въвеждане и внедряване от потребителите и предприятията на новите технологии, възникването на допреди неизвестни рискове, свързани с киберсигурността и на законодателни и пазарни промени, Комисията или Европейската група за сертифициране на киберсигурността следва да има правото да поиска от ENISA да подготви проекти за схеми, които не са включени в непрекъснатата работна програма на Съюза. В такива случаи Комисията и Европейската група за сертифициране на киберсигурността следва да направят също оценка на необходимостта от това искане, като вземат под внимание общите и конкретните цели на настоящия регламент и необходимостта да се гарантира последователност по отношение на планирането и използването на ресурсите от страна на ENISA.

След отправянето на такова искане ENISA следва да подготви своевременно проекти за схеми за конкретните ИКТ продукти, ИКТ услуги или ИКТ процеси. Комисията следва да направи оценка на положителното и отрицателното въздействие на своето искане върху въпросния конкретен пазар, особено върху малките и средните предприятия, иновациите, бариерите за навлизане на този пазар и цената за крайните ползватели. Комисията следва да бъде оправомощена да приема посредством актове за изпълнение европейските схеми за сертифициране на киберсигурността въз основава на проектите за схеми, изготвени от ENISA. Като се вземат предвид общата цел и целите, свързани със сигурността, определени в настоящия регламент, в европейските схеми за сертифициране на киберсигурността, приемани от Комисията, следва да бъде определен минимален набор от елементи по отношение на предмета, обхвата и функционирането на дадена схема. Тези елементи следва да включват, наред с другото, обхвата и предмета на сертифицирането на киберсигурността, включително обхванатите категории ИКТ продукти, ИКТ услуги и ИКТ процеси, подробна спецификация на изискванията за киберсигурност, например чрез позоваване на стандарти или технически спецификации, конкретните критерии и методи за оценка, както и желаното ниво на увереност („базово“, „съществено“ или „високо“), и нивата на оценка, когато е приложимо. ENISA следва да може да откаже искане на Европейската група за сертифициране на киберсигурността. Такива решения следва да бъдат вземани от управителния съвет и следва да бъдат надлежно обосновани.

(85) ENISA следва да поддържа уебсайт, предоставящ информация и повишаващ осведомеността относно европейските схеми за сертифициране на киберсигурността, който следва да включва, наред с другото, исканията за изготвяне на проект за схема, както и обратната информация, получена в процеса на консултации, проведени от ENISA през етапа на изготвянето. Този уебсайт следва да предоставя и информация относно европейските сертификати за киберсигурност и ЕС декларациите за съответствие, издавани съгласно настоящия регламент, включително информация за тяхното оттегляне или за изтичането на срока на действие на такива европейски сертификати за киберсигурност и ЕС декларации за съответствие. На уебсайта също следва да бъдат посочени националните схеми за сертифициране на киберсигурността, които са заменени от европейска схема за сертифициране на киберсигурността.

(86) Нивото на увереност чрез европейска схема за сертифициране е основата на увереността, че даден ИКТ продукт, ИКТ услуга или ИКТ процес отговаря на изискванията за сигурност на конкретна европейска схема за сертифициране на киберсигурността. С цел да се гарантира последователността на европейската рамка за сертифициране на киберсигурността, дадена европейска схема за сертифициране на киберсигурността следва да може да определи нивата на увереност за европейските сертификати за киберсигурност и ЕС декларациите за съответствие, издавани в рамките на тази схема. Всеки европейски сертификат за киберсигурност може да посочва едно от следните нива на увереност: „базово“, „съществено“ или „високо“, докато ЕС декларацията за съответствие може да посочва единствено до ниво на увереност „базово“. Нивата на увереност предвиждат съответстваща взискателност и задълбоченост на оценката на ИКТ продукт, ИКТ услуга или ИКТ процес и се характеризират с позоваване на техническите спецификации, стандарти и процедури, свързани с тях, включително техническите проверки, чиято цел е да се смекчат или предотвратят инциденти. Всяко ниво на увереност следва да бъде последователно по отношение на различните секторни области, в които се прилага сертифициране.

(87) Дадена европейска схема за сертифициране на киберсигурността може да определи няколко нива на оценка в зависимост от стриктността и задълбочеността на използваната методика за оценка. Нивата на оценка следва да съответстват на едно от нивата на увереност и да бъдат свързани с подходяща комбинация от компоненти на увереността. За всички нива на увереност ИКТ продуктът, ИКТ услугата или ИКТ процесът следва да съдържа редица сигурни функции, както е установено в схемата, които могат да включват: сигурна конфигурация в готов вид, подписан код, сигурна актуализация и овладяване на зловреден код, използващ уязвимостите на софтуера, и пълна защита на стековата или динамичната памет. Тези функции следва да бъдат разработени и поддържани, като се използват ориентирани към сигурността подходи за разработване и свързани с това инструменти, за да се гарантира надеждното включване на ефективни софтуерни и хардуерни механизми.

(88) По отношение на ниво на увереност „базово“ оценката следва да се ръководи най-малко от следните компоненти на увереността: оценката следва да включва като минимум преглед на техническата документация на ИКТ продукта, ИКТ услугата или ИКТ процеса от орган за оценяване на съответствието. Когато сертифицирането включва ИКТ процеси, на технически преглед следва да подлежи и процесът, използван за проектиране, разработване и поддържане на ИКТ продукт или ИКТ услуга. Когато дадена европейска схема за сертифициране на киберсигурността предвижда самооценяване на съответствието, следва да е достатъчно производителят или доставчикът на ИКТ продукти, ИКТ услуги или ИКТ процеси да е извършил самооценяване на съответствието на ИКТ продуктите, ИКТ услугите или ИКТ процесите със схемата за сертифициране.

(89) По отношение на ниво на увереност „съществено“ оценката следва, в допълнение към ниво на увереност „базово“, да се ръководи най-малко от проверката на съответствието на функционалностите за сигурност на ИКТ продукта, ИКТ услугата или ИКТ процеса с неговата техническа документация.

(90) По отношение на ниво на увереност „високо“ оценката следва, в допълнение към ниво на увереност „съществено“, да се ръководи най-малко от изпитване на ефективността, при което се оценява устойчивостта на функционалностите за сигурност на ИКТ продукт, ИКТ услуга или ИКТ процес срещу сложни кибератаки, извършени от лица, притежаващи значителни умения и ресурси.

(91) Използването на европейското сертифициране на киберсигурност и ЕС декларациите за съответствие следва да остане доброволно, освен ако не е предвидено друго в правото на Съюза или в правото на държавите членки, прието в съответствие с правото на Съюза. При липсата на хармонизирано право на Съюза държавите членки могат да приемат национални технически правила в съответствие с Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета ([20]), предвиждащи задължително сертифициране по европейска схема за сертифициране на киберсигурността. Държавите членки могат също да прилагат използването на европейското сертифициране на киберсигурността в контекста на обществените поръчки и Директива 2014/24/ЕС на Европейския парламент и на Съвета ([21]).

(92) В някои области би могло да бъде необходимо в бъдеще да се въведат конкретни изисквания за киберсигуност и тяхното сертифициране за определени ИКТ продукти, ИКТ услуги или ИКТ процеси да стане задължително, за да се подобри нивото на киберсигурност в Съюза. Комисията следва редовно да следи въздействието на приетите европейски схеми за сертифициране на киберсигурността върху наличието на сигурни ИКТ продукти, ИКТ услуги и ИКТ процеси на вътрешния пазар и следва да прави оценка на нивото на използване на схемите за сертифициране от производителите или доставчиците на ИКТ продукти, ИКТ услуги и ИКТ процеси в Съюза. Преценката за ефективността на европейските схеми за сертифициране на киберсигурността и за задължителния характер на конкретни схеми следва да се прави в светлината на законодателството на Съюза в областта на киберсигурността, по-специално на Директива (ЕС) 2016/1148, като се има предвид сигурността на мрежите и информационните системи, използвани от операторите на основни услуги.

(93) Европейските сертификати за киберсигурност и ЕС декларациите за съответствие следва да помагат на крайните ползватели да правят информиран избор. Ето защо ИКТ продуктите, ИКТ услугите и ИКТ процесите, които са сертифицирани или за които е издадена ЕС декларация за съответствие, следва да се придружават от структурирана информация, адаптирана към очакваното ниво на технически познания на крайния ползвател, за когото са предназначени. Цялата информация следва да бъде налична онлайн и когато е подходящо във физическа форма. Крайният ползвател следва да получи достъп до информацията относно обозначението на схемата за сертифициране, нивото на увереност, описанието на киберрисковете, свързани с ИКТ продукт, ИКТ услуга или ИКТ процес, издаващия орган или институция или следва да може да получи копие на европейския сертификат за киберсигурност. Освен това крайният ползвател следва да бъде информиран за политиката на подкрепа по отношение на киберсигурността, а именно в продължение на какъв период може да очаква да получава актуализации или корекции във връзка с киберсигурността, от производителя или доставчика на ИКТ продукти, ИКТ услуги или ИКТ процеси. Където е приложимо следва да се дават насоки за действията или настройките, които крайният ползвател може да извършва, за да поддържа или повиши киберсигурността на ИКТ продукта или ИКТ услугата, както и информация за единната точка за контакт, на която да съобщава за кибератаки и от която да търси подкрепа в случаите на кибератаки (освен автоматичното докладване). Тази информация следва да бъде актуализирана редовно и да бъде предоставена на уебсайт, който дава информация относно европейските схеми за сертифициране на киберсигурността.

(94) За да бъдат постигнати целите на настоящия регламент и да се избегне разпокъсаност на вътрешния пазар, националните схеми или процедури за сертифициране на киберсигурността за ИКТ продукти, ИКТ услуги или ИКТ процеси, обхванати от европейска схема за сертифициране на киберсигурността, следва да престанат да пораждат правно действие от датата, определена от Комисията в актове за изпълнение. Освен това държавите членки следва да не въвеждат нови национални схеми за сертифициране на киберсигурността на ИКТ продукти, ИКТ услуги или ИКТ процеси, които са вече обхванати от съществуваща европейска схема за сертифициране на киберсигурността. Държавите членки не следва обаче да бъдат възпрепятствани да приемат или да запазват национални схеми за сертифициране за целите на националната сигурност. Държавите членки следва да информират Комисията и Европейската група по киберсигурността за всяко свое намерение да изготвят национални схеми за сертифициране на киберсигурността. Комисията и Европейската група по киберсигурността следва да оценят въздействието от новите национални схеми за сертифициране на киберсигурността върху доброто функциониране на вътрешния пазар и в светлината на стратегическите интереси вместо това да бъде поискана европейска схема за сертифициране на киберсигурността.

(95) Европейските схеми за сертифициране на киберсигурност са насочени към това да подпомогнат хармонизирането на практиките за киберсигурност в Съюза. Те трябва да допринасят за повишаване на нивото на киберсигурност в рамките на Съюза. При изготвяне на европейските схеми за сертифициране на киберсигурност следва да се отчете и даде възможност за разработване на нови иновации в областта на киберсигурността.

([20]) Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета от 9 септември 2015 г. установяваща процедура за предоставянето на информация в сферата на техническите регламенти и правила относно услугите на информационното общество (ОВ L 241, 17.9.2015 г., стр. 1).

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

(96) Европейските схеми за сертифициране на киберсигурността следва да вземат предвид настоящите методи за разработване на софтуер и хардуер и по-специално въздействието на честите актуализации на софтуера или фърмуера върху отделните европейски сертификати за киберсигурност. В европейските схеми за сертифициране на киберсигурността следва да се уточняват условията, при които актуализацията би могла да наложи повторно сертифициране на ИКТ продукта, ИКТ услугата или ИКТ процеса или намаляване на обхвата на конкретен европейски сертификат за киберсигурност, предвид евентуалните отрицателни ефекти, които актуализацията би могла да има върху спазването на изискванията за сигурност на този сертификат.

(97) След като дадена европейски схема за сертифициране на киберсигурността бъде приета, производителите или доставчиците на ИКТ продукти, ИКТ услуги или ИКТ процеси следва да могат да подават заявления за сертифициране на своите ИКТ продукти или ИКТ услуги до органа за оценяване на съответствието по техен избор навсякъде в Съюза. Органите за оценяване на съответствието следва да се акредитират от национален орган по акредитация, ако отговарят на конкретни изисквания, определени в настоящия регламент. Акредитацията следва да се издава за максимален срок от пет години и следва да може да бъде подновявана при същите условия, ако органът за оценяване на съответствието все още отговаря на изискванията. Националните органи по акредитация следва да ограничават, временно да прекратяват или да отнемат акредитацията на органа за оценяване на съответствието, ако условията за акредитация не са били спазени или вече не се спазват, или ако органът за оценяване на съответствието е нарушава настоящия регламент.

(98) Препратките в националното законодателство до национален стандарт, който е престанал да има правно действие поради влизането в сила на европейска схема за сертифициране на киберсигурността, може да бъдат източник на объркване. Поради това държавите членки следва да отразяват приемането на дадена европейска схема за сертифициране на киберсигурността в своето национално законодателство.

(99) За да се постигнат равностойни стандарти в целия Съюз, да се улесни взаимното признаване и да се насърчи цялостното приемане на европейските сертификати за киберсигурност и на ЕС декларациите за съответствие, следва да се въведе система на партньорски проверки между националните органи за сертифициране на киберсигурността. Партньорската проверка следва да обхваща процедури за надзор на съответствието на ИКТ продуктите, ИКТ услугите и ИКТ процесите с европейските сертификати за киберсигурност, за наблюдение на задълженията на производителите или доставчиците на ИКТ продукти, ИКТ услуги или ИКТ процеси, които извършват самооценка, за наблюдение на съответствието на органите за оценка, както и на това доколко са подходящи експертните познания и опит на служителите на органите, издаващи сертификати за ниво на увереност „високо“. Комисията следва да може, посредством акт за изпълнение, да приеме най-малко петгодишен план за партньорската проверка, както и да въведе критерии и методологии за функционирането на системата на партньорските проверки.

(100) Без да се засяга общата система на партньорски проверки, която следва да бъде въведена от всички национални органи за сертифициране на киберсигурността в европейската рамка за сертифициране на киберсигурността, някои европейски схеми за сертифициране на киберсигурността може да включват механизъм за партньорско оценяване за органите, издаващи европейски сертификати за киберсигурност за ИКТ продукти, ИКТ услуги и ИКТ процеси с ниво на обезпеченост „високо“ в рамките на тези схеми. Европейската група за сертифициране на киберсигурността следва да подкрепи въвеждането на такива механизми за партньорско оценяване. Партньорско оценяване следва по-специално да бъде насочено към въпроса дали засегнатите органи изпълняват своите задачи хармонично и може да включва механизми за оспорване. Следва да бъде осигурен публичен достъп до резултатите от партньорското оценяване. Съответните органи могат да приемат подходящи мерки за адаптиране съответно на своите практики и експертен опит.

(101) Държавите членки следва да определят един или повече национални органи за сертифициране на киберсигурността, които да упражняват надзор по отношение на спазването на задълженията, произтичащи от настоящия регламент. Национален орган за сертифициране на киберсигурността може да бъде съществуващ или нов орган. Освен това дадена държава членка следва да може, след споразумение с друга държава членка, да определи един или повече национални органи за сертифициране на киберсигурността на територията на тази друга държава членка.

(102) Националните органи за сертифициране на киберсигурността следва по-специално да наблюдават и налагат задълженията на производителите или доставчиците на ИКТ продукти, ИКТ услуги или ИКТ процеси, установени на съответната им територия, във връзка с ЕС декларацията за съответствие, следва да подпомагат националните орани по акредитация при наблюдението и надзора на дейностите на органите за оценяване на съответствието, като им предоставят експертен опит и имаща отношение информация, следва да разрешават на органите за оценяване на съответствието да осъществяват задачите си, когато отговарят на допълнителни изисквания, установени в рамките на европейска схема за сертифициране на киберсигурността, и следва да наблюдават съответните промени в областта на сертифицирането на киберсигурността. Националните органи за сертифициране на киберсигурността следва да разглеждат жалбите, подадени от физически или юридически лица по отношение на европейските сертификати за киберсигурност, издадени от тези органи, или по отношение на европейските сертификати за киберсигурност, издадени от органите за оценяване на съответствието, когато тези сертификати посочват ниво на обезпеченост

„високо“, следва да разследват в необходимата степен предмета на жалбата и следва да информират жалбоподателя за напредъка и резултатите от разследването в разумен срок. Освен това националните органи за сертифициране на киберсигурността следва да си сътрудничат с други национални органи за сертифициране на киберсигурността или други публични органи, включително чрез споделяне на информация за възможни несъответствия на ИКТ продукти, ИКТ услуги и ИКТ процеси с изискванията на настоящия регламент или с конкретни европейски схеми за сертифициране на киберсигурността. Комисията следва да улесни споделянето на информация чрез предоставяне на обща електронна информационна система за подпомагане, например Информационната и комуникационна система за надзор на пазара (ICSMS) и системата за бързо предупреждение за опасни нехранителни продукти (RAPEX), които вече се използват от органите за надзор на пазара съгласно Регламент (ЕО) № 765/2008.

