2023/2841

18.12.2023 г.

РЕГЛАМЕНТ (ЕС, Евратом) 2023/2841 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

от 13 декември 2023 година

за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз, и по-специално член 298 от него,

като взеха предвид Договора за създаване на Европейската общност за атомна енергия, и по-специално член 106а от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

в съответствие с обикновената законодателна процедура ([1]),

като имат предвид, че:

(1) В цифровата ера информационните и комуникационните технологии са крайъгълен камък на откритата, ефикасна и независима европейска администрация. Развиващите се технологии и повишената сложност и взаимосвързаност на цифровите системи увеличават рисковете за киберсигурността, в резултат на което субектите на Съюза стават по-уязвими за киберзаплахи и инциденти, което в поражда заплаха за непрекъснатостта на тяхната дейност и за способността им да гарантират сигурността на своите данни. Въпреки че засиленото използване на услуги в облак, повсеместното използване на информационни и комуникационни технологии (ИКТ), високата степен на цифровизация, дистанционната работа и развиващите се технологии и свързаност представляват основни характеристики на всички дейности на субектите на Съюза, все още не е осигурена достатъчна степен на цифрова устойчивост.

(2) Картината на киберзаплахите, пред които са изправени субектите на Съюза, непрекъснато се развива. Тактиката, техниките и процедурите, използвани от авторите на заплахи, непрекъснато се развиват, но основните мотиви за подобни атаки почти не се променят: от кражба на ценна неразкрита информация до сдобиване с парични средства, манипулиране на общественото мнение или увреждане на цифровата инфраструктура. Продължава да расте темпът, с който авторите на заплахи осъществяват своите кибератаки, като същевременно кампаниите им стават все по-сложни и автоматизирани, като те са насочени срещу незащитени от атаки области, които продължават да се увеличават, и уязвимостите бързо се използват.

(3) ИКТ средите на субектите на Съюза се характеризират с взаимозависимост и с интегрирани потоци от данни, а ползвателите им са изградили тясно сътрудничество. Тази взаимосвързаност означава, че всяко прекъсване, дори когато първоначално е ограничено само до един субект на Съюза, може да породи каскадни последици в по-широк план, което е възможно да доведе до мащабно и дълготрайно отрицателно въздействие върху останалите субекти на Съюза. Освен това ИКТ средите на някои субекти на Съюза са свързани с ИКТ средите на държавите членки, в резултат на което инцидент при даден субект на Съюза поражда риск за киберсигурността на ИКТ средите на държавите членки и обратното. Споделянето на информацията за конкретни инциденти може да улесни откриването на сходни киберзаплахи или инциденти, засягащи държавите членки.

(4) Субектите на Съюза са примамливи мишени, които се сблъскват с висококвалифицирани и добре обезпечени с ресурси източници на заплахи, както и с други заплахи. Същевременно съществуват значителни разлики в нивото и зрелостта по отношение на киберустойчивостта на тези субекти и в способността им за откриване и реагиране на злонамерени действия в киберпространството. Поради това за дейността на субектите на Съюза е необходимо те да постигнат високо общо ниво на киберсигурност чрез прилагането на мерки за киберсигурност, съизмерими с установените рискове в тази област, обмен на информация и сътрудничество.

([1]) Позиция на Европейския парламент от 21 ноември 2023 г. (все още непубликувана в Официален вестник) и решение на Съвета от 8 декември 2023 г.

(5) Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета ([2]) има за цел да се подобрят допълнително киберустойчивостта и капацитетът за реагиране при инциденти на публичните и частните субекти, на компетентните органи и субекти, както и на Съюза като цяло. Поради това е необходимо да се гарантира, че субектите на Съюза следват този пример, като се предвидят необходимите правила, които са в съответствие с Директива (ЕС) 2022/2555 и се характеризират със същото равнище на амбиция.

(6) За да се постигне високо общо ниво на киберсигурност, е необходимо всеки субект на Съюза да създаде вътрешна рамка за управление, ръководство и контрол на рисковете за киберсигурността (наричана по-нататък „рамката“), която да гарантира ефективно и разумно управление на всички рискове за киберсигурността и която е съобразена с управлението на кризи и непрекъснатостта на дейността. Рамката следва да определя политики за киберсигурност, включително цели и приоритети, за целите на сигурността на мрежовите и информационните системи, обхващащи цялата некласифицирана ИКТ среда. Рамката следва да се основава на подход, отчитащ всички опасности, който има за цел да се защитят мрежовите и информационните системи и физическата среда на тези системи от събития като кражба, пожар, наводнение, телекомуникационни повреди или прекъсване на електрозахранването или от неразрешен физически достъп и от вреди и намеса в информацията и съоръженията за обработване на информация на даден субект на Съюза, които биха могли да застрашат наличността, верността, целостта или поверителността на данните, които се съхраняват, предават, обработват или до които се осигурява достъп чрез мрежови и информационни системи.

(7) За да управлява рисковете за киберсигурността, установени съгласно рамката, всеки субект на Съюза следва да предприеме подходящи и пропорционални технически, оперативни и организационни мерки. Тези мерки следва да обхващат областите и мерките за управление на рисковете за киберсигурността, предвидени в настоящия регламент, с цел укрепване на киберсигурността на всеки субект на Съюза.

(8) Активите и рисковете за киберсигурността, установени в рамката, както и заключенията, направени вследствие на редовните оценки на зрелостта по отношение на киберсигурността, следва да бъдат отразени в план за киберсигурност, изготвен от всеки субект на Съюза. Планът за киберсигурност следва да включва приетите мерки за управление на рисковете за киберсигурността.

(9) Тъй като осигуряването на киберсигурност е непрекъснат процес, пригодността и ефективността на предприетите съгласно настоящия регламент мерки следва редовно да се преразглеждат с оглед на променящите се рискове за киберсигурността, активи и зрялост на субектите на Съюза по отношение на киберсигурността. Рамката следва да подлежи на преглед редовно и най-малко веднъж на всеки четири години, а планът за киберсигурност следва да се преразглежда веднъж на всеки две години или по-често, когато е необходимо, след оценката на зрелостта по отношение на киберсигурността или след всеки съществен преглед на рамката.

(10) Мерките за управление на рисковете за киберсигурността, въведени от субектите на Съюза, следва да включват политики, които имат за цел, когато е възможно, осигуряването на прозрачност на изходния код, като се вземат предвид гаранциите за правата на трети лица или субекти на Съюза. Тези политики следва да бъдат пропорционални на риска за киберсигурността и те имат за цел да улеснят анализа на киберзаплахите, като същевременно не създават задължения за разкриване на кода или права за достъп до кода на трето лице извън приложимите договорни условия.

(11) Инструментите и приложенията за киберсигурност с отворен код могат да допринесат за по-висока степен на откритост. Отворените стандарти улесняват оперативната съвместимост между инструментите за сигурност и са от полза за сигурността на заинтересованите страни. Инструментите и приложенията за киберсигурност с отворен код могат да привлекат вниманието на по-широката общност на разработчиците, което ще позволи диверсификация на доставчиците. Отвореният код може да доведе до по-прозрачен процес на проверка на инструментите, свързани с киберсигурността, и процес на откриване на уязвимости, насочван от общността. Поради това субектите на Съюза следва да могат да насърчават използването на софтуер с отворен код и отворени стандарти чрез провеждане на политики, свързани с използването на свободно достъпни данни и отворен код в рамките на процеса на осигуряване на сигурност чрез прозрачност.

([2]) Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива за МИС 2) (ОВ L 333, 27.12.2022 г., стр. 80).

(12) Разликите между субектите на Съюза изискват гъвкавост при прилагането на настоящия регламент. Мерките за високо общо ниво на киберсигурност, предвидени в настоящия регламент, следва да не включват задължения, които директно възпрепятстват изпълнението на функциите на субектите на Съюза или нарушават тяхната институционална автономност. Поради това тези субекти следва да създадат свои собствени рамки и да приемат свои собствени мерки за управление на рисковете за киберсигурността и планове за киберсигурност. При прилагането на тези мерки следва надлежно да се отчитат съществуващите полезни взаимодействия между субектите на Съюза с цел правилно управление на ресурсите и оптимизиране на разходите. Следва да се обърне надлежно внимание и на това мерките да не засягат по отрицателен начин ефикасния обмен на информация и сътрудничеството между субектите на Съюза, както и между субектите на Съюза и партньорите им в държавите членки.