(103) За да се гарантира последователно прилагане на европейската рамка за сертифициране на киберсигурността, следва да се създаде Европейска група за сертифициране на киберсигурността, състояща се от представители на национални органи за сертифициране на киберсигурността или други съответни национални органи. Основните задачи на групата следва да са да съветва и подпомага Комисията при работата ѝ за гарантиране на последователното изпълнение и прилагане на европейската рамка за сертифициране на киберсигурността, да подпомага ENISA и да си сътрудничи тясно с нея при изготвянето на проекти на схеми за сертифициране на киберсигурността, в надлежно обосновани случаи да изиска от ENISA подготовката на проект за схема, както и да приема становища, адресирани до ENISA във връзка с проекти за схеми и становища, адресирани до Комисията относно поддръжката и преразглеждането на съществуващите европейски схеми за сертифициране на киберсигурността. Групата следва да улеснява обмена на добри практики и експертен опит между различните национални органи за сертифициране на киберсигурността, отговарящи за оправомощаването на органите за оценяване на съответствието и издаването на европейски сертификати за киберсигурност.

(104) С цел да се повиши осведомеността и да се улесни приемането на бъдещи европейски схеми за сертифициране на киберсигурността, Комисията може да издава общи или специфични за сектора насоки за киберсигурност, например относно добри практики в областта на киберсигурността или отговорно поведение по отношение на киберсигурността, които да подчертават положителните ефекти от използването на сертифицирани ИКТ продукти, ИКТ услуги и ИКТ процеси.

(105) С цел да се улесни допълнително търговията и като се отчита, че веригите за доставки на ИКТ са глобални, споразуменията за взаимно признаване, отнасящи се до европейските сертификати за киберсигурност, могат да бъдат сключвани от Съюза в съответствие с член 218 от Договора за функционирането на Европейския съюз (ДФЕС). Комисията, като взема предвид консултациите с ENISA и Европейската група за сертифициране на киберсигурността, може да препоръча започване на съответните преговори. Всяка европейска схема за сертифициране на киберсигурността следва да предвижда специфични условия за такива споразумения за взаимно признаване с трети страни.

(106) За да се гарантират еднакви условия за прилагане на настоящия регламент, на Комисията следва да се предоставят изпълнителни правомощия. Тези правомощия следва да се упражняват в съответствие с Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета ([22]).

(107) За приемането на актове за изпълнение относно европейските схеми за сертифициране на киберсигурността на ИКТ продукти, ИКТ услуги или ИКТ процеси, за приемането на актове за изпълнение относно провеждането на разследвания от страна на ENISA, за приемането на актове за изпълнение относно план за партньорски проверки на националните органи за сертифициране на киберсигурността, както и за приемането на актове за изпълнение относно обстоятелствата, форматите и процедурите за уведомяване на Комисията относно органите за оценяване на съответствието от националните органи за сертифициране на киберсигурността, следва да се използва процедурата по разглеждане.

(108) Дейностите на ENISA следва да бъдат оценявани редовно и от независим орган. При оценката следва да се имат предвид целите на ENISA, нейните работни практики и значимостта на задачите ѝ, в частност нейните задачи във връзка с оперативното сътрудничество на равнището на Съюза. В оценката следва също така да се разглеждат въздействието, ефективността и ефикасността на европейската рамка за сертифициране на киберсигурността. В случай на проверка Комисията следва да оценява по какъв начин може да бъде утвърдена ролята на ENISA на отправна точка за консултации и експертен опит и също следва да направи оценка на възможността за роля на ENISA в подпомагането на оценяването на ИКТ продуктите, ИКТ услугите и ИКТ процесите от трети държави, които не отговарят на правилата на Съюза, когато такива продукти, услуги и процеси навлизат в Съюза.

([22]) Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета от 16 февруари 2011 г. за установяване на общите правила и принципи относно реда и условията за контрол от страна на държавите-членки върху упражняването на изпълнителните правомощия от страна на Комисията (ОВ L 55, 28.2.2011 г., стр. 13).

(109) Тъй като целите на настоящия регламент не могат да бъдат постигнати в достатъчна степен от държавите членки, а поради обхвата и последиците му могат да бъдат постигнати по-добре на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от Договора за Европейския съюз (ДЕС). В съответствие с принципа на пропорционалност, както е определено в споменатия член, настоящият регламент не надхвърля необходимото за постигането на тези цели.

(110) Регламент (ЕС) № 526/2013 следва да бъде отменен,

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

ДЯЛ I

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет и обхват

1. С оглед да се гарантира правилното функциониране на вътрешния пазар, като същевременно се постигне висока степен на киберсигурност, киберустойчивост и доверие в киберпространството в рамките на Съюза, с настоящия регламент:

а) се определят целите, задачите и организационните аспекти на ENISA (Агенцията на Европейския съюз за киберсигурност); и

б) се определя рамка за създаването на европейски схеми за сертифициране на киберсигурността с цел да се гарантира подходящо ниво на киберсигурност за ИКТ продукти, ИКТ услуги и ИКТ процеси в Съюза, както и с цел да се избегне разпокъсаност на вътрешния пазар по отношение на схемите за сертифициране на киберсигурността в Съюза.

Посочената в първа алинея, буква б) рамка се прилага, без да се засягат специфичните разпоредби в останалите правни актове на Съюза за доброволното или задължителното сертифициране.

2. Настоящият регламент не засяга компетентността на държавите членки по отношение на дейностите, свързани с обществената сигурност, отбраната, националната сигурност и дейностите на държавата в областта на наказателното право.

Член 2

Определения

За целите на настоящия регламент се прилагат следните определения:

1) „киберсигурност“ означава дейностите, необходими за защита от киберзаплахи на мрежите и информационните системи, на ползвателите на такива мрежи и системи и други лица, засегнати от киберзаплахи;

2) „мрежа и информационна система“ означава мрежа и информационна система съгласно определението в член 4, точка 1 от Директива (ЕС) 2016/1148;

3) „национална стратегия относно сигурността на мрежите и информационните системи“ означава национална стратегия относно сигурността на мрежите и информационните системи съгласно определението в член 4, точка 3 от Директива (ЕС) 2016/1148;

4) „оператор на основни услуги“ означава оператор на основни услуги съгласно определението в член 4, точка 4 от Директива (ЕС) 2016/1148;

5) „доставчик на цифрови услуги“ означава доставчик на цифрова услуга съгласно определението в член 4, точка 6 от Директива (ЕС) 2016/1148;

6) „инцидент“ означава инцидент съгласно определението в член 4, точка 7 от Директива (ЕС) 2016/1148;

7) „действия при инцидент“ означава действия при инцидент съгласно определението в член 4, точка 8 от Директива (ЕС) 2016/1148;

8) „киберзаплаха“ означава всяко потенциално обстоятелство, събитие или действие, което може да навреди, наруши или по друг начин да окаже неблагоприятно въздействие върху мрежите и информационните системи, ползвателите на такива мрежи и системи и други лица;

9) „европейска схема за сертифициране на киберсигурността“ означава определен на равнището на Съюза цялостен набор от правила, технически изисквания, стандарти и процедури, установени на равнище на Съюза и които се прилагат по отношение на сертифицирането или оценката на съответствието на специфични ИКТ продукти, ИКТ услуги или ИКТ процеси;

10) „национална схема за сертифициране на киберсигурността“ означава цялостен набор от правила, технически изисквания, стандарти и процедури, разработени и приети от национален публичен орган и които се прилагат по отношение на сертифицирането или оценката на съответствието на ИКТ продукти, ИКТ услуги и ИКТ процеси, попадащи в обхвата на конкретната схема;

11) „европейски сертификат за киберсигурност“ означава издаден от съответния орган документ, удостоверяващ, че за даден ИКТ продукт, ИКТ услуга или ИКТ процес е извършена оценка за съответствие спрямо специфичните изисквания за сигурност, определени в дадена европейска схема за сертифициране на киберсигурността;

12) „ИКТ продукт“ означава елемент или група елементи на мрежа или на информационна система;

13) „ИКТ услуга“ означава услуга, състояща се в изцяло или главно в предаване, съхранение, извличане или обработка на информация посредством мрежи и информационни системи;

14) „ИКТ процес“ означава набор от дейности, извършвани с цел проектиране, разработване, предоставяне или поддържане на ИКТ продукт или ИКТ услуга;

15) „акредитация“ означава акредитация съгласно определението в член 2, точка 10 от Регламент (ЕО) № 765/2008;

16) „национален орган по акредитация“ означава национален орган по акредитация съгласно определението в член 2, точка 11 от Регламент (ЕО) № 765/2008;

17) „оценяване на съответствието“ означава оценяване на съответствието съгласно определението в член 2, точка 12 от Регламент (ЕО) № 765/2008;

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

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

20) „техническа спецификация“ означава документ, определящ техническите изисквания, които трябва да бъдат изпълнени от ИКТ продукт, ИКТ услуга или ИКТ процес, или процедурите за оценяване на съответствието, свързани с ИКТ продукт, ИКТ услуга или ИКТ процес;

21) „ниво на увереност“ означава основа за увереност, че даден ИКТ продукт, ИКТ услуга или ИКТ процес отговаря на изискванията за сигурност на конкретна европейска схема за сертифициране на киберсигурността, посочва на кое ниво ИКТ продуктът, ИКТ услугата или ИКТ процесът е оценен, но само по себе си не измерва сигурността на съответния ИКТ продукт, ИКТ услуга или ИКТ процес;

22) „самооценяване на съответствието“ означава действие, извършвано от производител или доставчик на ИКТ продукти, ИКТ услуги или ИКТ процеси, с което се оценява дали тези ИКТ продукти, ИКТ услуги или ИКТ процеси отговарят на изискванията на конкретна европейска схема за сертифициране на киберсигурността.

ДЯЛ II

ENISA (АГЕНЦИЯТА НА ЕВРОПЕЙСКИЯ СЪЮЗ ЗА КИБЕРСИГУРНОСТ)

ГЛАВА I

Мандат и цели

Член 3

Мандат

1. ENISA поема задачите, възложени ѝ с настоящия регламент, насочени към постигането на високо общо равнище на киберсигурност в целия Съюз, включително чрез активна подкрепа за държавите членки, институциите, органите, службите и агенциите на Съюза за подобряване на киберсигурността. ENISA служи като референтно звено за консултации и експертен опит по киберсигурността за институциите, органите, службите и агенциите на Съюза, както и за останалите заинтересовани страни в Съюза.

Като изпълнява задачите, възложени ѝ с настоящия регламент, ENISA допринася за намаляване на разпокъсаността на вътрешния пазар.

2. ENISA изпълнява задачите, възложени ѝ чрез правни актове на Съюза, с които се определят мерки за сближаване на свързаните с киберсигурността законови, подзаконови и административни разпоредби на държавите членки.

3. При изпълнението на задачите си ENISA действа като независима, като избягва дублиране с дейностите на държавите членки и като отчита съществуващия експертен опит на държавите членки.

4. ENISA развива своите собствени ресурси, включително технически и човешки способности и умения, необходими за изпълнението на задачите, възложени ѝ с настоящия регламент.

Член 4

Цели

1. ENISA функционира като експертен център по въпросите на киберсигурността на основата на своята независимост, научното и техническо качество на предоставяните консултации и помощ, предлаганата от нея информация, прозрачността на процедурите ѝ за действие, методите ѝ на работа, както и на добросъвестното изпълнение на възложените ѝ задачи.

2. ENISA подпомага институциите, органите, службите и агенциите на Съюза, както и държавите членки, при разработването и прилагането на политиките на Съюза, свързани с киберсигурността, включително секторните политики в областта на киберсигурността.

3. ENISA подпомага изграждането на капацитет и подготвеността в целия Съюз, като съдейства на институциите, органите, службите и агенциите на Съюза, както и на държавите членки и заинтересованите страни от публичния и частния сектор, с цел засилване на защитата на техните мрежи и информационни системи, развитие и подобряване на киберустойчивостта и капацитета за реагиране и развиване на уменията и знанията в областта на киберсигурността.

4. ENISA насърчава сътрудничеството, включително обмена на информация, и координацията на равнището на Съюза между държавите членки, институциите, органите, службите и агенциите на Съюза и съответните заинтересовани страни от публичния и частния сектор по въпросите на киберсигурността.

5. ENISA допринася за повишаването на способностите в областта на киберсигурността на равнището на Съюза, за да подкрепя действията на държавите членки за предотвратяване на киберзаплахи и реакцията спрямо тях, по-специално в случаи на трансгранични инциденти.

6. ENISA насърчава използването на европейското сертифициране с оглед на избягването на разпокъсаността на вътрешния пазар. ENISA допринася за създаването и поддържането на европейската рамка за сертифициране на киберсигурността съгласно дял III от настоящия регламент, с цел постигане на повече прозрачност в увереността за киберсигурността на ИКТ продукти, ИКТ услуги и ИКТ процеси като по този начин се укрепва доверието в цифровия вътрешен пазар и неговата конкурентоспособност.

7. ENISA насърчава високото равнище на осведоменост за киберсигурността, включително киберхигиената и киберграмотността сред гражданите, организациите и предприятията.

ГЛАВА II

Задачи

Член 5

Разработване и прилагане на политиката и правото на Съюза

ENISA допринася за разработването и прилагането на политиката и правото на Съюза, като:

1) подпомага и консултира относно разработването и прегледа на политиката и правото на Съюза в областта на киберсигурността и по специфични за сектора политически и законодателни инициативи, засягащи въпросите на киберсигурността, особено посредством представянето на независими становища и анализи, както и извършването на подготвителна работа;

2) подпомага държавите членки в последователното прилагане на политиката и правото на Съюза по отношение на киберсигурността, по-специално във връзка с Директива (ЕС) 2016/1148, включително посредством становища, насоки, консултации и споделяне на най-добри практики по въпроси като управление на риска, докладване на инциденти и обмен на информация, както и посредством улесняване на обмена на най-добри практики между компетентните органи в това отношение;

3) подпомага държавите членки и институциите, органите, службите и агенциите на Съюза при разработването и насърчаването на политики за киберсигурност, свързани с поддържането на общата наличност или целостта на обществото ядро на отворения интернет;

4) дава своя принос за работата на групата за сътрудничество съгласно член 11 от Директива (ЕС) 2016/1148 чрез предоставяне на експертен опит и помощ;

5) подпомага:

   а) разработването и прилагането на политиката на Съюза в областта на електронната идентичност и удостоверителните услуги, по-специално чрез предоставяне на консултации и технически насоки, както и чрез улесняване на обмена на най-добри практики между компетентните органи;

   б) насърчаването на повишено равнище на сигурност на електронните съобщения, включително чрез предоставяне на консултации и експертен опит, както и чрез подпомагане на обмена на най-добри практики между компетентните органи;

   в) държавите членки при изпълнението на свързаните с киберсигурността специфични аспекти на политиката и правото на Съюза, отнасящи се до защитата на данните и неприкосновеността на личния живот, включително, при поискване, чрез предоставяне на становища на Европейския комитет по защита на данните;

6) подпомага редовното преразглеждане на дейностите по политиката на Съюза чрез изготвяне на годишен доклад за напредъка по прилагането на съответната нормативна уредба относно:

   а) информацията за уведомленията за инциденти в държавите членки, предоставена от единните звена за контакт на групата за сътрудничество съгласно член 10, параграф 3 от Директива (ЕС) 2016/1148;

   б) обобщения на докладването пред ENISA от страна на надзорните органи за пробиви в сигурността или целостта на системите, получено от доставчиците на удостоверителни услуги, както е предвидено в член 19, параграф 3 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета ([23]);

   в) докладването на инциденти, свързани със сигурността, осъществено от доставчиците на обществени електронни съобщителни мрежи или на обществено достъпни електронни съобщителни услуги и предоставяно на ENISA от компетентните органи съгласно член 40 от Директивата (ЕС) 2018/1972.

([23]) 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).

Член 6

Изграждане на капацитет

1. ENISA съдейства:

а) на държавите членки в усилията им да подобрят предотвратяването, откриването, анализа и способността за реагиране на киберзаплахи и киберинциденти, като им предоставя знания и експертен опит;

б) на държавите членки и институциите, органите, службите и агенциите на Съюза при разработването и прилагането на политиките за оповестяване на уязвимостта на доброволна основа;

в) на институциите, органите, службите и агенциите на Съюза в усилията им да подобрят предотвратяването, установяването, анализа и способностите си за реагиране на киберзаплахи и киберинциденти, по-специално чрез целесъобразна подкрепа за CERT-EU;

г) на държавите членки, по тяхна молба, за създаване на национални CSIRT, съгласно член 9, параграф 5 от Директива (ЕС) 2016/1148;

д) на държавите членки, по тяхна молба, за разработване на национални стратегии относно мрежите и информационните системи съгласно член 7, параграф 2 от Директива (ЕС) 2016/1148 и насърчава разпространението на тези стратегии, както и отбелязва напредъка при изпълнението им в рамките на Съюза, за да популяризира добрите практики;

е) на институциите на Съюза при изготвянето и прегледа на стратегиите на Съюза за киберсигурността, като насърчава тяхното разпространение и проследява напредъка в изпълнението им;

ж) на националните CSIRT и CSIRT на Съюза, като увеличава техните способности, включително чрез насърчаване на диалога и обмена на информация, за да гарантира, че всеки CSIRT отговаря на общ набор от минимални способности и работи в съответствие с най-добрите практики съобразно актуалните технологични постижения;

з) на държавите членки чрез редовното организиране най-малко на всеки две години на посочените в член 7, параграф 5 учения в областта на киберсигурността на равнището на Съюза, и чрез препоръки за политиката въз основа на процеса на оценка на ученията и направените от тях изводи;

и) на съответните публични органи чрез предлагане на обучения по киберсигурност, по целесъобразност съвместно със заинтересованите страни;

й) на групата за сътрудничество при обмена на най-добри практики, по-специално относно определянето от държавите членки на оператори на основни услуги, съгласно член 11, параграф 3, буква л) от Директива (ЕС) 2016/1148, включително по отношение на трансграничните зависимости във връзка с рисковете и инцидентите.