(13) В интерес на оптимизирането на използването на ресурсите в настоящия регламент следва да се предвиди възможността два или повече субекти на Съюза със сходни структури да си сътрудничат при извършването на оценките на зрелостта по отношение на киберсигурността за съответните си субекти.

(14) С цел да се избегне налагането на непропорционална финансова и административна тежест върху субектите на Съюза, изискванията за управление на риска за киберсигурността следва да бъдат пропорционални на риска за киберсигурността, който съществува по отношение на съответните мрежови и информационни системи, като се отчитат последните достижения в областта на тези мерки. Всеки субект на Съюза следва да се стреми да отдели подходяща част от своя ИКТ бюджет за подобряване на равнището си на киберсигурност. В дългосрочен план следва да бъде поставена ориентировъчна цел от порядъка на най-малко 10%. В оценката на зрелостта по отношение на киберсигурността следва също така да се прецени дали разходите на съответния субект на Съюза за киберсигурност са пропорционални на рисковете за киберсигурността, пред които е изправен. Без да се засягат правилата, свързани с годишния бюджет на Съюза съгласно Договорите, в предложението си за първия годишен бюджет, който ще бъде приет след влизането в сила на настоящия регламент, Комисията следва да вземе предвид задълженията, произтичащи от настоящия регламент, когато оценява бюджетните нужди и нуждите от персонал на субектите на Съюза, произтичащи от техните приблизителни оценки на разходите.

(15) Високото общо ниво на киберсигурност изисква поставянето на киберсигурността под надзора на висшето ръководство на всеки субект на Съюза. Висшето ръководство на съответния субект на Съюза следва да отговаря за прилагането на настоящия регламент, включително за установяването на рамката, предприемането на мерки за управление на рисковете за киберсигурността и одобряването на плана за киберсигурност. Предприемането на действия във връзка с културата на киберсигурност, т.е. ежедневното практикуване на киберсигурност, е неразделна част от рамката и съответните мерки за управление на рисковете за киберсигурността във всички субекти на Съюза.

(16) Сигурността на мрежовите и информационните системи, работещи с класифицирана информация на ЕС (КИЕС), е от съществено значение. От субектите на Съюза, работещи с КИЕС, се изисква да прилагат въведените всеобхватни регулаторни рамки за защита на тази информация, включително специални правила за управление, политики и процедури за управление на риска. Необходимо е мрежовите и информационните системи, работещи с КИЕС, да съответстват на по-строги стандарти за сигурност от некласифицираните мрежови и информационни системи. Поради това мрежовите и информационните системи, работещи с КИЕС, са по-устойчиви на киберзаплахи и инциденти. Следователно, макар да се признава необходимостта от обща рамка в това отношение, настоящият регламент следва да не се прилага за мрежови и информационни системи, работещи с КИЕС. Ако обаче субект на Съюза изрично поиска това, екипът за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на ЕС (CERT-EU) следва да може да окаже помощ на съответния субект на Съюза във връзка с инциденти в класифицирана ИКТ среда.

(17) Субектите на Съюза следва да оценяват рисковете за киберсигурността във връзка с отношенията с доставчиците на стоки и услуги, включително доставчиците на услуги за съхранение и обработване на данни или на услуги за управление на сигурността, и да предприемат подходящи мерки за справяне с тях. Мерките за киберсигурност следва да бъдат допълнително конкретизирани в документи с насоки или препоръки, отправени от CERT-EU. При определянето на мерки и насоки следва надлежно да се вземат предвид актуалната степен на технологично развитие и когато е приложимо – съответните европейски и международни стандарти, както и съответното право и политики на Съюза, включително оценките на риска за киберсигурността и препоръките, отправени от групата за сътрудничество, създадена съгласно член 14 от Директива (ЕС) 2022/2555, например координираната оценка на риска в областта на киберсигурността на 5G мрежите на равнището на ЕС и инструментариума на ЕС за киберсигурност на 5G технологиите. Освен това, като се има предвид картината на киберзаплахите и колко е важно

изграждането на киберустойчивост за субектите на Съюза, би могло да се изисква сертифициране на съответните ИКТ продукти, услуги и процеси, съгласно специални европейски схеми за сертифициране на киберсигурността, приети в съответствие с член 49 от Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета ([3]).

(18) През май 2011 г. генералните секретари на институциите и органите на Съюза решиха да създадат експериментален екип за CERT-EU под надзора на междуинституционален управителен съвет. През юли 2012 г. генералните секретари потвърдиха практическите договорености и постигнаха съгласие CERT-EU да продължи да съществува като постоянна структура и да продължи да спомага за подобряването на общото ниво на сигурност на информационните технологии на институциите, органите и агенциите на Съюза като пример за видимо междуинституционално сътрудничество в областта на киберсигурността. CERT-EU беше създаден през септември 2012 г. като работна група на Комисията с междуинституционален мандат. През декември 2017 г. институциите и органите на Съюза сключиха междуинституционална договореност относно организацията и функционирането на CERT-EU ([4]). Настоящият регламент следва да предвижда цялостен набор от правила за организацията, функционирането и дейността на CERT-EU. Разпоредбите на настоящия регламент имат предимство пред разпоредбите на сключената през декември 2017 г. междуинституционална договореност относно организацията и функционирането на CERT-EU.

(19) CERT-EU следва да бъде преименуван на „Служба за киберсигурност за институциите, органите, службите и агенциите на Съюза“, но следва да запази краткото наименование CERT-EU, тъй като то вече е познато.

(20) В допълнение към възлагането на повече задачи и разширена роля на CERT-EU с настоящия регламент се създава Междуинституционален съвет по киберсигурност (МСК), с цел улесняване на постигането на високо общо ниво на киберсигурност сред субектите на Съюза. МКС следва да има изключителна функция за мониторинга и оказването на подкрепа при прилагането на настоящия регламент от страна на субектите на Съюза и за надзора на изпълнението на общите приоритети и цели от страна CERT-EU и за предоставянето на стратегически насоки на CERT-EU. Поради това в МСК следва да се гарантира представителството на институциите на Съюза и той следва да включва представители на органите, службите и агенциите на Съюза чрез Мрежата от агенции на Съюза (EUAN). Организацията и функционирането на МСК следва да бъдат допълнително уредени чрез вътрешен процедурен правилник, който може да допълнително да конкретизира правилата във връзка с редовните заседания на МСК, включително годишните срещи на политическото равнище, на които представители на висшето ръководство на всеки член на МСК ще позволят на МСК да провежда стратегически дискусии и ще дадат стратегически насоки на МСК. Освен това МСК следва да може да създаде изпълнителен комитет, който да го подпомага в работата му, и да делегира на комитета някои от своите задачи и правомощия, по-специално във връзка със задачите, които изискват специфичен експертен опит на неговите членове, например одобряване на каталога на услугите и на евентуалните му последващи актуализации, условията за споразуменията за нивото на обслужване, оценките на документи и доклади, представени от субектите на Съюза на МСК съгласно настоящия регламент, или задачите, свързани с изготвянето на решения относно мерките за постигане на съответствие, приети от МСК, и с мониторинга на тяхното изпълнение. МСК следва да утвърди процедурния правилник на изпълнителния комитет, включително неговите задачи и правомощия.

(21) МСК има за цел да окаже подкрепа на субектите на Съюза да подобрят състоянието на киберсигурността си чрез прилагане на настоящия регламент. За да подкрепя субектите на Съюза, МСК следва да дава насоки на ръководителя на CERT-EU, да приеме многогодишна стратегия за повишаване на нивото на киберсигурност в субектите на Съюза, да установи методиката и други аспекти на доброволните партньорски проверки и да улесни създаването на неформална група от местни служители по киберсигурността, подпомагана от Агенцията на Европейския съюз за киберсигурност (ENISA), с цел обмен на най-добри практики и информация във връзка с прилагането на настоящия регламент.

([3]) Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019 г., стр. 15).

([4]) Междуинституционална 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) (ОВ C 12, 13.1.2018 г., стр. 1).