2. ENISA подпомага обмена на информация в секторите и между тях, по-специално в секторите, изброени в приложение II към Директива (ЕС) 2016/1148, като предоставя становища относно най-добри практики и насоки относно наличните инструменти и процедури, както и относно начините за преодоляване на нормативните проблеми във връзка с обмена на информация.

Член 7

Оперативно сътрудничество на равнището на Съюза

1. ENISA подпомага оперативното сътрудничество между държавите членки, институциите, органите, службите и агенциите на Съюза и между заинтересованите страни.

2. ENISA съдейства на оперативно ниво и създава синергии с институциите, органите, службите и агенциите на Съюза, включително CERT-EU, със службите, работещи в областта на киберпрестъпността и с надзорните органи за защита на неприкосновеността на личния живот и на личните данни, с оглед решаване на въпроси от общ интерес, включително посредством:

а) обмен на ноу-хау и най-добри практики;

б) предоставяне на консултации и насоки по актуални въпроси, свързани с киберсигурността;

в) определяне след консултация с Комисията на практически договорености за изпълнението на конкретни задачи.

3. ENISA осигурява секретариата на мрежата на CSIRT съгласно член 12, параграф 2 от Директива (ЕС) 2016/1148 и в това си качество активно подкрепя обмена на информация и сътрудничеството между нейните членове.

4. ENISA оказва подкрепа на държавите членки в оперативното сътрудничество в рамките на мрежата на CSIRT чрез:

а) консултации за подобряване на способностите им за предотвратяване, откриване и реагиране на инциденти, и по искане на една или повече държави членки — чрез предоставяне на съвети във връзка с конкретна киберзаплаха;

б) помощ, по искане на една или повече държави членки, при оценката на инциденти със значително или съществено въздействие, като предоставя експертен опит и улеснява техническата работа по такива инциденти, включително по-специално като подкрепя доброволния обмен на важна информация и технически решения между държавите членки;

в) анализ на уязвимостите и на инциденти въз основа на публично достъпна информация или информация, предоставена доброволно за тази цел от държавите членки; и

г) по искане на една или повече държави членки, оказване на подкрепа във връзка с последващи технически разследвания на инциденти със значително или съществено въздействие по смисъла на Директива (ЕС) 2016/1148.

При изпълнението на тези задачи ENISA и CERT-EU си сътрудничат структурирано, за да се възползват от синергии и да избегнат дублирането на дейности.

5. ENISA организира редовни учения в областта на киберсигурността на равнището на Съюза и подпомага държавите членки и институциите, органите, службите и агенциите на Съюза, като организира учения в областта на киберсигурността по тяхно искане. Ученията в областта на киберсигурността на равнището на Съюза могат да включват технически, оперативни или стратегически елементи. Веднъж на всеки две години ENISA организира широкомащабно всеобхватно учение.

По целесъобразност ENISA също така участва и помага в организирането на секторни учения в областта на киберсигурността заедно със съответните организации, които участват и в учения на равнището на Съюза.

6. ENISA, в тясно сътрудничество с държавите членки, изготвя редовен задълбочен доклад за техническото състояние на киберсигурността на ЕС, който разглежда инциденти и киберзаплахи въз основа на информация от обществено достъпни източници, нейни собствени анализи и доклади, споделяни, наред с останалото, от CSIRT на държавите членки или единните звена за контакт, създадени съгласно Директива (ЕС) 2016/1148, и двете на доброволна основа, ЕС3и CERT-EU.

7. ENISA допринася за разработването на колективна реакция на равнището на Съюза и на равнището на държавите членки на широкомащабни трансгранични инциденти или кризи, свързани с киберсигурността, основно чрез:

а) обобщаване и анализ на доклади от национални източници, които са обществено достъпни или са споделени доброволно с цел да допринесе за общата ситуационна осведоменост;

б) осигуряване на ефективен поток на информация и предоставяне на механизми за ескалация между мрежата на CSIRT и техническите и политическите фактори на равнището на Съюза;

в) улесняване, при поискване, на справянето в технически аспект с такива инциденти или кризи, включително по-специално чрез подпомагане на доброволното споделяне на технически решения между държавите членки;

г) подпомагане на институциите, органите, службите и агенциите на Съюза и, по тяхно искане - на държавите членки, при комуникацията с обществеността във връзка с такива инциденти или кризи;

д) изпитване на плановете за сътрудничество в отговор на такива инциденти или кризи на равнището на Съюза, а по тяхно искане — подкрепа за държавите членки при изпитването на тези планове на национално равнище.

Член 8

Пазар, сертифициране на киберсигурността и стандартизация

1. ENISA насърчава разработването и изпълнението на политиката на Съюза за сертифициране на киберсигурността на ИКТ продукти, ИКТ услуги и ИКТ процеси, както е предвидено в дял III от настоящия регламент, като:

а) непрекъснато следи събитията в съответните области на стандартизацията и препоръчва подходящи технически спецификации за използване при разработването на европейски схеми за сертифициране на киберсигурността съгласно член 54, параграф 1, буква в), когато такива стандарти не са налични;

б) изготвя проекти за европейски схеми за сертифициране на киберсигурността („проекти за схеми“) на ИКТ продукти, ИКТ услуги и ИКТ процеси в съответствие с член 49;

в) оценява приетите европейски схеми за сертифициране на киберсигурността в съответствие с член 49, параграф 8;

г) участва в партньорски проверки съгласно член 59, параграф 4;

д) съдейства на Комисията като осигурява секретариата на Европейската група за сертифициране на киберсигурността съгласно член 62, параграф 5.

2. ENISA осигурява секретариата на Европейската група за сертифициране на киберсигурността съгласно член 22, параграф 4;

3. ENISA съставя и публикува насоки и разработва добри практики относно изискванията за киберсигурност за ИКТ продукти, ИКТ услуги и ИКТ процеси в сътрудничество с националните органи по сертифицирането на киберсигурността и с отрасъла по формален, структуриран и прозрачен начин;

4. ENISA допринася за изграждане на капацитет, свързан с процесите на оценяване и сертифициране, чрез съставяне и издаване на насоки, както и чрез оказване на помощ на държавите членки по тяхно искане.

5. ENISA улеснява въвеждането и използването на европейски и международни стандарти за управление на риска и за сигурността на ИКТ продукти, ИКТ услуги и ИКТ процеси.

6. ENISA, в сътрудничество с държавите членки и с отрасъла, съставя препоръки и насоки по отношение на техническите области, свързани с изискванията за сигурност за операторите на основни услуги и доставчиците на цифрови услуги, както и по отношение на вече съществуващите стандарти, включително националните стандарти на държавите членки, съгласно член 19, параграф 2 от Директива (ЕС) 2016/1148.

7. ENISA извършва и разпространява редовни анализи на основните тенденции на пазара на киберсигурността по отношение както на търсенето, така и на предлагането, с оглед развитието на пазара за киберсигурност в Съюза.

Член 9

Знания и информация

ENISA:

а) анализира нововъзникващите технологии и предоставя тематично ориентирани оценки за очакваните социални, правни, икономически и регулаторни въздействия на технологичните нововъведения върху киберсигурността;

б) извършва дългосрочни стратегически анализи на киберзаплахите и киберинцидентите, за да открие възникващи тенденции и да спомогне за предотвратяване на инциденти;

в) в сътрудничество с експерти от органите на държавите членки и съответните заинтересовани страни предоставя консултации, насоки и най-добри практики за сигурността на мрежите и информационните системи, по-специално за сигурността на инфраструктурите, поддържащи изброените в приложение II към Директива (ЕС) 2016/1148 сектори, и инфраструктурите, използвани от доставчици на цифровите услуги, изброени в приложение III към същата директива;

г) събира, организира и предоставя на разположение на обществеността чрез специален портал информация относно киберсигурността, осигурена от институциите, органите, службите и агенциите на Съюза и информация относно киберсигурността, предоставена на доброволна основа от държавите членки и заинтересованите страни от частния и публичния сектор;

д) събира и анализира обществено достъпна информация за значителни инциденти и съставя доклади с цел предоставяне на насоки на гражданите, организациите и предприятията в целия Съюз.

Член 10

Повишаване на осведомеността и образование

ENISA:

а) повишава обществената осведоменост относно рисковете, свързани с киберсигурността и предоставя насоки относно добрите практики за отделни ползватели, насочени към гражданите, организациите и предприятията, включително по отношение на киберхигиената и киберграмотността;

б) в сътрудничество с държавите членки, институциите, органите, службите и агенциите на Съюза, и с отрасъла, организира редовни информационни кампании за повишаване на киберсигурността и нейната видимост в Съюза и насърчава широк обществен дебат;

в) подпомага държавите членки в усилията им за повишаване на осведомеността относно киберсигурността и насърчава образованието в областта на киберсигурността;

г) подкрепя по-тясното координиране и обмена на добри практики между държавите членки във връзка с осведомеността и образованието в областта на киберсигурността.

Член 11

Научни изследвания и иновации

Във връзка с научните изследвания и иновациите, ENISA:

а) консултира институциите, органите, службите и агенциите на Съюза и държавите членки относно нуждата от научни изследвания в областта на киберсигурността, с което съдейства за ефективна реакция на настоящите и нововъзникващите рискове и киберзаплахи, включително за нови и нововъзникващи информационни и комуникационни технологии, както и за ефективното използване на технологиите за предотвратяване на риска;

б) участва, съобразно предоставени ѝ от Комисията правомощия, като изпълнител на програми за финансиране на научните изследвания и иновациите или като бенефициент.

в) дава принос към стратегическата програма за научни изследвания и иновации на равнището на Съюза в областта на киберсигурността.

Член 12

Международно сътрудничество

ENISA дава своя принос към усилията на Съюза за сътрудничество с трети държави и международни организации, както и в контекста на съответните рамки за международно сътрудничество, с оглед на насърчаването на международното сътрудничество в областта на киберсигурността, като:

а) участва по целесъобразност като наблюдател при организирането на международни учения, анализира и докладва на управителния съвет резултатите от тези учения;

б) по искане на Комисията улеснява обмена на добри практики;

в) по искане на Комисията ѝ предоставя експертен опит;

г) предоставя консултации и подкрепа на Комисията по въпроси, свързани с договори за взаимно признаване на сертификати за киберсигурност с трети държави, в сътрудничество с Европейската група за сертифициране на киберсигурността, създадена съгласно член 62.

ГЛАВА III

Организация на ENISA

Член 13

Структура на ENISA

Административната и управленска структура на ENISA се състои от:

а) управителен съвет;

б) изпълнителен съвет;

в) изпълнителен директор;

г) консултативна група на ENISA.

д) мрежа на националните служители за връзка.

Раздел 1

Управителен съвет

Член 14

Състав на управителния съвет

1. Управителният съвет се състои от един член, назначен от всяка държава членка и двама членове, назначени от Комисията. Всички членове имат право на глас.

2. Всеки член на управителния съвет има заместник. При отсъствие на члена, заместникът го представлява.

3. Членовете на управителния съвет и техните заместници се назначават въз основа на познанията им в областта на киберсигурността, като се вземат предвид съответните им умения в областта на управлението, администрацията и бюджетирането. Комисията и държавите членки полагат усилия за ограничаване на текучеството на своите представители в управителния съвет, за да се осигури непрекъснатост на работата на управителния съвет. Комисията и държавите членки се стремят към постигането на баланс между половете в управителния съвет.

4. Мандатът на членовете на управителния съвет и на техните заместници е четири години. Този мандат подлежи на подновяване.

Член 15

Функции на управителния съвет

1. Управителният съвет:

а) определя общата насока на дейността на ENISA и гарантира, че ENISA работи в съответствие с правилата и принципите, заложени в настоящия регламент; също така гарантира съгласуваността на работата на ENISA с дейностите, осъществявани от държавите членки, както и на равнището на Европейския съюз;

б) приема проекта на ENISA за единен програмен документ, посочен в член 24, преди представянето му на Комисията за становище;

в) приема, като взема предвид становището на Комисията, единния програмен документ на ENISA;

г) упражнява надзор върху изпълнението на многогодишните и годишните програми, включени в единния програмен документ;

д) приема годишния бюджет на ENISA и упражнява други функции във връзка с бюджета на ENISA в съответствие с глава IV;

е) оценява и приема консолидирания годишен доклад за дейностите на ENISA, включително отчетите и описание как ENISA е изпълнила своите показатели за изпълнение, изпраща доклада и неговата оценка най-късно до 1 юли на следващата година на Европейския парламент, Съвета, Комисията и Сметната палата и осигурява публичен достъп до годишния доклад;

ж) приема финансовите правила, приложими за ENISA, в съответствие с член 32;

з) приема стратегия за борба с измамите, пропорционална на риска от измами, като взема предвид анализа на разходите и ползите от действията, които следва да бъдат предприети;

и) приема правила за предотвратяване и управление на конфликти на интереси по отношение на своите членове;

й) осигурява подходящи последващи действия във връзка с констатациите и препоръките, произтичащи от разследвания на Европейската служба за борба с измамите (OLAF) и на различни вътрешни или външни одитни доклади и оценки;

к) приема своя процедурен правилник, включително правила за временни решения относно делегирането на специфични задачи съгласно член 19, параграф 7;

л) в съответствие с параграф 2 от настоящия член упражнява по отношение на персонала на ENISA правомощията, предоставени съгласно Правилника за длъжностните лица („Правилник за длъжностните лица“) и Условията за работа на другите служители на Европейския съюз („Условия за работа на другите служители“) и посочени в Регламент (ЕИО, Евратом, ЕОВС) № 259/68 ([24]), на органа по назначаването и на органа, оправомощен да сключва трудови договори („правомощия на органа по назначаването“);

м) приема правила за прилагане на Правилника за длъжностните лица и Условията за работа на другите служители в съответствие с процедурата, предвидена в член 110 от Правилника за длъжностните лица;

н) назначава изпълнителния директор и при необходимост удължава срока на мандата му или го отстранява от длъжност в съответствие с член 36;

о) назначава счетоводител, който може да бъде счетоводителят на Комисията и който се ползва с пълна независимост при изпълнението на своите задължения;

п) взема всички решения относно създаването на вътрешните структури на ENISA и при необходимост относно изменението на тези вътрешни структури, като взема под внимание нуждите за дейността на ENISA, както и доброто бюджетно управление;

р) разрешава установяването на работни договорености с оглед на член 7;

с) разрешава установяването и сключването на работни договорености в съответствие с член 42.

2. Управителният съвет, в съответствие с член 110 от Правилника за длъжностните лица, приема на основание член 2, параграф 1 от същия правилник и член 6 от Условията за работа на другите служители решение за делегиране на съответните правомощия на орган по назначаването на изпълнителния директор и за определяне на условията, при които делегираните правомощия могат да бъдат оттеглени. Изпълнителният директор има правото от своя страна да делегира тези правомощия на други лица.

([24]) ОВ L 56, 4.3.1968 г., стр. 1.

3. Когато изключителни обстоятелства налагат това, управителният съвет може да приеме решение за временно оттегляне на правомощията на орган по назначаването, делегирани на изпълнителния директор, както и на всички правомощия на орган по назначаването, които изпълнителният директор е делегирал на други лица, и да ги упражнява пряко или да ги делегира на някой от членовете си или на друг служител, различен от изпълнителния директор.

Член 16

Председател на управителния съвет

Управителният съвет избира с мнозинство от две трети от членовете си свой председател и заместник-председател измежду членовете си. Техният мандат е за четири години, като този срок може да бъде подновяван еднократно. Ако обаче по време на мандата им те престанат да бъдат членове на управителния съвет, мандатът изтича автоматично на същата дата. Заместник-председателят замества служебно председателя, ако председателят не е в състояние да изпълнява своите задължения.

Член 17

Заседания на управителния съвет

1. Заседанията на управителния съвет се свикват от неговия председател.

2. Управителният съвет провежда най-малко две редовни заседания годишно. Той провежда и извънредни заседания по искане на председателя си, на Комисията или на най-малко една трета от членовете си.

3. Изпълнителният директор взема участие в събранията на управителния съвет без право на глас.

4. По покана на председателя членове на Консултативната група на ENISA могат да участват в заседанията на управителния съвет без право на глас.

5. По време на заседанията на управителния съвет членовете на управителния съвет и техните заместници могат да бъдат подпомагани от съветници или експерти при спазване на правилника за дейността на управителния съвет.