(22) С цел да се постигне високо ниво на киберсигурност във всички субекти на Съюза, интересите на органите, службите и агенциите на Съюза, които управляват собствената си ИКТ среда, следва да бъдат представени в МСК от трима представители, определени от EUAN. Сигурността на обработването на лични данни, а следователно и тяхната киберсигурност, е крайъгълен камък за защитата на данните. С оглед на полезните взаимодействия между защитата на данните и киберсигурността Европейският надзорен орган по защита на данните следва да бъде представен в МСК в качеството му на субект на Съюза, по отношение на който се прилага настоящият регламент, със специфичен експертен опит в областта на защитата на данните, включително сигурността на електронните съобщителни мрежи. Като се има предвид значението на иновациите и конкурентоспособността в областта на киберсигурността, Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността следва да бъде представен в МСК. С оглед на функциите на ENISA като център за експертни познания в областта на киберсигурността и предоставяната от ENISA подкрепа, както и с оглед на значението на киберсигурността на космическата инфраструктура и услуги на Съюза, ENISA и Агенцията на Европейския съюз за космическата програма следва да бъдат представени в МСК. С оглед на функциите, възложени на CERT-EU съгласно настоящия регламент, ръководителят на CERT-EU следва да бъде канен от председателя на МСК на всички заседания на МСК, освен когато МСК обсъжда въпроси, свързани пряко с ръководителя на CERT-EU.

(23) МСК следва да извършва мониторинг за съответствието с настоящия регламент и изпълнението на насоките, препоръките и призивите за действие. МСК следва да получава подкрепа по технически въпроси от технически консултативни групи, съставени по преценка на МСК. Тези технически консултативни групи следва да работят в тясно сътрудничество със CERT-EU, със субектите на Съюза и с други заинтересовани страни, ако е необходимо.

(24) Когато МСК установи, че субект на Съюза не прилага ефективно настоящия регламент или отправените съгласно него насоки, препоръки или призиви за действие, МСК следва да може, без да се засягат вътрешните процедури на съответния субект на Съюза, да приложи мерките за постигане на съответствие. МСК следва да прилага постепенно мерките за постигане на съответствие, с тоест МСК следва първо да приеме най-леката мярка— а именно мотивирано становище — и само ако е необходимо, да приеме нарастващо по-строги мерки, като се стигне до най-строгата мярка, а именно— препоръка за временно спиране на потоците от данни към съответния субект на Съюза. Такава препоръка следва да се прилага само в изключителни случаи на продължителни, умишлени, повтарящи се или тежки нарушения на настоящия регламент от страна на съответния субект на Съюза.

(25) Мотивираното становище представлява най-леката мярка за постигане на съответствие с цел преодоляване на наблюдаваните пропуски в прилагането на настоящия регламент. МСК следва да може да предприема последващи действия във връзка с мотивирано становище с насоки, за да подпомогне съответния субект на Съюза да гарантира, че неговата рамка, мерки за управление на рисковете за киберсигурността, план за киберсигурност и докладване са в съответствие с настоящия регламент, а след това да отправи предупреждение за отстраняване на установените недостатъци от страна на субекта на Съюза в рамките на определен срок. Ако не се предприемат достатъчно ефективни действия за отстраняване на установените в предупреждението недостатъци, МСК следва да може да отправи мотивирано уведомление.

(26) МСК следва да може да препоръча извършването на одит на даден субект на Съюза. За тази цел съответният субект на Съюза следва да може да използва структурата си за вътрешен одит. МСК следва да може също така да поиска извършването на одит от служба за одит на трето лице, включително от доставчик на услуги от частния сектор, избран по взаимно съгласие.

(27) В изключителни случаи на продължително, умишлено, повтарящо се или тежко нарушение на настоящия регламент от страна на субект на Съюза, МСК следва да може да препоръча като крайна мярка на всички държави членки и субекти на Съюза временно спиране на потоците от данни към съответния субект на Съюза, което следва да се прилага до преустановяване на нарушението от страна на субекта на Съюза. Тази препоръка следва да се съобщава чрез подходящи и сигурни канали за комуникация.

(28) За да се гарантира правилното прилагане на настоящия регламент, ако счете, че трайно нарушение на настоящия регламент от страна на субект на Съюза е било причинено пряко от действия или бездействия на член на неговия персонал, включително на висшето ръководство, МСК следва да изиска от съответния субект на Съюза да предприеме подходящи действия, включително да поиска от него да разглежда възможността за предприемане на действия от дисциплинарен характер в съответствие с правилата и процедурите, установени в Правилника за длъжностните лица на Европейския съюз и Условията за работа на другите служители на Съюза, установени в Регламент (ЕИО, Евратом, ЕОВС) № 259/68 на Съвета ([5]) (наричан по-нататък „Правилникът за длъжностните лица“) и всички други приложими правила и процедури.

(29) CERT-EU следва да допринася за сигурността на ИКТ средата на всички субекти на Съюза. Когато решава дали да предостави технически консултации или информация по значими въпроси на политиката по искане на субект на Съюза, CERT-EU следва да гарантира, че това не възпрепятства изпълнението на останалите задачи, които са му възложени съгласно настоящия регламент. По отношение на субектите на Съюза CERT-EU следва да действа като еквивалент на координатора, определен с цел координирано оповестяване на уязвимости съгласно член 12, параграф 1 от Директива (ЕС) 2022/2555.

(30) CERT-EU следва да оказва подкрепа при изпълнението на мерки за високо общо ниво на киберсигурност чрез представяне на предложения за насоки и за препоръки на МСК или чрез отправяне на призиви за действие. Тези насоки и препоръки следва да се одобряват от МСК. При необходимост CERT-EU следва да отправя призиви за действие с описани спешни мерки за сигурност, които субектите на Съюза настоятелно се призовават да предприемат в рамките на определен срок. МСК следва да указва на CERT-EU да отправи, оттегли или измени предложение за насоки или за препоръка или призив за действие.

(31) CERT-EU следва също така да изпълнява функцията, предвидена за него в Директива (ЕС) 2022/2555 по отношение на сътрудничеството и обмена на информация с мрежата на екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС), създадена съгласно член 15 от посочената директива. Освен това в съответствие с Препоръка (ЕС) 2017/1584 на Комисията ([6]) CERT-EU следва да си сътрудничи и да координира реакцията със съответните заинтересовани страни. С цел да допринесе за постигането на високо ниво на киберсигурност в целия Съюз CERT-EU следва да споделя с партньорите в държавите членки информация за конкретни инциденти. CERT-EU следва също така да си сътрудничи с други публични и частни партньори, включително Организацията на Северноатлантическия договор (НАТО), след получаване на предварително одобрение от МСК.

(32) При оказването на подкрепа в областта на оперативната киберсигурност CERT-EU следва да използва наличния експертен опит на ENISA чрез структурирано сътрудничество съгласно Регламент (ЕС) 2019/881. 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. CERT-EU следва да си сътрудничи с ENISA във връзка с анализа на киберзаплахите и редовно да споделя с ENISA своя доклад относно картината на заплахите.

(33) CERT-EU следва да може да си сътрудничи и да обменя информация със съответните общности в областта на киберсигурността в рамките на Съюза и неговите държави членки, за да се насърчи оперативното сътрудничество и да се даде възможност на съществуващите мрежи да реализират пълния си потенциал за защита на Съюза.

(34) Тъй като услугите и задачите на CERT-EU са в интерес на субектите на Съюза, всеки субект на Съюза с ИКТ разходи следва да участва със справедлива вноска в разходите за тези услуги и задачи. Тези вноски не засягат бюджетната автономност на субектите на Съюза.

([5]) Регламент (ЕИО, Евратом, ЕОВС) № 259/68 на Съвета от 29 февруари 1968 г. относно определяне на Правилника за длъжностните лица и Условията за работа на другите служители на Европейските общности и относно постановяване на специални мерки, временно приложими за длъжностни лица на Комисията (ОВ L 56, 4.3.1968 г., стр. 1).

([6]) 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).

(35) Много кибератаки представляват част от по-мащабни кампании, насочени към групи от субекти на Съюза или общности, представляващи интерес, които включват субекти на Съюза. За да се даде възможност за изпреварващо откриване и реагиране на инциденти или предприемане на мерки за ограничаване и възстановяване след инциденти, субектите на Съюза следва да могат да уведомяват CERT-EU за инциденти, киберзаплахи, уязвимости и ситуации, близки до инцидент, и да споделят подходящи технически подробни сведения, които позволяват откриване или смекчаване, както и реагиране на подобни киберзаплахи, уязвимости и ситуации, близки до инцидент**,** в други субекти на Съюза. Като се следва същият подход като предвидения в Директива (ЕС) 2022/2555, субектите на Съюза следва да бъдат задължени да подадат ранно предупреждение до CERT-EU в срок от 24 часа от узнаването на значим инцидент. Този обмен на информация следва да даде възможност на CERT-EU да разпространи информацията до останалите субекти на Съюза, както и до подходящи партньори, за да се спомогне за защитата на ИКТ средите на субектите на Съюза и ИКТ средите на техните партньори срещу подобни инциденти.