6. ENISA осигурява секретариата на управителния съвет.

Член 18

Правила за гласуване в управителния съвет

1. Управителният съвет взема решенията си с мнозинство на своите членове.

2. Мнозинство от две трети от членовете на управителния съвет се изисква за приемане на единния програмен документ и на годишния бюджет, както и за назначаването, удължаването на мандата или освобождаването от длъжност на изпълнителния директор.

3. Всеки член има един глас. При отсъствие на даден член неговият заместник упражнява правото на глас на члена.

4. Председателят на управителния съвет участва в гласуването.

5. Изпълнителният директор не участва в гласуването.

6. Правилникът за дейността на управителния съвет определя по-подробно условията и реда за гласуване, по-специално условията, при които даден член може да действа от името на друг член.

Раздел 2

Изпълнителен съвет

Член 19

Изпълнителен съвет

1. Управителният съвет се подпомага от изпълнителен съвет.

2. Изпълнителният съвет:

а) подготвя решенията, които трябва да бъдат приети от управителния съвет;

б) заедно с управителния съвет осигурява подходящи мерки за съобразяване с резултатите и препоръките от разследванията на OLAF и различните вътрешни и външни одитни доклади и оценки;

в) без да се засягат отговорностите на изпълнителния директор, определени в член 20, подпомага и съветва изпълнителния директор при изпълнението на решенията на управителния съвет по административни и бюджетни въпроси съгласно член 20.

3. Изпълнителният съвет се състои от петима членове. Членовете на изпълнителния съвет се назначават измежду членовете на управителния съвет. Един от членовете е председателят на управителния съвет, който може също така да бъде председател на изпълнителния съвет, а друг от тях е един от представителите на Комисията. С назначаванията на членовете на изпълнителния съвет се цели постигане на баланс между половете в състава на изпълнителния съвет. Изпълнителният директор взима участие в заседанията на изпълнителния съвет, но няма право на глас.

4. Мандатът на членовете на изпълнителния съвет е четири години. Този мандат подлежи на подновяване.

5. Изпълнителният съвет заседава най-малко веднъж на всеки три месеца. Председателят на изпълнителния съвет свиква допълнителни заседания по искане на членовете на съвета.

6. Управителният съвет установява правилника за дейността на изпълнителния съвет.

7. Когато е необходимо при спешни случаи, изпълнителният съвет може да приема временни решения от името на управителния съвет, особено по въпроси на административното управление, включително за оттегляне на делегираните правомощия на орган по назначаването и в областта на бюджета. Такива временни решения се съобщават без излишно забавяне на управителния съвет. Управителният съвет решава дали да одобри или да отхвърли временното решение не по-късно от три месеца след неговото вземане. Изпълнителният съвет не взема решения от името на управителния съвет, които изискват мнозинство от две трети от членовете на управителния съвет.

Раздел 3

Изпълнителен директор

Член 20

Отговорности на изпълнителния директор

1. ENISA се ръководи от изпълнителен директор, който е независим при изпълнението на своите задължения. Изпълнителният директор се отчита на управителния съвет.

2. Изпълнителният директор докладва на Европейския парламент относно изпълнението на своите задължения, когато бъде поканен да направи това. Съветът може да покани изпълнителния директор да докладва за изпълнението на своите задължения.

3. Изпълнителният директор отговаря за:

а) текущото управление на ENISA;

б) изпълнението на решенията, приети от управителния съвет;

в) изготвянето на проекта на единния програмен документ и предаването му на управителния съвет за одобрение преди представянето му на Комисията;

г) изпълнението на единния програмен документ и докладването пред управителния съвет за неговото изпълнение;

д) изготвянето на консолидирания годишен доклад за дейностите на ENISA, включително изпълнението на годишната работна програма на ENISA, и представянето му на управителния съвет за оценка и приемане;

е) изготвянето на план за действие за съобразяване със заключенията от оценки за изминал период, и докладване за напредъка на всеки две години пред Комисията;

ж) изготвянето на план за действие за съобразяване със заключенията от вътрешните или външните одитни доклади и оценки, както и от разследвания на OLAF и представянето на доклади за напредъка два пъти годишно на Комисията и редовно на управителния съвет;

з) изготвя проект за финансовите правила, приложими за ENISA, съгласно посоченото в член 32;

и) изготвянето на проекта на декларация за разчета на приходите и разходите на ENISA и изпълнението на нейния бюджет;

й) защитата на финансовите интереси на Съюза чрез прилагането на превантивни мерки срещу измами, корупция и всякакви други незаконни дейности, посредством ефективни проверки и, при наличие на нередности, чрез събирането на недължимо платените суми, а също така, когато това е целесъобразно, чрез ефективни, съразмерни и възпиращи административни и финансови санкции;

к) изготвянето на стратегия на ENISA за борба с измамите и представянето ѝ на управителния съвет за одобрение;

л) установяването и поддържането на контакт с бизнес общността и потребителските организации с цел осигуряване на редовен диалог със съответните заинтересовани страни;

м) редовния обмен на становища и информация с институциите, органите, службите и агенциите на Съюза във връзка с техните дейности, свързани с киберсигурността, така че да се гарантира съгласуваност в разработването и прилагането на политиката на Съюза;

н) изпълнението на други задачи, възложени на изпълнителния директор с настоящия регламент.

4. При необходимост, в рамките на целите и задачите на ENISA, изпълнителният директор може да сформира *ad hoc* работни групи, съставени от експерти, включително от експерти на компетентните органи на държавите членки. Изпълнителният директор информира управителния съвет предварително за това. Процедурите, по-специално относно състава на работните групи, назначаването на експертите от изпълнителния директор и дейността на *ad hoc* работните групи, се определят във вътрешния правилник за дейността на ENISA.

5. Когато е необходимо, за целите на ефективното и ефикасно изпълнение на задачите на ENISA и въз основа на подходящ анализ на разходите и ползите, изпълнителният директор може да вземе решение за установяването на един или повече местни офиси в една или повече държави членки. Преди да вземе решение за установяването на местен офис, изпълнителният директор иска становището на съответните държави членки, включително държавата членка, в която се намира седалището на ENISA, и получава предварителното съгласие на Комисията и управителния съвет. В случаи на несъгласие по време на процеса на консултация между изпълнителния директор и съответните държави членки, въпросът се представя на Съвета за обсъждане. Общият брой на персонала във всички местни офиси е най-малкият възможен и не надвишава 40 % от общия брой на персонала на ENISA в държавата членка, в която се намира седалището на ENISA. Броят на персонала във всеки местен офис не надвишава 10 % от общия брой на персонала на ENISA в държавата членка, в която се намира седалището на ENISA.

В решението за създаване на местен офис се уточнява обхватът на дейностите, които ще се извършват в местния офис, така че да се избегнат ненужни разходи и дублиране на административни функции на ENISA.

Раздел 4

Консултативна група на ENISA, група на заинтересованите страни в областта на сертифицирането на киберсигурността и мрежа на националните служители за връзка

Член 21

Консултативна група на ENISA

1. По предложение на изпълнителния директор управителният съвет учредява по прозрачен начин Консултативната група на ENISA, съставена от доказани експерти, представляващи съответните заинтересовани страни, например отрасъла на ИКТ, доставчиците на обществени електронни съобщителни мрежи или услуги, МСП, операторите на основни услуги, потребителски групи, академични експерти в областта на киберсигурността и представители на компетентните органи, нотифицирани в съответствие с Директива (ЕС) 2018/1972, на европейските организации за стандартизация, както и на правоприлагащите органи и надзорните органи за защита на данните. Управителният съвет се стреми да гарантира подходящ баланс между половете, географски баланс, както и баланс между различните групи заинтересовани страни.

2. Процедурите за Консултативната група на ENISA, и по-специално тези относно нейния състав, относно посоченото в параграф 1 предложение на изпълнителния директор, броя и назначаването на членовете ѝ и дейността на Консултативната група на ENISA, се определят във вътрешния правилник за дейността на ENISA и до тях се осигурява публичен достъп.

3. Консултативната група на ENISA се председателства от изпълнителния директор или лице, определено от изпълнителния директор за всеки конкретен случай.

4. Мандатът на членовете на Консултативната група на ENISA е с продължителност две години и половина. Членовете на управителния съвет не могат да бъдат членове на Консултативната група на ENISA. Експертите на Комисията и от държавите членки имат право да присъстват на заседанията на Консултативната група на ENISA и да участват в нейната работа. Представители на други органи, които не са членове на Консултативната група на ENISA, но които изпълнителният директор счита за подходящи, могат да бъдат канени да присъстват на заседанията на Консултативната група на ENISA и да участват в работата ѝ.

5. Консултативната група на ENISA консултира ENISA при изпълнението на задачите на ENISA, с изключение на прилагането на разпоредбите на дял III от настоящия регламент. По-специално тя консултира изпълнителния директор относно изготвянето на предложение за годишната работна програма на ENISA и гарантирането на диалог със съответните заинтересовани страни по въпроси, свързани с годишната работна програма.

6. Консултативната група на ENISA редовно информира управителния съвет за своята дейност.

Член 22

Група на заинтересованите страни в областта на сертифицирането на киберсигурността

1. Създава се Група на заинтересованите страни в областта на сертифицирането на киберсигурността.

2. Групата на заинтересованите страни в областта на сертифицирането на киберсигурността се състои от членове, избрани измежду признати експерти, представляващи съответните заинтересовани страни. След провеждане на прозрачна и открита процедура Комисията избира членовете на Групата на заинтересованите страни в областта на сертифицирането на киберсигурността по предложение на ENISA, като гарантира баланс между различните групи заинтересовани страни, подходящ баланс между половете и географски баланс.

3. Групата на заинтересованите страни в областта на сертифицирането на киберсигурността:

а) консултира Комисията по стратегически въпроси, свързани с европейската рамка за сертифициране на киберсигурността;

б) при поискване, консултира ENISA по общи и стратегически въпроси, свързани със задачите на ENISA относно пазара, сертифицирането на киберсигурността и стандартизацията;

в) подпомага Комисията в подготовката на непрекъснатата работна програма на Съюза, посочена в член 47;

г) излиза със становища относно непрекъснатата работна програма на Съюза съгласно член 47, параграф 4; и

д) при спешни случаи дава съвети на Комисията и на Европейската група за сертифициране на киберсигурността относно необходимостта от допълнителни схеми за сертифициране, които не са включени в непрекъснатата работна програма на Съюза, съгласно посоченото в членове 47 и 48.

4. Групата на заинтересованите страни в областта на сертифицирането на киберсигурността се председателства съвместно от Комисията и ENISA, а секретариатът ѝ се осигурява от ENISA.

Член 23

Мрежа на националните служители за връзка

1. Управителният съвет, като действа по предложение на изпълнителния директор, създава мрежа на националните служители за връзка, съставена от представители на всички държави членки („национални служители за връзка“). Всяка държава членка посочва по един представител в мрежата на националните служители за връзка. Заседанията на мрежата на националните служители за връзка могат да се провеждат в различни експертни формати.

2. Мрежата на националните служители за връзка по-специално улеснява обмена на информация между ENISA и държавите членки и подкрепя ENISA в разпространението на нейните дейности, констатации и препоръки сред съответните заинтересовани страни в Съюза.

3. Националните служители за връзка действат като звена за контакт на национално равнище с цел улесняване на сътрудничеството между ENISA и националните експерти в контекста на изпълнението на годишната работна програма на ENISA.

4. Макар че националните служители за връзка си сътрудничат тясно с представителите в управителния съвет на съответните си държави членки, мрежата на националните служители за връзка не дублира работата нито на управителния съвет, нито на други форуми на Съюза.

5. Функциите и процедурите на мрежата на националните служители за връзка се определят във вътрешния правилник за дейността на ENISA и до тях се осигурява публичен достъп.

Раздел 5

Дейност

Член 24

Единен програмен документ

1. ENISA осъществява дейността си в съответствие с единен програмен документ, който съдържа нейното годишно и многогодишно програмиране и обхваща всички планирани дейности.

2. Всяка година изпълнителният директор изготвя проект на единен програмен документ, който съдържа годишно и многогодишно програмиране на съответните финансови и човешки ресурси съгласно член 32 от Делегиран регламент (ЕС) № 1271/2013 ([25]) на Комисията, като взема предвид насоките на Комисията.

3. До 30 ноември всяка година управителният съвет приема единния програмен документ, посочен в параграф 1, и го изпраща на Европейския парламент, Съвета и Комисията до 31 януари следващата година, както и всички следващи актуализирани варианти на този документ.

4. Единният програмен документ става окончателен след окончателното приемане на общия бюджет на Съюза и, ако е необходимо, съответно се коригира.

([25]) Делегиран регламент (ЕС) № 1271/2013 на Комисията от 30 септември 2013 г. относно рамковия Финансов регламент за органите, посочени в член 208 от Регламент (ЕС, Евратом) № 966/2012 на Европейския парламент и на Съвета (ОВ L 328, 7.12.2013 г., стр. 42).

5. Годишната работна програма включва подробни цели и очаквани резултати, включително показатели за изпълнение. В нея също така са описани действията, които ще се финансират, и са посочени финансовите и човешките ресурси, разпределени за всяко действие, в съответствие с принципите за бюджетиране и управление по дейности. Годишната работна програма е съгласувана с многогодишната работна програма, посочена в параграф 7. В годишната работна програма се посочват ясно добавените, променените или отменените задачи в сравнение с предходната финансова година.

6. Управителният съвет внася изменения в приетата годишна работна програма, когато на ENISA бъде възложена нова задача. Всяко съществено изменение на годишната работна програма се приема по същата процедура като първоначалната годишна работна програма. Управителният съвет може да делегира правомощието за внасяне на несъществени промени в годишната работна програма на изпълнителния директор.

7. В многогодишната работна програма е определен общият стратегически план, включително целите, очакваните резултати и показателите за изпълнението. В нея се съдържа също програмирането на ресурсите, включително на многогодишния бюджет и персонала.

8. Програмирането на ресурсите се актуализира ежегодно. Стратегическото програмиране се актуализира по целесъобразност, и по-специално в отговор на резултата от оценката, посочена в член 67.

Член 25

Деклариране на интереси

1. Членовете на управителния съвет, изпълнителният директор и длъжностните лица, временно командировани от държавите членки, представят декларация за ангажираност и декларация за липса или наличие на преки или косвени интереси, които биха могли да се считат за накърняващи тяхната независимост. Тези декларации са точни и изчерпателни, правят се писмено всяка година и се актуализират при необходимост.

2. Членовете на управителния съвет, изпълнителният директор и външните експерти, участващи в *ad hoc* работни групи, декларират точно и изчерпателно най-късно в началото на всяко заседание наличието на интереси, които биха могли да се считат за засягащи тяхната независимост по отношение на точките в дневния ред, и се въздържат от участие в обсъждането на тези точки и гласуването по тях.

3. ENISA установява във вътрешния правилник за дейността си практическите ред и условия за прилагане на правилата за деклариране на интереси, посочени в параграфи 1 и 2.

Член 26

Прозрачност

1. ENISA осъществява дейността си при високо ниво на прозрачност и в съответствие с член 28.

2. ENISA гарантира, че на обществеността и на заинтересованите страни се предоставя целесъобразна, обективна, достоверна и леснодостъпна информация, по-специално по отношение на резултатите от нейната дейност. Освен това тя оповестява публично декларациите за интереси, направени в съответствие с член 25.

3. По предложение на изпълнителния директор управителният съвет може да разреши на заинтересовани страни да наблюдават хода на някои от дейностите на ENISA.

4. ENISA установява във вътрешния правилник за дейността си практическите ред и условия за прилагане на правилата на прозрачност, посочени в параграфи 1 и 2.

Член 27

Поверителност

1. Без да се засяга член 28, ENISA няма право да разкрива на трети страни информация, която обработва или получава, за която е отправено обосновано искане за поверително обработване.

2. Членовете на управителния съвет, изпълнителният директор, членовете на Консултативната група на ENISA, участващите в работните *ad hoc* групи външни експерти и членовете на персонала на ENISA, включително временно командированите от държавите членки длъжностни лица, са задължени да спазват изискванията за поверителност съгласно член 339 от ДФЕС, дори и след приключване на службата им.

3. ENISA установява във вътрешния правилник за дейността си практическите ред и условия за прилагане на правилата на поверителност, посочени в параграфи 1 и 2.

4. Ако това се изисква за изпълнението на задачите на ENISA, управителният съвет решава да разреши на ENISA да работи с класифицирана информация. В такъв случай ENISA, със съгласието на службите на Комисията, приема правила за сигурност, като прилага принципите на сигурността, установени в решения (ЕС, Евратом) 2015/443 ([26]) и 2015/444 ([27]) на Комисията. Посочените правила за сигурност включват разпоредби за обмена, обработката и съхранението на класифицирана информация.

Член 28

Достъп до документи

1. Регламент (ЕО) № 1049/2001 се прилага за документи, притежавани от ENISA.

2. Управителният съвет приема реда за прилагането на Регламент (ЕО) № 1049/2001 в срок до 28 декември 2019 г.