(36) В настоящия регламент е предвиден многоетапен подход по отношение на докладването на значими инциденти с цел да се постигне подходящ баланс между бързото докладване, което спомага за ограничаването на потенциалното разпространение на значими инциденти и позволява на субектите на Съюза да потърсят помощ, от една страна, и задълбоченото докладване, с което се извличат ценни поуки от отделните инциденти и се подобрява с течение на времето киберустойчивостта на отделните субекти на Съюза и се допринася за подобряването на цялостното състояние на киберсигурността им, от друга страна. В това отношение настоящият регламент следва да включва докладването на инциденти, които въз основа на извършена от съответния субект на Съюза първоначална оценка биха могли да причинят сериозни оперативни смущения във функционирането или финансови загуби за съответния субект на Съюза или да засегнат други физически или юридически лица, като причинят значителни имуществени или неимуществени вреди. При тази първоначална оценка следва, наред с другото, да се вземат предвид засегнатите мрежови и информационни системи, и по-специално тяхното значение за функционирането на субекта на Съюза, сериозността и техническите характеристики на киберзаплахата и всички присъщи уязвимости, които се използват, както и опитът на субекта на Съюза при сходни инциденти. Показатели като степента, в която е засегнато функционирането на субекта на Съюза, продължителността на инцидента или броя на засегнатите физически или юридически лица биха могли да имат важно значение при определянето на това дали оперативното смущение е сериозно.

(37) Тъй като инфраструктурата и мрежовите и информационните системи на съответния субект на Съюза и държавата членка, в която се намира този субект на Съюза, са взаимосвързани, от решаващо значение е тази държава членка да бъде информирана без необосновано забавяне за всеки значим инцидент в рамките на този субект на Съюза. За целта засегнатият субект на Съюза следва да информира всички съответни партньори в държавите членки, които са определени или създадени съгласно членове 8 и 10 от Директива (ЕС) 2022/2555, за настъпването на значим инцидент, за който той докладва на CERT-EU. Когато CERT-EU узнае за настъпването на значим инцидент в дадена държава членка, той следва да уведоми своя съответен партньор в тази държава членка.

(38) Следва да се въведе механизъм за осигуряване на ефективен обмен на информация, координация и сътрудничество между субектите на Съюза в случай на съществени инциденти, включително ясно определяне на функциите и отговорностите на участващите субекти на Съюза. Представителят на Комисията в МСК следва, при спазване на плана за управление на киберкризи, да бъде звеното за контакт, за да се улесни обменът от страна на МСК на информация от значение във връзка със съществени инциденти с европейската мрежа на организациите за връзка при киберкризи (EU-CyCLONe) като принос към споделената ситуационна осведоменост. Функциите на представителя на Комисията в МСК като звено за контакт следва да не засягат отделните и обособени функции на Комисията в EU-CyCLONe съгласно член 16, параграф 2 от Директива (ЕС) 2022/2555.

(39) Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([7]) се прилага за всяко обработване на лични данни, извършвано съгласно настоящия регламент. Обработването на лични данни би могло да се извършва във връзка с мерките, приети в контекста на управлението на риска за киберсигурността, уязвимостите и действията при инциденти, обмена на информация за инциденти, киберзаплахи и уязвимости и координацията и сътрудничеството при реагиране при инциденти. Тези мерки биха могли да налагат обработването на определени категории лични данни, например IP адреси, единни ресурсни локатори (URL), имена на домейни, адреси на електронна поща, организационни роли на субекта на данните, времеви печати, теми на електронни съобщения или имена на файлове.

([7]) 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).

Всички мерки, предприети съгласно настоящия регламент, следва да са в съответствие с уредбата за защита на данните и неприкосновеността на личния живот, а субектите на Съюза, CERT-EU и, когато е приложимо, МСК следва да въведат всички съответни технически и организационни гаранции, за да осигурят това съответствие по отговорен начин.

(40) С настоящия регламент се установява правното основание за обработването на лични данни от субектите на Съюза, CERT-EU и, когато е приложимо, МСК за целите на изпълнението на техните задачи и изпълнението на задълженията им съгласно настоящия регламент, в съответствие с член 5, параграф 1, буква б) от Регламент (ЕС) 2018/1725. CERT-EU може да действа като обработващ лични данни или администратор в зависимост от задачата, която изпълнява съгласно Регламент (ЕС) 2018/1725.

(41) В определени случаи, с цел да спазят задълженията си съгласно настоящия регламент за осигуряване на високо ниво на киберсигурност, и по-специално в контекста на уязвимостта и действията при инциденти, може да се наложи субектите на Съюза и CERT-EU да обработват специални категории лични данни, посочени в член 10, параграф 1 от Регламент (ЕС) 2018/1725. С настоящия регламент се установява правното основание за обработването на специални категории лични данни от субектите на Съюза и CERT-EU в съответствие с член 10, параграф 2, буква ж) от Регламент (ЕС) 2018/1725. Обработването на специални категории лични данни съгласно настоящия регламент следва да бъде строго пропорционално на преследваната цел. При спазване на условията, предвидени в член 10, параграф 2, буква ж) от посочения регламент, субектите на Съюза и CERT-EU следва да могат да обработват такива данни само доколкото това е необходимо и когато това е изрично предвидено в настоящия регламент. Когато обработват специални категории лични данни, субектите на Съюза и CERT-EU следва да зачитат същността на правото на защита на данните и да предвиждат подходящи и конкретни мерки за защита на основните права и на интересите на субектите на данни.

(42) Съгласно член 33 от Регламент (ЕС) 2018/1725 субектите на Съюза и CERT-EU, като вземат предвид достиженията на техническия прогрес, разходите за изпълнение и естеството, обхвата, контекста и целите на обработването, както и рисковете с различна степен на вероятност и тежест за правата и свободите на физическите лица, следва да прилагат подходящи технически и организационни мерки, за да гарантират подходящо ниво на сигурност на личните данни, например предоставяне на права за ограничен достъп въз основа на принципа „необходимост да се знае“, прилагане на принципите за одитна пътека, приемане на верига за проследяване, съхранение на данни в покой в контролирана и подлежаща на одит среда, стандартизирани оперативни процедури и мерки за запазване на неприкосновеността на личния живот, например псевдонимизация или криптиране. Посочените мерки следва да не се прилагат по начин, който засяга целите на действията при инциденти и целостта на доказателствата. Когато субект на Съюза или CERT-EU предава лични данни, свързани с инцидент, включително специални категории лични данни, на различни партньори к за целите на настоящия регламент, това предаване следва да е в съответствие с Регламент (ЕС) 2018/1725. Когато специални категории лични данни се предават на трето лице, субектите на Съюза и CERT-EU следва да гарантират, че третото лице прилага мерки относно защитата на личните данни на равнище, равностойно на предвиденото в Регламент (ЕС) 2018/1725.

(43) Личните данни, обработвани за целите на настоящия регламент, следва да се съхраняват само докато това е необходимо в съответствие с Регламент (ЕС) 2018/1725. Субектите на Съюза и когато е приложимо, CERT-EU, когато действат като администратори, следва да определят срокове за съхранение, ограничени до необходимото за постигане на посочените цели. По-специално във връзка с личните данни, събирани за целите на справянето с инциденти, субектите на Съюза и CERT-EU следва да правят разграничение между личните данни, които се събират за откриване на киберзаплаха в своята ИКТ среда с цел предотвратяване на инцидент, и личните данни, които се събират с цел ограничаване на последиците от инцидент, реагиране на инцидент и възстановяване от него. За откриването на киберзаплаха е важно да се вземе предвид периодът от време, през който даден автор на заплаха може да остане незабелязан в дадена система. За целите на ограничаването на последиците от инцидент, реагирането на инцидент и възстановяването от него е важно да се прецени дали личните данни са необходими за проследяване и справяне с повтарящ се инцидент или инцидент от подобно естество, за който може да се докаже корелация.

(44) При обработването на информация от страна на субектите на Съюза и CERT-EU се спазват приложимите правила относно информационната сигурност. Включването на сигурността на човешките ресурси като мярка за управление на рисковете за киберсигурността също следва да е в съответствие с приложимите правила.

(45) За целите на обмена на информация се използват видими маркировки, за да се укаже, че получателите на информацията трябва да прилагат граници на споделяне, въз основа по-специално на споразумения за неразкриване на информация или на неформални споразумения за неразкриване на информация, например протокола за обмен на информация с цветен код за поверителност или други ясни указания от източника. Протоколът за обмен на информация с цветен код за поверителност следва да се разглежда като средство за предоставяне на информация за всякакви ограничения по отношение на по-нататъшното разпространение на информацията. Той се използва в почти всички ЕРИКС и в някои центрове за анализ и обмен на информация.

(46) Настоящият регламент следва да бъде оценяван редовно с оглед на бъдещите преговори за многогодишните финансови рамки, което ще предостави възможност за вземането на по-нататъшни решения относно функционирането и институционалната роля на CERT-EU, включително евентуалното му учредяване като служба на Съюза.

(47) МСК, със съдействието на CERT-EU, следва да извършва преглед и оценка на прилагането на настоящия регламент и да докладва констатациите си на Комисията. Въз основа на тази информация Комисията следва да докладва на Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите. В посочения доклад, с участието на МСК, следва да се оцени целесъобразността на включването в обхвата на настоящия регламент на мрежовите и информационните системи, работещи с КИЕС, по-специално при липсата на общи за субектите на Съюза правила за информационна сигурност.

(48) В съответствие с принципа на пропорционалност за реализирането на основната цел за постигане на високо общо ниво на киберсигурност в рамките на субектите на Съюза е необходимо и целесъобразно да се установят правила в областта на киберсигурността за субектите на Съюза. Настоящият регламент не надхвърля необходимото за постигането на поставената цел в съответствие с член 5, параграф 4 от Договора за Европейския съюз.

(49) Настоящият регламент е съобразен с факта, че субектите на Съюза се различават по размер и капацитет, включително по отношение на финансовите и човешките ресурси.

(50) Европейският надзорен орган по защита на данните беше консултиран в съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 и прие своето становище на 17 май 2022 г. ([8]),

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

ГЛАВА I

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет

С настоящия регламент се определят мерки, които имат за цел постигането на високо общо ниво на киберсигурност в рамките на субектите на Съюза по отношение на:

а) установяването от страна на всеки субект на Съюза на вътрешна рамка за управление, ръководство и контрол на рисковете за киберсигурността съгласно член 6;

б) управление, докладване и обмен на информация за рисковете за киберсигурността;

в) организацията, функционирането и дейността на Междуинституционалния съвет по киберсигурност, създаден съгласно член 10, както и организацията, функционирането и дейността на Службата за киберсигурност за институциите, органите, службите и агенциите на Съюза (CERT-EU);

г) мониторинга на прилагането на настоящия регламент.

([8]) ОВ C 258, 5.7.2022 г., стр. 10.

Член 2

Обхват

1. Настоящият регламент се прилага за субектите на Съюза, за Междуинституционалния съвет по киберсигурност, създаден съгласно член 10, и за CERT-EU.

2. Настоящият регламент се прилага, без да се засяга институционалната автономност съгласно Договорите.

3. С изключение на член 13, параграф 8, настоящият регламент не се прилага за мрежови и информационни системи, работещи с класифицирана информация на ЕС (КИЕС).

Член 3

Определения

За целите на настоящия регламент се прилагат следните определения:

1) „субекти на Съюза“ означава институциите, органите, службите и агенциите на Съюза, създадени съгласно или въз основа на Договора за Европейския съюз, Договора за функционирането на Европейския съюз (ДФЕС) или Договора за създаване на Европейската общност за атомна енергия;

2) „мрежова и информационна система“ означава мрежова и информационна система съгласно определението в член 6, точка 1 от Директива (ЕС) 2022/2555;

3) „сигурност на мрежовите и информационните системи“ означава сигурност на мрежовите и информационните системи съгласно определението в член 6, точка 2 от Директива (ЕС) 2022/2555;

4) „киберсигурност“ означава киберсигурност съгласно определението в член 2, точка 1 от Регламент (ЕС) 2019/881;

5) „висше ръководство“ означава ръководител, ръководен орган или координационен и надзорен орган, отговарящ за функционирането на даден субект на Съюза, на най-високото административно равнище, с правомощия да приема или одобрява решения в съответствие с правилата за управление на високо равнище на съответния субект на Съюза, без да се засягат официалните отговорности на други равнища на управление за постигане на съответствие и управление на рисковете за киберсигурността в съответните им области на отговорност;

6) „ситуация, близка до инцидент“ означава ситуация, близка до инцидент, съгласно определението в член 6, точка 5 от Директива (ЕС) 2022/2555;

7) „инцидент“ означава инцидент съгласно определението в член 6, точка 6 от Директива (ЕС) 2022/2555;

8) „съществен инцидент“ означава инцидент, водещ до смущение в мащаб, който надхвърля способността на даден субект на Съюза и на CERT-EU да реагират на съответния инцидент, или който има значително въздействие върху най-малко два субекта на Съюза;

9) „мащабен киберинцидент“ означава мащабен киберинцидент съгласно определението в член 6, точка 7 от Директива (ЕС) 2022/2555;

10) „действия при инцидент“ означава действия при инцидент съгласно определението в член 6, точка 8 от Директива (ЕС) 2022/2555;

11) „киберзаплаха“ означава киберзаплаха съгласно определението в член 2, точка 8 от Регламент (ЕС) 2019/881;

12) „значителна киберзаплаха“ означава значителна киберзаплаха съгласно определението в член 6, точка 11 от Директива (ЕС) 2022/2555;

13) „уязвимост“ означава уязвимост съгласно определението в член 6, точка 15 от Директива (ЕС) 2022/2555;

14) „риск за киберсигурността “ означава риск съгласно определението в член 6, точка 9 от Директива (ЕС) 2022/2555;

15) „компютърна услуга „в облак“ означава компютърна услуга „в облак“ съгласно определението в член 6, точка 30 от Директива (ЕС) 2022/2555;

Член 4

Обработване на лични данни

1. Обработването на лични данни съгласно настоящия регламент от страна на CERT-EU, Междуинституционалния съвет по киберсигурност, създаден съгласно член 10, и субекти на Съюза се извършва в съответствие с Регламент (ЕС) 2018/1725.

2. Когато изпълняват задачи или задължения съгласно настоящия регламент, CERT-EU, Междуинституционалният съвет по киберсигурност, създаден съгласно член 10, и субектите на Съюза обработват и обменят лични данни само доколкото това е необходимо и единствено с цел изпълнение на тези задачи или задължения.

3. Обработването на специални категории лични данни, посочени в член 10, параграф 1 от Регламент (ЕС) 2018/1725, се счита за необходимо на основание значим обществен интерес съгласно член 10, параграф 2, буква ж) от посочения регламент. Тези данни могат да бъдат обработвани само доколкото това е необходимо за прилагането на мерките за управление на рисковете за киберсигурността, посочени в членове 6 и 8, за предоставянето на услуги от CERT-EU съгласно член 13, за обмена на информация за конкретни инциденти съгласно член 17, параграф 3 и член 18, параграф 3, за обмена на информация съгласно член 20, за задълженията за докладване съгласно член 21, за координацията и сътрудничеството при реагиране на инциденти съгласно член 22 и за управлението на съществени инциденти съгласно член 23 от настоящия регламент. Когато действат като администратори на данни, субектите на Съюза и CERT-EU прилагат технически мерки за предотвратяване на обработването на специални категории лични данни за други цели и предвиждат подходящи и конкретни мерки за защита на основните права и на интересите на субектите на данни.

ГЛАВА II

МЕРКИ ЗА ВИСОКО ОБЩО НИВО НА КИБЕРСИГУРНОСТ

Член 5

Изпълнение на мерките

1. В срок до 8 септември 2024 г. Междуинституционалният съвет по киберсигурност, създаден съгласно член 10, след като се консултира с Агенцията на Европейския съюз за киберсигурност (ENISA) и след като получи насоки от CERT-EU, отправя насоки към субектите на Съюза с цел извършване на първоначален преглед на киберсигурността и създаване на вътрешна рамка за управление, ръководство и контрол на рисковете за киберсигурността съгласно член 6, извършване на оценки на зрелостта по отношение на киберсигурността съгласно член 7, предприемане на мерки за управление на рисковете за киберсигурността съгласно член 8 и приемане на плана за киберсигурност съгласно член 9.