3. Срещу решенията, взети от ENISA съгласно член 8 от Регламент (ЕО) № 1049/2001, може да се подава жалба до европейския омбудсман по реда и при условията на член 228 от ДФЕС или те може да се обжалват пред Съда на Европейския съюз по реда и при условията на член 263 от ДФЕС.

ГЛАВА IV

Съставяне и структура на бюджета на ENISA

Член 29

Съставяне на бюджета на ENISA

1. Всяка година изпълнителният директор изготвя проект на разчета за предвидените приходи и разходи на ENISA за следващата финансова година и го изпраща на управителния съвет заедно с проект на щатно разписание. Приходите и разходите са балансирани.

2. Въз основа на проекта на разчета за предвидените средства, управителният съвет ежегодно изготвя разчет за предвидените приходи и разходи на ENISA за следващата финансова година.

3. До 31 януари всяка година управителният съвет изпраща разчета за предвидените средства, който е част от проекта на единен програмен документ, на Комисията и на третите държави, с които Европейският съюз е сключил споразумения, както е посочено в член 42, параграф 2.

4. Въз основа на този разчет Комисията включва в проекта за бюджет на Съюза прогнозните средства, които прецени за необходими за щатното разписание, и размера на вноската, която се заделя от общия бюджет на Съюза, и ги представя на Европейския парламент и на Съвета в съответствие с член 314 от ДФЕС.

5. Европейският парламент и Съветът разрешават отпускане на бюджетни кредити за вноската от Съюза в ENISA.

6. Европейският парламент и Съветът приемат щатното разписание на ENISA.

([26]) Решение (ЕС, Евратом) 2015/443 на Комисията от 13 март 2015 г. относно сигурността в Комисията (ОВ L 72, 17.3.2015 г., стр. 41).
([27]) Решение (ЕС, Евратом) 2015/444 на Комисията от 13 март 2015 г. относно правилата за сигурност за защита на класифицираната информация на ЕС (ОВ L 72, 17.3.2015 г., стр. 53).

7. Заедно с единния програмен документ управителният съвет приема бюджета на ENISA. Бюджетът на ENISA става окончателен след окончателното приемане на общия бюджет на Съюза. Когато е необходимо, управителният съвет коригира бюджета и единния програмен документ на ENISA в съответствие с общия бюджет на Съюза.

Член 30

Структура на бюджета на ENISA

1. Без да се засягат други ресурси, приходите на ENISA включват:

а) вноска от общия бюджет на Съюза;

б) приходи, заделени за финансиране на определени разходи съгласно финансовите правила, посочени в член 32;

в) финансиране от Съюза под формата на споразумения за делегиране или *ad hoc* безвъзмездни средства в съответствие с нейните финансови правила, посочени в член 32, и с разпоредбите на съответните инструменти за подкрепа на политиките на Съюза;

г) вноски от трети държави, участващи в работата на ENISA, както е предвидено в член 42;

д) всякакви доброволни парични или непарични вноски от държавите членки.

Държавите членки, осигуряващи доброволни вноски съгласно първа алинея, точка д), не предявяват претенции за особени права или услуги в резултат от тези вноски.

2. Разходите на ENISA се състоят от разходи за персонал, административна и техническа поддръжка, разходи за инфраструктура и оперативни разходи, както и разходи в резултат от договори с трети страни.

Член 31

Изпълнение на бюджета на ENISA

1. Изпълнителният директор отговаря за изпълнението на бюджета на ENISA.

2. Вътрешният одитен орган на Комисията се ползва със същите правомощия спрямо ENISA като тези спрямо отделите на Комисията.

3. До 1 март на следващата финансова година (година N + 1) счетоводителят на ENISA изпраща междинния счетоводен отчет за финансовата година (година N) на счетоводителя на Комисията и на Сметната палата.

4. След като получи забележките на Сметната палата по междинния счетоводен отчет на ENISA съгласно член 246 от Регламент (ЕС, Евратом) 2018/1046 на Европейския парламент и на Съвета ([28]), счетоводителят на ENISA изготвя под своя отговорност нейния окончателен счетоводен отчет и го изпраща на управителния съвет за становище.

5. Управителният съвет дава становище относно окончателния счетоводен отчет на ENISA.

6. До 31 март на година N + 1, изпълнителният директор изпраща доклада за бюджетното и финансовото управление до Европейския парламент, Съвета, Комисията и Сметната палата.

7. До 1 юли на година N + 1 счетоводителят на ENISA изпраща окончателния счетоводен отчет на ENISA заедно със становището на управителния съвет до Европейския парламент, Съвета, счетоводителя на Комисията и до Сметната палата.

([28]) Регламент (ЕС, Евратом) 2018/1046 на Европейския парламент и на Съвета от 18 юли 2018 г. за финансовите правила, приложими за общия бюджет на Съюза, за изменение на регламенти (ЕС) № 1296/2013, (ЕС) № 1301/2013, (ЕС) № 1303/2013, (ЕС) № 1304/2013, (ЕС) № 1309/2013, (ЕС) № 1316/2013, (ЕС) № 223/2014 и (ЕС) № 283/2014 и на Решение № 541/2014/ЕС и за отмяна на Регламент (ЕС, Евратом) № 966/2012 (ОВ L 193, 30.7.2018 г., стр. 1).

8. В деня на предаване на окончателния счетоводен отчет на ENISA счетоводителят на ENISA също така изпраща на Сметната палата представително писмо относно този окончателен отчет с копие до счетоводителя на Комисията.

9. До 15 ноември на година N + 1 изпълнителният директор публикува окончателния счетоводен отчет на ENISA в *Официален вестник на Европейския съюз*.

10. До 30 септември на година N + 1 изпълнителният директор изпраща на Сметната палата отговор на нейните констатации, с копие до управителния съвет и Комисията.

11. Изпълнителният директор представя на Европейския парламент по искане на последния всякаква информация, необходима за безпрепятственото изпълнение на процедурата по освобождаване от отговорност за съответната финансова година, съгласно член 261, параграф 3 от Регламент (ЕС, Евратом) 2018/1046.

12. До 15 май на година N + 2 по препоръка на Съвета Европейският парламент освобождава изпълнителния директор от отговорност по отношение на изпълнението на бюджета за година N.

Член 32

Финансови правила

Финансовите правила, приложими за ENISA, се приемат от управителния съвет след консултация с Комисията. Те не се отклоняват от Делегиран регламент (ЕС) № 1271/2013, освен ако специфичните изисквания за функционирането на ENISA го налагат и ако Комисията е дала предварителното си съгласие.

Член 33

Борба с измамите

1. За улесняване на борбата с измамите, корупцията и други неправомерни дейности в рамките на Регламент (ЕС, Евратом) № 883/2013 на Европейския парламент и на Съвета ([29]), до 28 декември 2019 г. ENISA се присъединява към Междуинституционалното споразумение от 25 май 1999 г. между Европейския парламент, Съвета на Европейския съюз и Комисията на Европейските общности относно вътрешните разследвания от Европейската служба за борба с измамите (OLAF) ([30]). ENISA приема съответни разпоредби, приложими по отношение на всички служители на ENISA, като използва образеца в приложението към посоченото споразумение.

2. Сметната палата на Европейския съюз има правомощия за извършване на одити по документи и инспекции на място на всички бенефициенти на безвъзмездни средства, изпълнители и подизпълнители, които са получили средства от Съюза чрез ENISA.

3. OLAF може да извършва разследвания, включително проверки и инспекции на място, в съответствие с разпоредбите и процедурите, предвидени в Регламент (ЕС Евратом) № 883/2013 и Регламент (Евратом, ЕО) № 2185/96 ([31]) на Съвета, с цел да се установи дали е налице измама, корупция или друга незаконна дейност, накърняваща финансовите интереси на Съюза, във връзка с безвъзмездни средства или поръчка, финансирани от ENISA.

4. Без да се засягат параграфи 1, 2 и 3, споразуменията за сътрудничество с трети държави или международни организации, договорите, споразуменията и решенията на ENISA за отпускане на безвъзмездни средства съдържат разпоредби, с които Сметната палата и OLAF изрично се упълномощават да провеждат такива одити и разследвания съгласно съответните техни компетенции.

([29]) Регламент (ЕС, Евратом) № 883/2013 на Европейския парламент и на Съвета от 11 септември 2013 г. относно разследванията, провеждани от Европейската служба за борба с измамите (OLAF), и за отмяна на Регламент (ЕО) № 1073/1999 на Европейския парламент и на Съвета и Регламент (Евратом) № 1074/1999 на Съвета (ОВ L 248, 18.9.2013 г., стр. 1).

([30]) ОВ L 136, 31.5.1999 г., стр. 15.

([31]) Регламент (Евратом, ЕО) № 2185/96 на Съвета от 11 ноември 1996 г. относно контрола и проверките на място, извършвани от Комисията за защита на финансовите интереси на Европейските общности срещу измами и други нередности (ОВ L 292, 15.11.1996 г., стр. 2).

ГЛАВА V

Персонал

Член 34

Общи разпоредби

Правилникът за длъжностните лица и Условията за работа на другите служители, както и правилата за прилагането им, приети чрез споразумение между институциите на Съюза, се прилагат за персонала на ENISA.

Член 35

Привилегии и имунитети

Протокол № 7 за привилегиите и имунитетите на Европейския съюз, приложен към ДЕС и към ДФЕС, се прилага за ENISA и нейния персонал.

Член 36

Изпълнителен директор

1. Изпълнителният директор се назначава като срочно нает служител на ENISA съгласно член 2, буква а) от Условията за работа на другите служители.

2. Изпълнителният директор се назначава от управителния съвет от списък с кандидати, предложен от Комисията, след открита и прозрачна процедура по подбор.

3. За целите на сключването на договора за назначаване на изпълнителния директор ENISA се представлява от председателя на управителния съвет.

4. Преди назначаването избраният от управителния съвет кандидат се поканва да направи изявление пред съответната комисия на Европейския парламент и да отговори на въпроси на членовете.

5. Мандатът на изпълнителния директор е пет години. Към края на този период Комисията извършва оценка, която взема предвид оценката на работата на изпълнителния директор и бъдещите цели и предизвикателства пред ENISA.

6. Управителният съвет взема решения относно назначаването, удължаването на мандата и освобождаването от длъжност на изпълнителния директор в съответствие с член 18, параграф 2.

7. По предложение на Комисията, в което е взета предвид посочената в параграф 5 оценка, управителният съвет може еднократно да удължи мандата на изпълнителния директор с пет години.

8. Управителният съвет уведомява Европейския парламент за намерението си да удължи мандата на изпълнителния директор. Най-късно три месеца преди такова удължаване изпълнителният директор, ако бъде поканен, прави изявление пред съответната комисия на Европейския парламент и отговаря на въпроси на членовете.

9. Изпълнителен директор, чийто мандат е бил удължен, не участва в нова процедура за подбор за същата длъжност.

10. Изпълнителният директор може да бъде отстранен от длъжност единствено с решение на управителния съвет по предложение на Комисията.

Член 37

Командировани национални експерти и други служители

1. ENISA може да използва командировани национални експерти или друг персонал, който не е нает от ENISA. Правилникът за длъжностните лица и Условията за работа на другите служители не се прилагат за такъв персонал.

2. Управителният съвет приема решение за определяне на правилата относно командироването на национални експерти към ENISA.

ГЛАВА VI

Общи разпоредби относно ENISA

Член 38

Юридически статут на ENISA

1. ENISA е орган на Съюза и притежава правосубектност.

2. Във всяка държава членка ENISA се ползва с най-широката правоспособност, предоставяна на юридически лица съгласно националното право. По-специално тя може да придобива или да се разпорежда с движимо и недвижимо имущество и да бъде страна по съдебни производства.

3. ENISA се представлява от изпълнителния директор.

Член 39

Отговорност на ENISA

1. Договорната отговорност на ENISA се урежда от правото, приложимо към съответния договор.

2. Съдът на Европейския съюз е компетентен да се произнася с решение на основание на арбитражна клауза, съдържаща се в сключен от ENISA договор.

3. В случай на извъндоговорна отговорност ENISA поправя всяка вреда, причинена от нея или от нейните служители при изпълнението на техните задължения, съгласно общите принципи, общи за правните системи на държавите членки.

4. Съдът на Европейския съюз е компетентен по отношение на всякакви спорове, отнасящи се до поправянето на вреди, съгласно посоченото в параграф 3.

5. По отношение на личната отговорност на персонала на ENISA спрямо ENISA се прилагат съответните условия, приложими по отношение на персонала на ENISA.

Член 40

Езиков режим

1. Към ENISA се прилага Регламент № 1 на Съвета ([32]). Държавите членки и другите органи, определени от държавите членки, могат да се обръщат към ENISA и да получават отговор на избран от тях официален език на институциите на Съюза.

2. Преводаческите услуги, необходими за функционирането на ENISA, се предоставят от Центъра за преводи за органите на Европейския съюз.

Член 41

Защита на личните данни

1. При обработката на лични данни от ENISA се прилагат разпоредбите на Регламент (ЕС) 2018/1725.

2. Управителният съвет приема мерките по прилагане, съгласно посоченото в член 45, параграф 3 от Регламент (ЕС) 2018/1725. Управителният съвет може да приеме допълнителни мерки, необходими за прилагането на Регламент (ЕС) 2018/1725 от ENISA.

([32]) Регламент № 1 на Съвета за определяне на езиковия режим на Европейската икономическа общност (ОВ 17, 6.10.1958 г., стр. 385/58).

Член 42

Сътрудничество с трети държави и международни организации

1. Доколкото е необходимо за постигането на целите, посочени в настоящия регламент, ENISA може да си сътрудничи с компетентните органи на трети държави или с международни организации, или и двете. За тази цел след предварително одобрение от Комисията ENISA може да установява работни договорености с органите на трети държави и с международни организации. Тези работни договорености не създават правни задължения за Съюза и неговите държави членки.

2. ENISA е отворена за участие на трети държави, които са сключили споразумения със Съюза за тази цел. Съгласно съответните разпоредби на тези споразумения се установяват работни договорености, уточняващи по-специално естеството, степента и начина на участие на тези държави в работата на ENISA и включват разпоредби, свързани с участието в инициативите, предприемани от ENISA, финансовите вноски и персонала. По въпросите, свързани с персонала, посочените работни договорености трябва да са в съответствие с Правилника за длъжностните лица и Условията за работа на другите служители.

3. Управителният съвет приема стратегия за отношенията с трети държави и международни организации, отнасящи се до въпроси от компетентността на ENISA. Комисията гарантира, че ENISA действа в обхвата на своя мандат и съществуващата институционална рамка, посредством сключване на подходящи работни договорености с изпълнителния директор.

Член 43

Правила за сигурност относно защитата на чувствителна некласифицирана информация и класифицирана информация

След като се консултира с Комисията, ENISA приема свои правила за сигурност, прилагайки принципите, залегнали в правилата за сигурност на Комисията за защита на чувствителна некласифицирана информация и класифицирана информация на Европейския съюз, съгласно посоченото в Решения (ЕС, Евратом) 2015/443 и (ЕС, Евратом) 2015/444. Правилата за сигурност на ENISA обхващат, наред с другото, разпоредби за обмена, обработката и съхранението на такава информация.

Член 44

Споразумение за седалището и условия за функциониране

1. В споразумението за седалището между ENISA и приемащата държава членка, което се сключва след получаване на одобрение от управителния съвет, се предвиждат необходимите клаузи за разполагане на ENISA в приемащата държава членка и за оборудването, което ще се предостави от същата държава членка, както и специалните правила, приложими в приемащата държава членка към изпълнителния директор, членовете на управителния съвет, персонала на ENISA и членовете на техните семейства.

2. Държавата членка, приемаща ENISA предоставя най-добрите възможни условия за гарантиране на правилното функциониране на ENISA, като взима предвид достъпността на мястото, наличието на съответната учебна инфраструктура за децата на членовете на персонала, подходящ достъп до пазара на труда, социално осигуряване и медицински услуги както за децата, така и за съпрузите на членовете на персонала.

Член 45

Административен контрол

Дейността на ENISA подлежи на надзор от европейския омбудсман в съответствие с член 228 от ДФЕС.

ДЯЛ III

РАМКА ЗА СЕРТИФИЦИРАНЕ НА КИБЕРСИГУРНОСТТА

Член 46

Европейска рамка за сертифициране на киберсигурността

1. Европейската рамка за сертифициране на киберсигурността се създава с цел да се подобрят условията за функционирането на вътрешния пазар, като се повиши нивото на киберсигурност в Съюза и се даде възможност за хармонизиран подход на равнището на Съюза спрямо европейските схеми за сертифициране на киберсигурността, с оглед на създаването на цифров единен пазар за ИКТ продукти, ИКТ услуги и ИКТ процеси.

2. С европейската рамка за сертифициране на киберсигурността се предвижда механизъм за установяване на европейски схеми за сертифициране на киберсигурността и за удостоверяване, че ИКТ продуктите, ИКТ услугите и ИКТ процесите, които са били оценени в съответствие с такива схеми, отговарят на определени изисквания за сигурност с цел да се защити наличността, автентичността, целостта или поверителността на съхраняваните, предаваните или обработваните данни или на функциите и услугите, предлагани или направени достъпни чрез тези продукти, услуги и процеси през целия им жизнен цикъл.

Член 47

Непрекъсната работна програма на Съюза за европейското сертифициране на киберсигурността

1. Комисията публикува непрекъсната работна програма на Съюза за европейското сертифициране на киберсигурността (наричана по-нататък „непрекъсната работна програма на Съюза“), в която набелязва стратегическите приоритети за бъдещите европейски схеми за сертифициране на киберсигурността.

2. Непрекъснатата работна програма на Съюза включва по-специално списък на ИКТ продуктите, ИКТ услугите и ИКТ процесите или категориите такива продукти, услуги и процеси, които могат да се възползват от включване в обхвата на дадена европейска схема за сертифициране на киберсигурността.

3. Включването на който и да било конкретен ИКТ продукт, ИКТ услуга и ИКТ процес или категория такива продукти, услуги или процеси в непрекъснатата работна програма на Съюза става на едно или повече от следните основания:

а) наличието и разработването на национални схеми за сертифициране на киберсигурността, които да обхващат някоя конкретна категория ИКТ продукти, ИКТ услуги или ИКТ процеси и по-специално по отношение на опасността от фрагментиране;

б) съответно право или политика на Съюза или национално право или политика;

в) пазарно търсене;

г) развитие на картината на киберзаплахите;

д) искане за изготвянето на конкретен проект за схема от Европейската група за сертифициране на киберсигурността.

4. Комисията взема надлежно предвид становищата на Европейската група за сертифициране на киберсигурността и на Групата на заинтересованите страни в областта на сертифицирането относно проекта на непрекъсната работна програма на Съюза.

5. Първата непрекъсната работна програма на Съюза се публикува до 28 юни 2020 г. Непрекъснатата работна програма на Съюза се актуализира най-малко веднъж на три години и при необходимост по-често.

Член 48

Искане за европейска схема за сертифициране на киберсигурността

1. Комисията може да поиска от ENISA да изготви проект за схема или да преразгледа съществуваща европейска схема за сертифициране на киберсигурността въз основа на непрекъснатата работна програма на Съюза.

2. В надлежно обосновани случаи Комисията или Европейската група за сертифициране на киберсигурността може да поиска от ENISA да изготви проект за схема или да преразгледа съществуваща европейска схема за сертифициране на киберсигурността, която не е включена в непрекъснатата работна програма на Съюза. Непрекъснатата работна програма на Съюза се актуализира съответно.

Член 49

Изготвяне, приемане и преразглеждане на европейските схеми за сертифициране на киберсигурността

1. По искане на Комисията съгласно член 48 ENISA изготвя проект за схема, която отговаря на изискванията на членове 51, 52 и 54.

2. По искане на Европейската група за сертифициране на киберсигурността съгласно член 48, параграф 2, ENISA може да изготви проект за схема, която отговаря на изискванията на членове 51, 52 и 54. Ако ENISA отхвърли такова искане, тя мотивира отказа си. Всяко решение за отхвърляне на такова искане се взема от управителния съвет.

3. При изготвянето на проект за схема ENISA провежда консултации с всички съответни заинтересовани страни посредством официален, отворен, прозрачен и приобщаващ процес на консултация.

4. За всеки проект за схема ENISA създава *ad hoc* работна група в съответствие с член 20, параграф 4, която да предостави на ENISA конкретни съвети и експертно мнение.

5. ENISA си сътрудничи тясно с Европейската група за сертифициране на киберсигурността. Тази група предоставя на ENISA съдействие и експертни консултации във връзка с изготвянето на проекта за схема и приема становище относно проекта за схема.

6. ENISA се съобразява максимално със становището на Европейската група за сертифициране на киберсигурността, преди да предаде на Комисията изготвения съгласно параграфи 3, 4 и 5 проект за схема. Становището на Европейската група за сертифициране на киберсигурността няма обвързващ характер за ENISA и липсата му не може да попречи на ENISA да предаде проекта за схема на Комисията.

7. На основата на проекта за схема, изготвен от ENISA, Комисията може да приема актове за изпълнение, с които да установи европейска схема за сертифициране на киберсигурността за ИКТ продукти, ИКТ услуги и ИКТ процеси, отговаряща на изискванията на членове 51, 52 и 54. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 66, параграф 2.

8. Най-малко на всеки пет години ENISA прави оценка на всяка приета европейска схема за сертифициране на киберсигурността, като взема под внимание обратната информация, получена от заинтересованите страни. Ако е необходимо, Комисията или Европейската група за сертифициране на киберсигурността може да поиска от ENISA да започне процес за разработване на проект за преразгледана схема в съответствие с член 48 и настоящия член.

Член 50

Уебсайт за европейските схеми за сертифициране на киберсигурността

1. ENISA поддържа специален уебсайт за предоставяне на информация и повишаване на осведомеността във връзка с европейските схеми за сертифициране на киберсигурността, европейските сертификати за киберсигурност и ЕС декларациите за съответствие, включително информация във връзка с европейските схеми за сертифициране на киберсигурността, които вече не са в сила, оттеглените и с изтекъл срок на действие европейски сертификати за киберсигурност и ЕС декларации за съответствие, както и хранилището на връзки към информацията за киберсигурността, която се предоставя в съответствие с член 55.

2. По целесъобразност на уебсайта, посочен в параграф 1, се посочват и онези национални схеми за сертифициране на киберсигурността, които са заменени от европейска схема за сертифициране на киберсигурността.

Член 51

Цели, свързани със сигурността на европейските схеми за сертифициране на киберсигурността

Европейските схеми за сертифициране на киберсигурността се проектират така, че да постигнат, според нуждите, най-малко следните цели, свързани със сигурността:

а) да се защитят съхраняваните, предаваните или по друг начин обработваните данни срещу случайно или неразрешено съхраняване, обработка, достъп или разкриване по време на целия жизнен цикъл на ИКТ процеса, ИКТ услугата или ИКТ продукта;

б) да се защитят съхраняваните, предаваните или по друг начин обработваните данни срещу случайно или неразрешено унищожаване, загуба, промяна или липса по време на целия жизнен цикъл на ИКТ продукта, ИКТ услугата или ИКТ процеса;

в) оправомощените лица, програми и машини да имат достъп единствено до данните, услугите и функциите, за които се отнасят правата им на достъп;

г) да се установят и документират известните зависимости и уязвимости;

д) да се регистрира до кои данни, услуги или функции е бил осъществен достъп или са били използвани или обработвани по друг начин, кога и от кого;

е) да бъде възможно да се провери до кои данни, услуги или функции е бил осъществен достъп или са били използвани или обработвани по друг начин, кога и от кого;

ж) да се провери ИКТ продуктите, ИКТ услугите и ИКТ процесите да не съдържат известните към момента уязвимости;

з) своевременно да се възстанови наличието и достъпа до данни, услуги и функции в случай на физически или технически инцидент;

и) ИКТ продуктите, ИКТ услугите и ИКТ процесите да бъдат сигурни по подразбиране и по проект;

й) ИКТ продуктите, ИКТ услугите или ИКТ процесите да се предоставят с актуализиран софтуер и хардуер, които не съдържат обществено известни към момента уязвимости, и да бъдат осигурени механизми за безопасни актуализации.

Член 52

Нива на увереност на европейските схеми за сертифициране на киберсигурността

1. Европейските схеми за сертифициране на киберсигурността могат да предвиждат едно или повече от следните нива на увереност за ИКТ продуктите, ИКТ услугите и ИКТ процесите: „базово“, „съществено“ или „високо“. Нивото на увереност следва да е съизмеримо със степента на риска, свързан с предвидената употреба на ИКТ продукта, ИКТ услугата или ИКТ процеса, с оглед на вероятността от инцидент и неговото въздействие.

2. Европейските сертификати за киберсигурност и ЕС декларациите за съответствие посочват всяко ниво на увереност, предвидено в европейска схема за сертифициране на киберсигурността, в рамките на която е издаден европейският сертификат за киберсигурност или ЕС декларацията за съответствие.

3. Изискванията за сигурност, които отговарят на всяко ниво на увереност се посочват в съответната европейска схема за сертифициране на киберсигурността включително съответните функционалности за сигурност и съответното ниво на стриктност и задълбоченост на оценката, през която трябва да премине даден ИКТ продукт, ИКТ услуга или ИКТ процес.

4. Сертификатът или ЕС декларацията за съответствие се характеризират с препратка към съответните технически спецификации, стандарти и процедури, включително технически проверки, чиято цел е да се намали рискът от киберинциденти или те да бъдат предотвратени.

5. Европейският сертификат за киберсигурност или ЕС декларацията за съответствие, посочващи ниво на увереност „базово“, дава увереност, че ИКТ продуктите, ИКТ услугите и ИКТ процесите, за които този сертификат или тази ЕС декларация за съответствие са издадени, отговарят на съответните изисквания за сигурност, включително функционалности за сигурност, и че са били оценени на ниво, което има за цел да се сведат до минимум известните основни рискове от инциденти и кибератаки. Дейностите по оценка, които трябва да се предприемат, включват най-малко преглед на техническата документация. Когато такъв преглед не е подходящ, се предприемат заместващи дейности с равностоен ефект.

6. Европейският сертификат за киберсигурност, посочващ ниво на увереност „съществено“, дава увереност, че ИКТ продуктите, ИКТ услугите и ИКТ процесите, за които този сертификат е издаден, отговарят на съответните изисквания за сигурност, включително функционалности за сигурността, и че са били оценени на ниво, което има за цел да се сведат до минимум известните киберрискове, рискове от инциденти и кибератаки, извършвани от субекти с ограничени умения и ресурси. Дейностите по оценка, които трябва да се предприемат, включват най-малко следното: преглед, за да се докаже отсъствието на обществено известни уязвимости и изпитване, за да се докаже, че ИКТ продуктите, ИКТ услугите или ИКТ процесите правилно изпълняват необходимите функционалности за сигурност. Когато такива дейности по оценка не са подходящи, се предприемат заместващи дейности с равностоен ефект.

7. Европейският сертификат за киберсигурност, посочващ ниво на увереност „високо“ дава увереност, че ИКТ продуктите, ИКТ услугите и ИКТ процесите, за които сертификатът е издаден, отговарят на съответните изисквания за сигурност, включително функционалности за сигурност, и че са били оценени на ниво, което има за цел да се сведе до минимум рискът от най-висш тип кибератаки, извършвани от субекти със значителни умения и ресурси. Дейностите по оценка включват най-малко следното: преглед, за да се докаже отсъствието на обществено известни уязвимости; изпитване, за да се докаже, че в ИКТ продуктите, ИКТ услугите или ИКТ процесите правилно изпълняват необходимите функционалности за сигурност, на най-високото ниво на съвременните технологии; и оценяване на устойчивостта им на атаки от опитни нападатели чрез опити за проникване. Когато такива дейности по оценка не са подходящи, се предприемат заместващи дейности с равностоен ефект.

8. В дадена европейска схема за сертифициране на киберсигурността може да бъдат посочени няколко нива на оценка в зависимост от взискателността и задълбочеността на използваната методика за оценка. Всяко от нивата на оценка съответства на едно от нивата на увереност на сигурността и се определя от подходяща комбинация компоненти на увереността.

Член 53

Самооценяване на съответствието

1. Дадена европейска схема за сертифициране на киберсигурността може да позволява извършване на самооценяване на съответствието, като отговорност за нея носи единствено производителят или доставчикът на ИКТ продукти, ИКТ услуги или ИКТ процеси. Самооценяване на съответствието се разрешава само във връзка с ИКТ продукти, ИКТ услуги или ИКТ процеси с ниско ниво на риск, съответстващо на ниво на увереност „базисно“.

2. Производителят или доставчикът на ИКТ продукти, ИКТ услуги или ИКТ процеси може да издаде ЕС декларация за съответствие, в която заявява, че е изпълнил определените в схемата изисквания. Чрез издаването на такава декларация производителят или доставчикът на ИКТ продукти, ИКТ услуги или ИКТ процеси поема отговорност за съответствието на ИКТ продукта, ИКТ услугата или ИКТ процеса с определените в схемата изисквания.

3. Производителят или доставчикът на ИКТ продукти, ИКТ услуги или ИКТ процеси съхранява ЕС декларацията за съответствие, техническата документация и всякаква друга съответна информация, отнасяща се до съответствието на ИКТ продуктите или ИКТ услугите със схемата, която е на разположение на националния орган за сертифициране на киберсигурността, посочен в член 58, параграф 1, за срок, определен в съответната европейска схема за сертифициране на киберсигурността. Копие от ЕС декларацията за съответствие се предоставя на националния орган за сертифициране на киберсигурността и на ENISA.

4. Издаването на ЕС декларация за съответствие е доброволно, освен ако не е предвидено друго в правото на Съюза или в правото на държавите членки.

5. ЕС декларацията за съответствие се признава във всички държави членки.

Член 54

Елементи на европейските схеми за сертифициране на киберсигурността

1. Европейските схеми за сертифициране на киберсигурността включват най-малко следните елементи:

а) предмет и обхват на схемата за сертифициране, включително вида или категориите ИКТ продукти, ИКТ услуги или ИКТ процеси, обхванати от нея;

б) ясно описание на предназначението на схемата и на начина, по който избраните стандарти, методи за оценка и нива на увереност отговарят на потребностите на ползвателите на схемата, за които тя е предназначена.

в) позоваване на международни, европейски или национални стандарти, които са били приложени при оценката или, когато не са налични такива стандарти или те не са подходящи, на технически спецификации, които отговарят на изискванията на приложение II към Регламент (ЕС) № 1025/2012, или ако не са налични такива спецификации — на технически спецификации или други изисквания за киберсигурност, предвидени в европейската схема за сертифициране на киберсигурността;

г) когато е уместно, едно или повече нива на увереност;

д) указание дали схемата позволява самооценяване на съответствието;

е) когато е приложимо, специални или допълнителни изисквания, приложими спрямо органите за оценяване на съответствието, така че да се гарантира тяхната техническа компетентност за оценяване на изискванията за киберсигурност;

ж) конкретните критерии и методи за оценка (включително типовете оценки), използвани, с цел да се докаже постигането на свързаните със сигурността цели, посочени в член 51;

з) когато е приложимо, необходимата за сертифицирането информация, която трябва да бъде изпратена или по друг начин предоставена от кандидата на разположение на органите за оценяване на съответствието;

и) когато схемата предвижда маркировки или етикети — условията, при които те могат да бъдат използвани;

й) правилата за наблюдение на съответствието на ИКТ продуктите, ИКТ услугите или ИКТ процесите с изискванията на европейските сертификати за киберсигурност или на ЕС декларациите за съответствие, включително механизми за удостоверяване на трайното съответствие с определените изисквания за киберсигурност;

к) когато е приложимо, условията за издаване, поддържане, продължаване и подновяване на европейски сертификат за киберсигурност, както и условията за разширяване или ограничаване на обхвата на сертифицирането;

л) правила относно последиците за ИКТ продукти, ИКТ услуги и ИКТ процеси, които са били сертифицирани или за които има издадена ЕС декларация за съответствието, но които не съответстват на изискванията на схемата;

м) правила за начина, по който неоткрити до момента уязвимости на киберсигурността на ИКТ продукти, ИКТ услуги и ИКТ процеси трябва да се докладват и отстраняват;

н) когато е приложимо, правила за съхраняването на документация от органите за оценяване на съответствието;

о) списък на националните или международни схеми за сертифициране на киберсигурността, които обхващат същия тип или категории ИКТ продукти, ИКТ услуги и ИКТ процеси, изисквания за сигурност, критерии и методи за оценка и нива на увереност;

п) съдържанието и формата на европейските сертификати за киберсигурност и ЕС декларации за съответствие, които трябва да бъдат издадени;

р) срока, през който следва да бъде налична ЕС декларацията за съответствие, техническата документация и всякаква друга съответна информация, която трябва да се представи от производителя или доставчика на ИКТ продукти, ИКТ услуги или ИКТ процеси;

с) максималния срок на валидност на европейските сертификати за киберсигурност, издадени в рамките на схемата;

т) начините за осведомяване относно европейските сертификати за киберсигурност, издадени, изменени или отнети в рамките на схемата;

у) условията за взаимно признаване на схемите за сертифициране с трети държави;

ф) когато е приложимо, правилата относно установения в схемата механизъм за партньорско оценяване за органите и институциите, издаващи европейски сертификати за киберсигурност за ниво на увереност „високо“ съгласно член 56, параграф 6. Този механизъм не засяга партньорската проверка, предвидена в член 59;

х) формата и процедурите, с които производителите или доставчиците на ИКТ продукти, ИКТ услуги или ИКТ процеси трябва да се съобразяват, когато предоставят и актуализират допълнителната информация за киберсигурността в съответствие с член 55.

2. Определените изисквания на европейската схема за сертифициране на киберсигурността трябва да са в съответствие с всички приложими правни изисквания, по-специално с изискванията, произтичащи от хармонизираното право на Съюза.

3. Когато това е предвидено в конкретен правен акт на Съюза, даден сертификат или ЕС декларация за съответствие, издадени в рамките на европейска схема за сертифициране на киберсигурността може да се използва за удостоверяване на презумпцията за съответствие с изискванията на посочения правен акт.