2. При прилагането на членове 6- 9 субектите на Съюза вземат предвид насоките, посочени в параграф 1 от настоящия член, както и приложимите насоки и препоръки, приети съгласно членове 11 и 14.

Член 6

Рамка за управление, ръководство и контрол на рисковете за киберсигурността

1. В срок до 8 април 2025 г. всеки субект на Съюза, след като извърши първоначален преглед на киберсигурността, например одит, установява вътрешна рамка за управление, ръководство и контрол на рисковете за киберсигурността (наричана по-нататък „рамката“). Установяването на рамката се контролира от висшето ръководство на субекта на Съюза, което носи отговорност за нея.

2. Рамката обхваща цялата некласифицирана ИКТ среда на съответния субект на Съюза, включително всяка локална ИКТ среда и оперативна технологична мрежа, активи и услуги в условията на компютърни услуги „в облак“, възложени на подизпълнители или хоствани от трети лица, мобилни устройства, корпоративни мрежи, бизнес мрежи, които не са свързани с интернет, и всякакви устройства, свързани с посочените среди (наричана по-нататък „ИКТ средата“). Рамката се основава на подход, обхващащ всички опасности.

3. Рамката трябва да гарантира високо ниво на киберсигурност. С рамката се установяват вътрешни политики за киберсигурност, включително цели и приоритети, за сигурността на мрежовите и информационните системи, както и функциите и отговорностите на служителите на субекта на Съюза, на които е възложено да гарантират ефективното прилагане на настоящия регламент. Рамката включва и механизми за измерване на ефективността на прилагането.

4. Рамката подлежи на редовен преглед, с оглед на променящите се рискове за киберсигурността, и най-малко на всеки четири години. Когато е целесъобразно и при искане на Междуинституционалния съвет по киберсигурност, създаден съгласно член 10, рамката на съответния субект на Съюза може да се актуализира въз основа на насоките на CERT-EU относно установени инциденти или евентуални пропуски, наблюдавани в рамките на прилагането на настоящия регламент.

5. Висшето ръководство на всеки субект на Съюза отговаря за прилагането на настоящия регламент и следи за спазването от страна на неговата организация на задълженията, свързани с рамката.

6. Когато е целесъобразно и без да се засяга отговорността му за прилагането на настоящия регламент, висшето ръководство на всеки субект на Съюза може да делегира конкретни задължения по настоящия регламент на висши длъжностни лица по смисъла на член 29, параграф 2 от Правилника за длъжностните лица или на други длъжностни лица на равностойно равнище в рамките на съответния субект на Съюза. Независимо от това делегиране, от висшето ръководство може да се търси отговорност за нарушения на настоящия регламент от страна на съответния субект на Съюза.

7. Всеки субект на Съюза трябва да разполага с ефективни механизми, за да гарантира, че подходящ процент от ИКТ бюджета се изразходва за киберсигурност. При определянето на този процент надлежно се взема предвид рамката.

8. Всеки субект на Съюза назначава местен служител по киберсигурността или служител на равностойна позиция, който действа като единно звено за контакт по отношение на всички аспекти на киберсигурността. Местният служител по киберсигурността улеснява прилагането на настоящия регламент и се отчита пряко и редовно пред висшето ръководство за напредъка по прилагането. Без да се засяга фактът, че местният служител по киберсигурността е единното звено за контакт във всеки субект на Съюза, даден субект на Съюза може да делегира на CERT-EU определени задачи на местния служител по киберсигурността във връзка с прилагането на настоящия регламент въз основа на споразумение за нивото на обслужване, сключено между съответния субект на Съюза и CERT-EU, или изпълнението на тези задачи може да се споделя от няколко субекта на Съюза. Когато тези задачи са делегирани на CERT-EU, Междуинституционалният съвет по киберсигурност, създаден съгласно член 10, решава дали предоставянето на съответната услуга трябва да бъде част от базовите услуги на CERT-EU, като взема предвид човешките и финансовите ресурси на съответния субект на Съюза. Всеки субект на Съюза уведомява без необосновано забавяне CERT-EU за назначените местни служители по киберсигурността и за всяка последваща промяна, свързана с тях.

CERT-EU изготвя и осигурява актуализирането на списък на назначените местни служители по киберсигурността.

9. Висшите длъжностни лица по смисъла на член 29, параграф 2 от Правилника за длъжностните лица или други длъжностни лица на равностойно равнище в рамките на съответния субект на Съюза, както и съответните членове на персонала, на който е възложено изпълнението на мерките и задълженията за управление на рисковете за киберсигурността, предвидени в настоящия регламент, редовно преминават специално обучение, за да придобият достатъчно знания и умения с цел разбиране и оценка на практиките във връзка с рисковете за киберсигурността и управлението на рисковете за киберсигурността, както и на тяхното въздействие върху дейността на съответния субект на Съюза.

Член 7

Оценки на зрелостта по отношение на киберсигурността

1. В срок до 8 юли 2025 г. и най-малко на всеки две години след това всеки субект на Съюза извършва оценка на зрелостта по отношение на киберсигурността, включваща всички елементи на неговата ИКТ среда.

2. Оценките на зрелостта по отношение на киберсигурността се извършват, когато е целесъобразно, с помощта на трето лице специалист.

3. Субектите на Съюза със сходни структури могат да си сътрудничат при извършването на оценки на зрелостта по отношение на киберсигурността за съответните си субекти.

4. По искане на Междуинституционалния съвет по киберсигурност, създаден съгласно член 10, и с изричното съгласие на съответния субект на Съюза резултатите от оценката на зрелостта по отношение на киберсигурността могат да бъдат обсъдени в рамките на Междуинституционалния съвет по киберсигурност или в рамките на неформалната група на местните служители по киберсигурността с цел извличане на поуки от натрупания опит и споделяне на най-добри практики.

Член 8

Мерки за управление на рисковете за киберсигурността

1. Всеки субект на Съюза предприема без необосновано забавяне и във всички случаи до 8 септември 2025 г., под надзора на своето висше ръководство, подходящи и пропорционални технически, оперативни и организационни мерки за управление на рисковете за киберсигурността, установени съгласно рамката, и за предотвратяване на инциденти или за свеждане до минимум на тяхното въздействие. Като се вземат предвид достиженията на техническия прогрес и когато е приложимо, съответните европейски и международни стандарти, посочените мерки трябва да гарантират ниво на сигурност на мрежовите и информационните системи в цялата ИКТ среда, съизмеримо с наличните рискове за киберсигурността. При оценката на пропорционалността на тези мерки надлежно се вземат предвид степента на изложеност на съответния субект на Съюза на рискове за киберсигурността, неговият размер, вероятността от настъпване на инциденти и тяхната сериозност, включително тяхното обществено, икономическо и междуинституционално въздействие.

2. При изпълнението на мерките за управление на рисковете за киберсигурността субектите на Съюза предприемат действия най-малко в следните области:

а) политиката в областта на киберсигурността, включително мерките, необходими за постигане на целите и приоритетите, посочени в член 6 и параграф 3 от настоящия член;

б) политики за анализ на рисковете за киберсигурността и сигурност на информационните системи;

в) цели на политиката по отношение на използването на компютърни услуги „в облак“;

г) одит на киберсигурността, когато е целесъобразно, който може да включва оценка на рисковете за киберсигурността, уязвимостта и киберзаплахите, както и редовно тестване на проникването, извършвано от надежден частен доставчик;

д) изпълнение на препоръките, произтичащи от одитите на киберсигурността, посочени в буква г), чрез актуализации на киберсигурността и на политиката;

е) организация на киберсигурността, включително определяне на функциите и отговорностите;

ж) управление на активите, включително инвентарен опис на ИКТ активите и картографиране на ИКТ мрежата;

з) сигурност на човешките ресурси и контрол на достъпа;

и) сигурност на операциите;

й) сигурност на комуникациите;

к) придобиване, разработване и поддържане на системите, включително политики за действията при уязвимости и тяхното оповестяване;

л) когато е възможно, политики за прозрачността на изходния код;

м) сигурност на веригата на доставки, включително аспектите, свързани със сигурността на отношенията между всеки субект на Съюза и неговите преки доставчици на стоки и услуги;

н) действия при инциденти и сътрудничество със CERT-EU, като например извършване на мониторинг на сигурността и водене на регистри;

о) управление на непрекъснатостта на дейността, като например управление на съхраняването на резервни копия на данните и възстановяване след бедствия, и управление на кризи; и

п) насърчаване и развитие на образованието, уменията, повишаването на осведомеността, упражненията и програмите за обучение в областта на киберсигурността.