4. При липса на хармонизирано право на Съюза, в правото на държавите членки може да се предвиди също така, че дадена европейска схема за сертифициране на киберсигурността може да се използва за установяване на презумпцията за съответствие с правните изисквания.

Член 55

Допълнителна информация за киберсигурността на сертифицирани ИКТ продукти, ИКТ услуги и ИКТ процеси

1. Производителят или доставчикът на сертифицирани ИКТ продукти, ИКТ услуги или ИКТ процеси, за които е издадена ЕС декларация за съответствие, осигурява публичен достъп до следната допълнителна информация за киберсигурността:

а) насоки и препоръки, които да помагат на крайните ползватели да конфигурират, инсталират, разгърнат, експлоатират и поддържат по сигурен начин ИКТ продуктите или ИКТ услугите;

б) периода, през който на крайните ползватели ще бъде предложена подкрепа във връзка със сигурността, по-специално по отношение на наличността на актуализации, свързани с киберсигурността;

в) информация за връзка с производителя или доставчика и приемливи начини за получаване на информация за уязвимостта от крайните ползватели или научните изследователи в областта на сигурността;

г) позоваване на хранилищата онлайн със списък на публично оповестените уязвимости, свързани с ИКТ продукта, ИКТ услугата или ИКТ процеса и със съответните инструкции за киберсигурност.

2. Информацията по параграф 1 се предоставя в електронен вид и остава на разположение, като при необходимост се актуализира, най-малко до изтичането на срока на действие на съответния европейски сертификат за киберсигурност или на ЕС декларацията за съответствие.

Член 56

Сертифициране на киберсигурността

1. ИКТ продуктите, ИКТ услугите и ИКТ процесите, сертифицирани по европейска схема за сертифициране на киберсигурността, приета съгласно член 49, се считат за съответстващи на изискванията на такава схема.

2. Сертифицирането на киберсигурността е доброволно, освен ако не е посочено друго в правото на Съюза или в правото на държавите членки.

3. Комисията прави редовно оценяване на ефективността и използването на приетите европейски схеми за сертифициране на киберсигурността и дали някоя конкретна схема следва да бъде направена задължителна посредством съответното право на Съюза, така че да се гарантира подходящо ниво на киберсигурност на ИКТ продуктите, ИКТ услугите и ИКТ процесите в Съюза и да се подобри функционирането на вътрешния пазар. Първото оценяване се прави до 31 декември 2023 г. и най-малко веднъж на 2 години след това се правят последващи оценявания. Въз основа на резултатите от тези оценявания, Комисията набелязва ИКТ продуктите, ИКТ услугите и ИКТ процесите, обхванати от съществуваща схема за сертифициране, които следва да бъдат включени в обхвата на задължителна схема за сертифициране.

Като приоритет Комисията насочва вниманието си към секторите, изброени в приложение II към Директива (ЕС) 2016/1148, които се подлагат на оценяване най-късно две години след приемането на първата европейска схема за сертифициране на киберсигурността.

При подготовката на оценяването Комисията:

а) отчита въздействието на мерките върху производителите или доставчиците на такива ИКТ продукти, ИКТ услуги или ИКТ процеси, както и върху ползвателите, от гледна точка на разходите за тези мерки и социалните или икономическите ползи от очакваното повишено ниво на сигурност на ИКТ продуктите, ИКТ услугите или ИКТ процесите, към които са насочени;

б) взема под внимание наличието и разпространението на съответното право на държавите членки и на трети държави;

в) провежда отворен, прозрачен и приобщаващ процес на консултиране с всички заинтересовани страни и държави членки;

г) отчита сроковете за изпълнение, необходимостта от преходни мерки и срокове, по-специално по отношение на възможното въздействие на мярката върху производителите или доставчиците на ИКТ продукти, ИКТ услуги или ИКТ процеси, включително МСП.

д) предлага най-бързия и ефективен начин, по който трябва да се осъществи преходът от доброволни към задължителни схеми за сертифициране.

4. Органите за оценяване на съответствието, посочени в член 60, издават европейски сертификати за киберсигурност по настоящия член, когато се посочва ниво на увереност „базово“ или „съществено“, на основата на критерии, включени в европейската схема за сертифициране на киберсигурността, приета от Комисията съгласно член 49.

5. Чрез дерогация от параграф 4, в надлежно обосновани случаи дадена европейска схема за сертифициране на киберсигурността може да предвиди, че европейски сертификати за киберсигурност в резултат от тази схема може да бъдат издадени само от публичен орган, когато са посочени основателни причини за такава дерогация. Такъв орган е един от следните:

а) национален орган за сертифициране на киберсигурността, посочен в член 58, параграф 1; или

б) публичен орган, акредитиран като орган за оценяване на съответствието съгласно член 60, параграф 1.

6. Когато европейска схема за сертифициране на киберсигурността, приета по член 49, изисква ниво на увереност „високо“, европейският сертификат за киберсигурност в рамките на тази схема може да бъде издаден само от национален орган за сертифициране на киберсигурността или в следните случаи от орган за оценяване на съответствието:

а) след предварително одобрение от националния орган за сертифициране на киберсигурността за всеки отделен европейски сертификат за киберсигурност, издаден от орган за оценяване на съответствието; или

б) след предварително общо делегиране на задачата по издаването на такива европейски сертификати за киберсигурност на орган за оценяване на съответствието от националния орган за сертифициране на киберсигурността.

7. Физическото или юридическото лице, което подлага ИКТ продукти, ИКТ услуги или ИКТ процеси на процедурите за сертифициране, предоставя на националния орган за сертифициране на киберсигурността по член 58, когато този орган е издаващият орган на европейския сертификат за киберсигурност, или на органа за оценяване на съответствието по член 60, цялата необходима информация за провеждане на сертифицирането.

8. Притежателят на европейски сертификат за киберсигурност уведомява органа или институцията, посочени в параграф 7, за всички открити впоследствие уязвимости или нередности във връзка със сигурността на сертифицирания ИКТ продукт, ИКТ услуга или ИКТ процес, които може да окажат въздействие върху тяхното съответствие с изискванията, свързани със сертифицирането. Органът или институцията изпраща тази информация без излишно забавяне на съответния национален орган за сертифициране на киберсигурността.

9. Европейски сертификат за киберсигурност се издава за срока, определен от европейската схема за сертифициране на киберсигурността, и може да бъде подновен, ако съответните изисквания продължават да се изпълняват.

10. Европейски сертификат за киберсигурност, издаден съгласно настоящия член, се признава във всички държави членки.

Член 57

Национални сертификати и схеми за сертифициране на киберсигурността

1. Без да се засягат разпоредбите на параграф 3 от настоящия член, националните схеми за сертифициране на киберсигурността и свързаните с тях процедури за ИКТ продукти, ИКТ услуги и ИКТ процеси, обхванати от европейска схема за сертифициране на киберсигурността, прекратяват правното си действие от датата, посочена в акта за изпълнение, приет съгласно член 49, параграф 7. Националните схеми за сертифициране на киберсигурността и свързаните с тях процедури за ИКТ продукти, ИКТ услуги и ИКТ процеси, които не са обхванати от европейска схема за сертифициране на киберсигурността, продължават да съществуват.

2. Държавите членки не въвеждат нови национални схеми за сертифициране на киберсигурността на ИКТ продукти, ИКТ услуги и ИКТ процеси, вече обхванати от европейска схема за сертифициране на киберсигурността, която е в сила.

3. Съществуващите сертификати, издадени в рамките на национални схеми за сертифициране на киберсигурността и обхванати от европейска схема за сертифициране на киберсигурността, остават в сила до изтичането си.

4. За да се избегне разпокъсаност на вътрешния пазар, държавите членки уведомяват Комисията и Европейската група за сертифициране на киберсигурността за всяка инициатива за изготвяне на нови национални схеми за сертифициране на киберсигурността.

Член 58

Национални органи за сертифициране на киберсигурността

1. Всяка държава членка определя един или повече национални органи за сертифициране на киберсигурността на своя територия или, по взаимно съгласие с друга държава членка, определя един или повече национални органи за сертифициране на киберсигурността, установени във въпросната друга държава членка, които да отговарят за задачите по надзора в определящата държава членка.

2. Всяка държава членка уведомява Комисията за определените национални органи за сертифициране на киберсигурността. Когато дадена държава членка е определила повече от един орган, тя информира Комисията също за задачите, които са възложени на всеки от тях.

3. Без да се засягат разпоредбите на член 56, параграф 5, буква а) и член 56, параграф 6, всеки национален орган за сертифициране на киберсигурността е независим от субектите, върху които упражнява надзор, по отношение на своята организация, решения за финансиране, правна структура и процес на вземане на решения.

4. Държавите членки гарантират, че дейностите на националните органи за сертифициране на киберсигурността, свързани с издаването на европейски сертификати за киберсигурност, посочени в член 56, параграф 5, буква а) и член 56, параграф 6, са строго разделени от техните надзорни дейности, посочени в настоящия член и че двата вида дейности са независими едни от други.

5. Държавите членки гарантират, че националните органи за сертифициране на киберсигурността разполагат с достатъчно ресурси за упражняване на правомощията си и за изпълнение на възложените им задачи по ефективен и ефикасен начин.

6. За ефективното изпълнение на настоящия регламент е целесъобразно националните органи за сертифициране на киберсигурността да участват активно, реално, ефективно и съобразно правилата за поверителност в Европейската група за сертифициране на киберсигурността.

7. Националните органи за сертифициране на киберсигурността:

а) упражняват надзор и следят за спазването на правилата, включени в европейски схеми за сертифициране на киберсигурността съгласно член 54, параграф 1, буква й), за да наблюдават съответствието на ИКТ продуктите, ИКТ услугите и ИКТ процесите с изискванията на издадените европейски сертификати за киберсигурност на съответната им територия, в сътрудничество с други съответни органи за надзор на пазара;

б) наблюдават и следят за спазването на задълженията на производителите или доставчиците на ИКТ продукти, ИКТ услуги и ИКТ процеси, които са установени на тяхна територия и които извършват самооценяване на съответствието, и по-специално наблюдават и следят за спазването на задълженията на тези производители или доставчици, посочени в член 53, параграфи 2 и 3 и в съответната европейска схема за сертифициране на киберсигурността;

в) без да се засягат разпоредбите на член 60, параграф 3, съдействат активно на националните органи по акредитация и ги подпомагат за наблюдението и надзора на дейностите на органите за оценяване на съответствието за целите на настоящия регламент;

г) наблюдават и упражняват надзор над дейностите на публичните органи, посочени в член 56, параграф 5;

д) в приложимите случаи издават разрешение на органите за оценяване на съответствието съгласно член 60, параграф 3 и ограничават, временно прекратяват или отнемат съществуващо разрешение при неспазване на изискванията на настоящия регламент от страна на органите за оценяване на съответствието;

е) разглеждат жалбите, внесени от физически или юридически лица във връзка с европейски сертификати за киберсигурност, издадени от национални органи за сертифициране на киберсигурността или във връзка с европейски сертификати за киберсигурност — от органите за оценяване на съответствието в съответствие с член 56, параграф 6, или във връзка с ЕС декларации за съответствие, издадени съгласно член 53, както и разследват жалбите по същество, доколкото е необходимо, и информират жалбоподателя за напредъка и резултатите от разследването в разумен срок;

ж) представят годишен обобщаващ доклад за предприетите дейности по букви б), в) и г) от настоящия параграф или по параграф 8 на ENISA и на Европейската група за сертифициране на киберсигурността;

з) сътрудничат си с другите национални органи за сертифициране на киберсигурността или други публични органи, включително чрез споделяне на информация за възможни несъответствия на ИКТ продукти, ИКТ услуги и ИКТ процеси с изискванията на настоящия регламент или с изискванията на конкретни европейски схеми за сертифициране на киберсигурността; и

и) наблюдават промените в областта на сертифицирането на киберсигурността.

8. Всеки национален орган за сертифициране на киберсигурността разполага най-малко със следните правомощия:

а) да изисква от органите за оценяване на съответствието, от притежателите на европейски сертификати за киберсигурност и от издаващите ЕС декларации за съответствие да представят всяка информация, която му е необходима за изпълнението на техните задачи;

б) да провежда под формата на одити разследвания на органите за оценяване на съответствието, притежателите на европейски сертификати за киберсигурност и издаващите ЕС декларации за съответствие за целите на проверка на съответствието с настоящия дял;

в) да взема подходящи мерки съгласно националното право, за да гарантира, че органите за оценяване на съответствието, притежателите на европейски сертификати за киберсигурност и издаващите ЕС декларации за съответствие спазват настоящия регламент или дадена европейска схема за сертифициране на киберсигурността;

г) да получава достъп до всички помещения на всички органи за оценяване на съответствието или на притежателите на европейски сертификати за киберсигурност за целите на провеждане на разследвания съгласно процесуалното право на Съюза или на държавата членка;

д) да отнема в съответствие с националното право европейските сертификати за киберсигурност, издадени от националните органи за сертифициране на киберсигурността или от органите за оценяване на съответствието в съответствие с член 56, параграф 6, когато тези сертификати не са в съответствие с настоящия регламент или с дадена европейска схема за сертифициране на киберсигурността;

е) да налага санкции съгласно националното право, както е предвидено в член 65, и да изисква незабавното преустановяване на нарушенията на задълженията по настоящия регламент.

9. Националните органи за сертифициране на киберсигурността си сътрудничат помежду си и с Комисията, и по-специално обменят информация, опит и добри практики във връзка със сертифицирането на киберсигурността и техническите въпроси, засягащи киберсигурността на ИКТ продукти, ИКТ услуги и ИКТ процеси.

Член 59

Партньорска проверка

1. С цел постигане на равностойни стандарти в целия Съюз за европейските сертификати за киберсигурност и ЕС декларациите за съответствие, националните органи за сертифициране на киберсигурността подлежат на партньорска проверка.

2. Партньорската проверка се извършва на базата на надеждни и прозрачни критерии и процедури за оценяване, по-специално по отношение на изискванията към структурата, човешките ресурси, процеса, поверителността и жалбите.

3. Партньорската проверка оценява:

а) по целесъобразност, дали дейностите на националните органи за сертифициране на киберсигурността, свързани с издаването на европейските сертификати за киберсигурност по член 56, параграф 5, буква а) и член 56, параграф 6, се осъществяват при строго разделение на техните надзорни дейности, посочени в член 58 и дали двата вида дейности са независими едни от други;

б) процедурите за надзор и изпълнение на правилата за наблюдение на съответствието на ИКТ продуктите, ИКТ услугите и ИКТ процесите с европейските сертификати за киберсигурност съгласно член 58, параграф 7, буква а);

в) процедурите за наблюдение и изпълнение на задълженията на производителите или доставчиците на ИКТ продукти, ИКТ услуги или ИКТ процеси съгласно член 58, параграф 7, буква б);

г) процедурите за наблюдение, издаване на разрешения и надзор над дейностите на органите за оценяване на съответствието;

д) по целесъобразност, дали органите или институциите, които издават сертификати за ниво на увереност „високо“ съгласно член 56, параграф 6, разполагат с необходимите експертни познания и опит.

4. Партньорската проверка се извършва най-малко от два национални органа за сертифициране на киберсигурността от други държави членки и Комисията и се провежда най-малко веднъж на всеки пет години. ENISA може да участва в партньорската проверка.

5. Комисията може да приема актове за изпълнение за изготвяне на план за партньорската проверка, който да обхваща период от най-малко пет години и в който да се определят критериите за състава на екипа на партньорската проверка, методиката, която трябва да се използва при партньорската проверка, графика, периодичността и други задачи, свързани с партньорската проверка. При приемането на посочените актове за изпълнение Комисията взема надлежно предвид съображенията на Европейската група за сертифициране на киберсигурността. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 66, параграф 2.

6. Резултатите от партньорските проверки се разглеждат от Европейската група за сертифициране на киберсигурността, която изготвя резюмета, до които може да бъде осигурен публичен достъп, и която при необходимост издава насоки или препоръки за действия или мерки, които да бъдат предприети от съответните субекти.

Член 60

Органи за оценяване на съответствието

1. Органите за оценяване на съответствието се акредитират от националните органи по акредитация, определени по силата на Регламент (ЕО) № 765/2008. Такава акредитация се издава само когато органът за оценяване на съответствието отговаря на изискванията, определени в приложението към настоящия регламент.

2. Когато европейски сертификат за киберсигурност се издава от национален орган за сертифициране на киберсигурността по член 56, параграф 5, буква а) и член 56, параграф 6, сертифициращата структура на националния орган за сертифициране на киберсигурността се акредитира като орган за оценяване на съответствието съгласно параграф 1 от настоящия член.

3. Когато европейските схеми за сертифициране на киберсигурността установяват конкретни или допълнителни изисквания съгласно член 54, параграф 1, буква е), само на органи за оценяване на съответствието, които отговарят на тези изисквания, може да бъде възложено от националния орган за сертифициране на киберсигурността да изпълняват задачи по тези схеми.

4. Акредитацията, посочена в параграф 1, се издава на органите за оценяване на съответствието за максимален срок от пет години и може да бъде подновена при същите условия, ако органът за оценяване на съответствието все още отговаря на изискванията, определени в настоящия член. Националните органи по акредитация вземат в разумен срок всички подходящи мерки за ограничаване, временно спиране или отнемане на акредитацията на органа за оценяване на съответствието, издадена по параграф 1, ако условията за акредитация не са били спазени или вече не се спазват или ако органът за оценяване на съответствието нарушава настоящия регламент.

Член 61

Нотификация

1. За всяка европейска схема за сертифициране на киберсигурността, националните органи за сертифициране на киберсигурността уведомяват Комисията за органите за оценяване на съответствието, които са акредитирани и когато е приложимо — оправомощени по член 60, параграф 3, да издават европейски сертификати за киберсигурност за определени нива на увереност, както е посочено в член 52. Националните органи за сертифициране на киберсигурността уведомяват Комисията без неоправдано закъснение за всяка свързана с тях промяна.

2. Една година след датата на влизане в сила на дадена европейска схема за сертифициране на киберсигурността Комисията публикува списък на органите за оценяване на съответствието, за които е била уведомена по същата схема, в *Официален вестник на Европейския съюз*.

3. Ако Комисията получи уведомление след изтичане на срока, посочен в параграф 2, тя публикува в *Официален вестник на Европейския съюз* измененията на списъка на нотифицираните органи за оценяване на съответствието, в рамките на два месеца от датата на получаване на уведомлението.

4. Всеки национален орган за сертифициране на киберсигурността може да представи на Комисията искане за заличаване на орган за оценяване на съответствието, нотифициран от този орган, от списъка, посочен в параграф 2. Комисията публикува в *Официален вестник на Европейския съюз* съответните изменения на списъка в срок от един месец от датата на получаване на искането от националния орган за сертифициране на киберсигурността.

5. Комисията може да приеме актове за изпълнение, за да установи обстоятелствата, форматите и процедурите за уведомяването, посочено в параграф 1 от настоящия член. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 66, параграф 2.

Член 62

Европейска група за сертифициране на киберсигурността

1. Създава се Европейска група за сертифициране на киберсигурността.

2. Европейската група за сертифициране на киберсигурността е съставена от представители на националните органи за сертифициране на киберсигурността или представители на други съответни национални органи. Всеки член на Европейска група за сертифициране на киберсигурността не може да представлява повече от две държави членки.

3. Заинтересованите страни и съответните трети страни може да бъдат поканени да присъстват на заседанията на Европейска група за сертифициране на киберсигурността и да участват в нейната работа.

4. Групата има следните задачи:

а) да консултира и подпомага Комисията в работата ѝ с цел гарантиране на съгласувано изпълнение и прилагане на настоящия дял, по-специално по въпросите на непрекъснатата работна програма на Съюза, политиката на сертифицирането на киберсигурността, координирането на подходите към политиките, както и на изготвянето на европейските схеми за сертифициране на киберсигурността;

б) да подпомага, консултира и сътрудничи на ENISA във връзка с подготовката на проекти за схеми съгласно член 49;

в) да приеме становище относно проекта за схема, изготвена от ENISA, съгласно член 49;

г) да поиска ENISA да подготви даден проект за европейска схема за сертифициране на киберсигурността съгласно член 48, параграф 2;

д) да приема становища, адресирани до Комисията, свързани с поддръжката и преразглеждането на съществуващите европейски схеми за сертифициране на киберсигурността;

е) да проучва важните новости в областта на сертифицирането на киберсигурността и да обменя информация и добри практики във връзка със схемите за сертифициране на киберсигурността;

ж) да улеснява сътрудничеството между националните органи за сертифициране на киберсигурността по настоящия дял чрез изграждане на капацитет и обмен на информация, по-специално чрез установяване на методи за ефективен обмен на информация, свързана с въпроси на сертифицирането на киберсигурността;

з) да оказва подкрепа за прилагането на механизмите за партньорско оценяване в съответствие с правилата, установени в европейска схема за сертифициране на киберсигурността съгласно член 54, параграф 1, буква ф).

и) да улеснява привеждането на европейските схеми за сертифициране на киберсигурността в съответствие с международно признатите стандарти, включително като преразглежда съществуващите европейски схеми за сертифициране киберсигурността и когато е уместно, като отправя препоръки до ENISA да работи със съответните международни организации за стандартизация, за да се отстранят слабите страни или пропуските в наличните международно признати стандарти.

5. Комисията председателства Европейската група за сертифициране на киберсигурността и осигурява нейния секретариат с помощта на ENISA, в съответствие с член 8, параграф 1, буква д).

Член 63

Право на подаване на жалба

1. Физическите и юридическите лица имат правото да подадат жалба пред органа, издал европейския сертификат за киберсигурност, или, когато жалбата е свързана с европейски сертификат за киберсигурност, издаден от орган за оценяване на съответствието при спазване на член 56, параграф 6, до съответния национален орган за сертифициране на киберсигурността.

2. Органът или институцията, до които е подадена жалбата, уведомява жалбоподателя за хода на предприетите действия и за взетото решение и уведомява жалбоподателя за правото на съдебна защита, посочено в член 64.

Член 64

Право на ефективна съдебна защита

1. Независимо от евентуалните административни или други несъдебни средства за защита, физическите и юридическите лица имат правото на ефективна съдебна защита по отношение на:

а) решенията на орган или институция, посочени в член 63, параграф 1, където е приложимо, във връзка с неправилно издаване, отказ за издаване или признаване на европейски сертификати за киберсигурност, притежавани от тези физически и юридически лица;

б) непредприемането на действия във връзка с жалба, подадена до органа или институцията, посочени в член 63, параграф 1.

2. Производствата по настоящия член се завеждат в съдилищата на държавата членка, в която се намират органът или институцията, срещу които се води съдебното производство.

Член 65

Санкции

Държавите членки определят правилата за санкциите, приложими при нарушаване на настоящия дял и на европейските схеми за сертифициране на киберсигурността, и вземат всички необходими мерки, за да гарантират прилагането на тези санкции. Предвидените санкции трябва да са ефективни, пропорционални и възпиращи. Държавите членки уведомяват Комисията за тези правила и мерки без забавяне и за всяко последващо изменение, което ги засяга.

ДЯЛ IV

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 66

Процедура на комитет

1. Комисията се подпомага от комитет. Този комитет е комитет по смисъла на Регламент (ЕС) № 182/2011.

2. При позоваване на настоящия параграф се прилага член 5, параграф 4, буква б) от Регламент (ЕС) № 182/2011.

Член 67

Оценка и преглед

1. До 28 юни 2024 г. и на всеки пет години след това Комисията оценява въздействието и ефективността на работата на ENISA и нейните работни практики, както и евентуалната необходимост от изменение на мандата на ENISA и финансовите последици от такова изменение. В оценката се взема предвид всякаква обратна информация, предоставена в ENISA в отговор на нейните дейности. Ако Комисията сметне, че съществуването на ENISA вече не е оправдано с оглед на възложените ѝ цели, мандат и задачи, Комисията може да предложи настоящият регламент да бъде изменен в частта му, свързана с ENISA.

2. В оценката също така се разглежда въздействието и ефективността на разпоредбите на дял III от настоящия регламент по отношение на целите за осигуряване на адекватно ниво на киберсигурност на ИКТ продуктите, ИКТ услугите и ИКТ процесите в Съюза и за подобряване на функционирането на вътрешния пазар.

3. В оценката се преценява дали са необходими съществени изисквания за киберсигурност за достъп до вътрешния пазар, за да се предотврати влизането в пазара на Съюза на ИКТ продукти, ИКТ услуги и ИКТ процеси, които не отговарят на базовите изисквания за киберсигурност.

4. До 28 юни 2024 г. и на всеки пет години след това, Комисията изпраща доклад за оценката заедно със своите заключения на Европейския парламент, Съвета и управителния съвет. До заключенията от доклада се осигурява публичен достъп.

Член 68

Отмяна и правоприемство

1. Регламент (ЕС) № 526/2013 се отменя считано от 27 юни 2019 г.

2. Позоваванията на Регламент (ЕС) № 526/2013 и на ENISA, създадена с посочения регламент, се считат за позовавания на настоящия регламент и на ENISA, създадена с настоящия регламент.

3. ENISA, създадена с настоящия регламент, е правоприемник на ENISA, създадена с Регламент (ЕС) № 526/2013, по отношение на цялата собственост, споразумения, правни задължения, трудови договори, финансови ангажименти и задължения. Всички решения на управителния съвет и изпълнителния съвет, приети съгласно Регламент (ЕС) № 526/2013, остават в сила при условие че са в съответствие с настоящия регламент.

4. ENISA се учредява за неограничен срок, считано от 27 юни 2019 г.

5. Изпълнителният директор, назначен съгласно член 24, параграф 4 от Регламент (ЕС) № 526/2013, продължава да изпълнява задълженията на изпълнителен директор, посочени в член 20 от настоящия регламент за остатъка от мандата си. Другите условия от договора на изпълнителния директор остават непроменени.

6. Членовете и техните заместници в управителния съвет, назначени съгласно член 6 от Регламент (ЕС) № 526/2013, продължават да изпълняват задълженията си и да упражняват функциите на управителния съвет, посочени в член 15 от настоящия регламент за остатъка от мандата си.

Член 69

Влизане в сила

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

2. Членове 58, 60, 61, 63, 64 и 65 се прилагат от 28 юни 2021 г.

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

Съставено в Страсбург на 17 април 2019 година.

За Европейския парламент	*За Съвета*
Председател	*Председател*
A. TAJANI	G. CIAMBA

ПРИЛОЖЕНИЕ

ИЗИСКВАНИЯ, НА КОИТО ТРЯБВА ДА ОТГОВАРЯТ ОРГАНИТЕ ЗА ОЦЕНЯВАНЕ НА СЪОТВЕТСТВИЕТО

Органите за оценяване на съответствието, които желаят да бъдат акредитирани, трябва да отговарят на следните изисквания:

1. Органът за оценяване на съответствието се създава съгласно националното право и притежава юридическа правосубектност.

2. Органът за оценяване на съответствието е трета страна, която е независима от организацията или от ИКТ продуктите, ИКТ услугите или ИКТ процесите, които оценява.

3. Орган, който принадлежи към стопанска асоциация или професионална федерация, представляваща предприятия, участващи в проектирането, производството, доставката, сглобяването, използването или поддръжката на ИКТ продукти, ИКТ услуги или ИКТ процеси, които този орган оценява, може да се счита за орган за оценяване на съответствието, при условие че са доказани неговата независимост и липсата на конфликт на интереси.

4. Органът за оценяване на съответствието, неговото висше ръководство и персоналът, който отговаря за изпълнението на задачите по оценяване на съответствието, не могат да са проектант, производител, доставчик, монтажник, купувач, собственик, ползвател или извършващ поддръжката субект на оценявания ИКТ продукт, ИКТ услуга или ИКТ процес или упълномощен представител на някоя от тези страни. Това не изключва използването на оценявани ИКТ продукти, които са необходими за дейностите на органа за оценяване на съответствието, или използването на такива ИКТ продукти за лични цели.

5. Органът за оценяване на съответствието, неговото висше ръководство и персоналът, отговорен за изпълнение на задачите по оценяване на съответствието, не вземат пряко участие в проектирането, производството, конструирането, предлагането на пазара, монтирането, използването или поддръжката на оценяваните ИКТ продукти, ИКТ услуги или ИКТ процеси, нито представляват страни, ангажирани в тези дейности. Органът за оценяване на съответствието, неговото висше ръководство и персоналът, отговорен за изпълнение на задачите по оценяване на съответствието не участват в никаква дейност, която може да е в противоречие с тяхната независима преценка или тяхното почтено поведение по отношение на техните дейности по оценяване на съответствието. Тази забрана се прилага по-конкретно за консултантски услуги.

6. Ако собственик или управляващ на орган за оценяване на съответствието е публичноправен субект или институция, се гарантират независимостта и липсата на конфликт на интереси между националния орган за сертифициране на киберсигурността и органа за оценяване на съответствието, и се документират.

7. Органите за оценяване на съответствието гарантират, че дейностите на техните поделения и подизпълнители не влияят върху поверителността, обективността или безпристрастността на техните дейности по оценяване на съответствието.

8. Органите за оценяване на съответствието и техният персонал осъществяват дейностите по оценяване на съответствието с най-висока степен на професионална почтеност и с необходимата техническа компетентност в определената област и са напълно неподвластни на всякакъв натиск или облаги, включително такива от финансов характер, които биха могли да повлияят на тяхната преценка или на резултатите от техните дейности по оценяване на съответствието, особено от страна на лица или групи лица, заинтересовани от резултатите от тези дейности.

9. Органът за оценяване на съответствието е в състояние да изпълнява всички задачи по оценяване на съответствието, които са му възложени по силата на настоящия регламент, независимо дали тези задачи се изпълняват от самия орган за оценяване на съответствието или от негово име и на негова отговорност. Всяко възлагане на подизпълнители или консултиране на външен персонал надлежно се документира, не включва участието на посредници и е предмет на писмено споразумение, обхващащо, наред с другото, поверителността и конфликтите на интереси. Въпросният орган за оценяване на съответствието поема пълна отговорност за изпълняваните задачи.

10. По всяко време и за всяка процедура за оценяване на съответствието, както и за всеки вид, категория или подкатегория ИКТ продукти, ИКТ услуги или ИКТ процеси органът за оценяване на съответствието разполага с необходимите:

    а) персонал с технически знания и достатъчен и подходящ опит за изпълнение на задачите за оценяване на съответствието;

    б) описания на процедурите, в съответствие с които се извършва оценяването на съответствието, за да се гарантира прозрачността на тези процедури и възможността за тяхното възпроизвеждане. Той разполага с подходящи политики и процедури, които позволяват разграничаване между задачите, които изпълнява като орган за оценяване на съответствието, нотифициран съгласно член 61, и останалите му дейности;

в) процедури за изпълнение на дейности, които надлежно отчитат размера на дадено предприятие, отрасъла, в който то осъществява дейността си, неговата структура, степента на сложност на технологията на въпросния ИКТ продукт, ИКТ услуга или ИКТ процес и масовия или сериен характер на производството.

11. Органът за оценяване на съответствието трябва да разполага със средствата, необходими за изпълнението на технически и административни задачи, свързани с дейностите по оценяване на съответствието, по подходящ начин, както и с достъп до цялото необходимо оборудване и съоръжения.

12. Лицата, отговорни за провеждането на дейностите по оценяване на съответствието, разполагат със:

а) солидно техническо и професионално обучение, обхващащо цялата дейност по оценяване на съответствието;

б) задоволително познаване на изискванията за оценяването на съответствието, което извършват, както и подходящи правомощия за извършването на такова оценяване;

в) подходящи знания и разбиране на приложимите изисквания и стандарти за изпитване;

г) способност да изготвят сертификати, записи и доклади, доказващи, че оценките на съответствието са били извършени.

13. Безпристрастността на органите за оценяване на съответствието, тяхното висше ръководство, лицата, отговорни за провеждането на дейностите по оценяване на съответствието, и всички подизпълнители, които извършват оценяването, трябва да е гарантирана.

14. Възнаграждението на висшето ръководство и на лицата, отговорни за провеждането на дейностите по оценяване на съответствието, който извършва оценяването в даден орган за оценяване на съответствието, не зависи от броя на извършените оценявания на съответствието или резултатите от тях.

15. Органите за оценяване на съответствието сключват застраховка за покриване на отговорността им, освен ако отговорността се поема от държавата членка съгласно националното ѝ право или държавата членка е пряко отговорна за оценяване на съответствието.

16. Органът за оценяване на съответствието и неговият персонал, комитети, дъщерни дружества, подизпълнители и всички други свързани органи или персоналът на външни органи на даден орган за оценяване на съответствието пазят поверителността и спазват служебна тайна по отношение на информацията, получена при изпълнение на техните задачи по оценяване на съответствието съгласно настоящия регламент, или по силата на всяка разпоредба от вътрешното право, която привежда в действие на настоящия регламент, освен когато оповестяването на информацията се изисква съгласно правото на Съюза или на държава членка, на което тези лица са субект, и с изключение по отношение на компетентните органи на държавите членки, в които осъществяват дейностите си. Осигурява се защита на правата на интелектуална собственост. Органът за оценяване на съответствието разполага с въведени документирани процедури във връзка с изискванията по настоящата точка.

17. С изключение на точка 16, изискванията по настоящото приложение по никакъв начин не възпрепятстват обмена на техническа информация и насоки във връзка с нормативната уредба между орган за оценяване на съответствието и лице, кандидатстващо или обмислящо да кандидатства за сертифициране.

18. Органите за оценяване на съответствието извършват дейностите си съгласно набор от последователни, справедливи и разумни условия, като вземат предвид интересите на МСП във връзка с таксите.

19. Органите за оценяване на съответствието отговарят на изискванията на съответния стандарт, който е хармонизиран по силата на Регламент (ЕО) № 765/2008 за акредитацията на органи за оценяване на съответствието, които извършват сертифициране на ИКТ продукти, ИКТ услуги или ИКТ процеси.

20. Органите за оценяване на съответствието гарантират, че изпитвателните лаборатории, използвани за целите на оценяването на съответствието, отговарят на изискванията на съответния стандарт, който е хармонизиран по силата на Регламент (ЕО) № 765/2008 за акредитацията на лаборатории, които извършват изпитвания.