За целите на първа алинея, буква м) субектите на Съюза вземат предвид уязвимостите, присъщи на всеки пряк доставчик на стоки и услуги, и цялостното качество на продуктите и практиките в областта на киберсигурността на своите доставчици на стоки и услуги, включително техните процедури за сигурно разработване.

3. Субектите на Съюза предприемат най-малко следните конкретни мерки за управление на рисковете за киберсигурността:

а) технически правила за осигуряване и поддържане на възможност за дистанционна работа;

б) конкретни стъпки за преминаване към принципи на нулево доверие;

в) използване на многофакторни решения за удостоверяване на автентичността като норма в мрежовите и информационните системи;

г) използване на криптография и криптиране, и по-специално криптиране от край до край, както и защитен цифров подпис;

д) когато е целесъобразно, защитени гласови, видео и текстови съобщения и защитени системи за спешни повиквания в рамките на субекта на Съюза;

е) изпреварващи мерки за откриване и отстраняване на зловреден софтуер и шпионски софтуер;

ж) установяване на сигурността на веригите за доставка на софтуер чрез критерии за сигурно разработване и оценка на софтуера;

з) изготвяне и приемане на програми за обучение в областта на киберсигурността, съизмерими с възложените задачи и очакваните способности за висшето ръководство и служителите на субекта на Съюза, на които е възложено да гарантират ефективното прилагане на настоящия регламент;

и) редовно обучение на служителите в областта на киберсигурността;

й) когато е приложимо, участие в анализи на риска от взаимосвързаността между субектите на Съюза;

к) подобряване на правилата за възлагане на поръчки, за да се улесни постигането на високо общо ниво на киберсигурност чрез:

i) премахване на договорните пречки, които ограничават доставчиците на ИКТ услуги да споделят информация със CERT-EU относно инциденти, уязвимости и киберзаплахи;

ii) договорни задължения за докладване на инциденти, уязвимости и киберзаплахи, както и за въвеждане на подходящи механизми за реагиране и мониторинг на инцидентите.

Член 9

Планове за киберсигурност

1. При отчитане на заключенията от оценката на зрелостта по отношение на киберсигурността, извършена съгласно член 7, и на активите и установените в рамката рискове за киберсигурността, както и мерките за управление на рисковете за киберсигурността, предприети съгласно член 8, висшето ръководство на всеки субект на Съюза одобрява план за киберсигурност без необосновано забавяне и във всеки случай до 8 януари 2026 г. Планът за киберсигурност цели повишаване на цялостната киберсигурност на субекта на Съюза, като по този начин допринася за утвърждаването на високо общо ниво на киберсигурност в рамките на субектите на Съюза. Планът за киберсигурност включва най-малко мерките за управление на рисковете за киберсигурността, предприети съгласно член 8. Планът за киберсигурност се преразглежда на всеки две години или по-често, когато е необходимо, след оценките на зрелостта по отношение на киберсигурността, които се извършват съгласно член 7, или след всеки съществен преглед на рамката.

2. Планът за киберсигурност включва плана на субекта на Съюза за управление на киберкризи при съществени инциденти.

3. Субектът на Съюза представя изготвения план за киберсигурност на Междуинституционалния съвет по киберсигурност, създаден съгласно член 10.

ГЛАВА III

МЕЖДУИНСТИТУЦИОНАЛЕН СЪВЕТ ПО КИБЕРСИГУРНОСТ

Член 10

Междуинституционален съвет по киберсигурност

1. Създава се Междуинституционален съвет по киберсигурност (МСК).

2. МСК отговаря за:

а) мониторинга и подкрепата за целите на прилагането на настоящия регламент от страна на субектите на Съюза;

б) надзора по отношение на изпълнението на общите приоритети и цели от страна на CERT-EU и даването на стратегически насоки на CERT-EU.

3. МСК се състои от:

а) по един представител, определен от всеки от посочените по-долу:

i) Европейския парламент;

ii) Европейския съвет;

iii) Съвета на Европейския съюз;

iv) Комисията;

v) Съда на Европейския съюз;

vi) Европейската централна банка;

vii) Европейската сметна палата;

viii) Европейската служба за външна дейност;

ix) Европейския икономически и социален комитет;

x) Европейския комитет на регионите;

xi) Европейската инвестиционна банка;

xii) Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността;

xiii) ENISA;

xiv) Европейския надзорен орган по защита на данните (ЕНОЗД);

xv) Агенцията на Европейския съюз за космическата програма;

б) трима представители, определени от Мрежата от агенции на Съюза (EUAN) въз основа на предложение на нейния Консултативен комитет за ИКТ, за да представляват интересите на органите, службите и агенциите на Съюза, управляващи своя собствена ИКТ среда и различни от посочените в буква а).

Субектите на Съюза, които са представени в МСК, се стремят да постигнат баланс между половете сред определените представители.

4. Членовете на МСК може да се подпомагат от заместник. Председателят може да покани и други представители на субектите на Съюза, посочени в параграф 3, или на други субекти на Съюза да присъстват на заседанията на МСК без право на глас.

5. Ръководителят на CERT-EU и председателите на групата за сътрудничество, мрежата на ЕРИКС и EU-CyCLONe, създадени съответно съгласно членове 14, 15 и 16 от Директива (ЕС) 2022/2555, или техните заместници могат да участват в заседанията на МСК като наблюдатели. В изключителни случаи и в съответствие с вътрешния процедурен правилник на МСК той може да реши друго.

6. МСК приема свой вътрешен процедурен правилник.

7. МСК определя, съответствие със своя вътрешен процедурен правилник, председател измежду своите членове за срок от три години. Заместник-председателят става пълноправен член на МСК за същия срок.

8. МСК провежда заседания най-малко три пъти годишно по инициатива на своя председател, по искане на CERT-EU или по искане на някой от своите членове.

9. Всеки член на МСК има един глас. Решенията на МСК се вземат с обикновено мнозинство, освен ако в настоящия регламент не е предвидено друго. Председателят на МСК не гласува, освен при равен брой гласове, когато председателят може да участва в гласуването с решаващ глас.

10. МСК може да предприема действия чрез опростена писмена процедура, която започва в съответствие със своя вътрешен процедурен правилник. Съгласно тази процедура съответното решение се счита за одобрено в определения от председателя срок, освен ако някой от членовете не направи възражение.

11. Секретариатът на МСК се осигурява от Комисията и се отчита пред председателя на МСК.

12. Представителите, определени от EUAN, предават решенията на МСК на членовете на EUAN. Всеки член на EUAN има право да отправя до тези представители или до председателя на МСК всякакви въпроси, които счита, че трябва да бъдат отнесени до МСК.

13. МСК може да създаде изпълнителен комитет, който да го подпомага в неговата работа, и да му делегира някои от своите задачи и правомощия. МСК утвърждава процедурния правилник на изпълнителния комитет, включително неговите задачи и правомощия, както и мандата на неговите членове.

14. До 8 януари 2025 г. и ежегодно след това МСК представя на Европейския парламент и на Съвета доклад, в който подробно се описва напредъкът, постигнат при прилагането на настоящия регламент, и се посочва по-специално степента на сътрудничество на CERT-EU с неговите партньори във всяка от държавите членки. Докладът представлява част от материалите за двугодишния доклад за състоянието на киберсигурността в Съюза, който се приема съгласно член 18 от Директива (ЕС) 2022/2555.

Член 11

Задачи на МСК

При изпълнение на своите отговорности МСК по-специално:

а) дава насоки на ръководителя на CERT-EU;

б) извършва ефективен мониторинг и надзор върху прилагането на настоящия регламент и оказва подкрепа на субектите на Съюза с цел укрепване на тяхната киберсигурност, включително, когато е целесъобразно, като изисква *ad hoc* доклади от субектите на Съюза и CERT-EU;

в) след стратегическа дискусия приема многогодишна стратегия за повишаване на нивото на киберсигурност в субектите на Съюза, оценява тази стратегия редовно и във всеки случай на всеки пет години, и когато е необходимо, я изменя;

г) установява методиката и организационните аспекти за извършването на доброволни партньорски проверки от субектите на Съюза с цел извличане на поуки от споделения опит, укрепване на взаимното доверие, постигане на високо общо ниво на киберсигурност, както и повишаване на способностите на субектите на Съюза в областта на киберсигурността, като се гарантира, че тези партньорски проверки се извършват от експерти в областта на киберсигурността, определени от субект на Съюза, различен от проверявания субект на Съюза, и че методиката се основава на член 19 от Директива (ЕС) 2022/2555 и, когато е целесъобразно, е адаптирана към субектите на Съюза;

д) одобрява годишната работна програма на CERT-EU въз основа на предложение на ръководителя на CERT-EU и извършва мониторинг на нейното изпълнение;

е) одобрява каталог на услугите на CERT-EU въз основа на предложение на ръководителя на CERT-EU и евентуалните му актуализации;

ж) одобрява годишното финансово планиране на приходите и разходите за дейностите на CERT-EU, включително неговото щатно разписание, въз основа на предложение на ръководителя на CERT-EU;

з) одобрява правилата за споразуменията за нивото на обслужване въз основа на предложение на ръководителя на CERT-EU;

и) разглежда и одобрява годишния доклад, изготвен от ръководителя на CERT-EU, който обхваща дейностите на CERT-EU и управлението на средствата от страна на CERT-EU;

й) одобрява на ключовите показатели за ефективност (КПЕ) по отношение на CERT-EU, които са установени въз основа на предложение на ръководителя на CERT-EU, и извършва мониторинг в тази връзка;

к) одобрява договорености за сътрудничество, споразумения за нивото на обслужване или договори между CERT-EU и други субекти съгласно член 18;

л) приема насоки и препоръки въз основа на предложение на CERT-EU съгласно член 14 и дава указания на CERT-EU за издаване, оттегляне или изменение на предложение за насоки или препоръки или за призив за действие;

м) създава технически консултативни групи с конкретни задачи, които да подпомагат работата на МСК, одобрява техния мандат и определя съответните им председатели;

н) получава и оценява документи и доклади, представени от субектите на Съюза съгласно настоящия регламент, като например оценките на зрелостта по отношение на киберсигурността;

о) улеснява създаването на неформална група на местните служители по киберсигурността на субектите на Съюза, ползваща се с подкрепата на ENISA, с цел обмен на най-добри практики и информация във връзка с прилагането на настоящия регламент;

п) като взема предвид предоставената от CERT-EU информация за установените рискове за киберсигурността и извлечените поуки, извършва мониторинг на адекватността на механизмите за взаимосвързаност между ИКТ средите на субектите на Съюза и дава консултации във връзка с възможни подобрения;

р) изготвя план за управление на киберкризи с цел да окаже подкрепа на оперативно равнище при координираното управление на съществени инциденти, засягащи субекти на Съюза, и да допринесе за редовния обмен на съответна информация, по-специално по отношение на въздействието и тежестта на съществени инциденти и възможните начини за смекчаване на последиците от тях;

с) координира приемането на плановете на отделните субекти на Съюза за управление на киберкризи, посочени в член 9, параграф 2;

т) приема препоръки относно сигурността на веригата на доставки, посочени в член 8, параграф 2, първа алинея, буква м), като взема предвид резултатите от координираните на равнището на Съюза оценки на риска за сигурността на критичните вериги на доставка, посочени в член 22 от Директива (ЕС) 2022/2555, за да окаже подкрепа на субектите на Съюза при приемането на ефективни и пропорционални мерки за управление на рисковете за киберсигурността.

Член 12

Съответствие

1. МСК извършва ефективен мониторинг съгласно член 10, параграф 2 и член 11 на прилагането на настоящия регламент и на приетите насоки, препоръки и призиви за действие от страна на субектите на Съюза. МСК може да поиска от субектите на Съюза информация или документация, необходими за тази цел. За целите на приемането на мерки за постигане на съответствие съгласно настоящия член, когато съответният субект на Съюза е пряко представляван в МСК, този субект на Съюза няма право на глас.

2. Когато МСК установи, че субект на Съюза не прилага ефективно настоящия регламент или отправените съгласно него насоки, препоръки или призиви за действие, той може, без да се засягат вътрешните процедури на съответния субект на Съюза и след като даде на съответния субект на Съюза възможност да представи коментари:

а) да изпрати мотивирано становище на съответния субект на Съюза, съдържащо наблюдаваните пропуски в прилагането на настоящия регламент;

б) да даде насоки на съответния субект на Съюза, след консултация със CERT-EU, за да гарантира, че неговата рамка, мерки за управление на рисковете за киберсигурността, планове за киберсигурност и докладване се привеждат в съответствие с настоящия регламент в рамките на определен срок;

в) да отправи предупреждение за отстраняване на установените недостатъци в рамките на определен срок, включително препоръки за изменение на мерките, приети от съответния субект на Съюза съгласно настоящия регламент;

г) да отправи мотивирано уведомление до съответния субект на Съюза, в случай че недостатъците, установени в отправеното съгласно буква в) предупреждение, не са отстранени в достатъчна степен в рамките на определения срок;

д) да отправи:

i) препоръка за извършване на одит; или

ii) искане за извършване на одит от служба за одит на трето лице;

е) ако е приложимо, да информира Сметната палата, в съответствие с нейния мандат, за твърдяното нарушение;

ж) да отправи препоръка всички държави членки и субекти на Съюза да спрат временно потоците от данни към съответния субект на Съюза.

За целите на първа алинея, буква в) адресатите на предупреждението се ограничават по подходящ начин, когато е необходимо предвид риска за киберсигурността.

Отправените съгласно първа алинея предупреждения и препоръки се насочват към висшето ръководство на съответния субект на Съюза.

3. Когато МСК е приел мерки съгласно параграф 2, първа алинея, букви а) – ж), съответният субект на Съюза предоставя подробни сведения за мерките и действията, предприети за отстраняване на установените от МСК предполагаеми недостатъци. Субектът на Съюза представя тези подробни сведения в разумен срок, който се договаря с МСК.

4. Когато МСК счете, че е налице трайно нарушение на настоящия регламент от страна на субект на Съюза, произтичащо пряко от действия или бездействия на длъжностно лице или друг служител на Съюза, включително на висшето ръководство, МСК изисква от съответния субект на Съюза да предприеме подходящи действия, включително изисква от него да разгледа възможността за предприемането на действия от дисциплинарен характер, в съответствие с правилата и процедурите, установени в Правилника за длъжностните лица, и всякакви други приложими правила и процедури. За тази цел МСК предава необходимата информация на съответния субект на Съюза.

5. Когато субектите на Съюза уведомят, че не са в състояние да спазят сроковете, определени в член 6, параграф 1 и член 8, параграф 1, МСК може в надлежно обосновани случаи, като взема предвид размера на субекта на Съюза, да разреши удължаването на тези срокове.

ГЛАВА IV

CERT-EU

Член 13

Мисия и задачи на CERT-EU

1. Мисията на CERT-EU е да допринася за сигурността на некласифицираната ИКТ среда на субектите на Съюза посредством предоставяне на консултации в областта на киберсигурността, осигуряване на подкрепа за предотвратяването, откриването, действията, смекчаването, реагирането и възстановяването от инциденти и извършването на дейност като техен координационен център за обмен на информация и реагиране при инциденти в областта на киберсигурността.

2. CERT-EU събира, управлява, анализира и обменя информация със субектите на Съюза относно киберзаплахи, уязвимости и инциденти в некласифицираната ИКТ инфраструктура. Той координира реакцията при инциденти на междуинституционално равнище и на равнището на субекта на Съюза, включително като предоставя или координира предоставянето на специализирана оперативна помощ.

3. CERT-EU изпълнява следните задачи с цел подпомагане на субектите на Съюза:

а) оказва подкрепа при прилагането на настоящия регламент и допринася за координацията във връзка с прилагането на настоящия регламент чрез мерките, изброени в член 14, параграф 1, или чрез доклади ad-hoc, поискани от МСК;

б) предлага стандартните услуги на ЕРИКС за субектите на Съюза посредством пакет от услуги за киберсигурност, описани в неговия каталог на услугите (базови услуги);

в) поддържа мрежа от различни партньори с цел оказване подкрепа във връзка с услугите, посочени в членове 17 и 18;

г) насочва вниманието на МСК към всички проблеми, свързани с прилагането на настоящия регламент и с изпълнението на насоките, препоръките и призивите за действие;

д) въз основа на посочената в параграф 2 информация, допринася за ситуационната осведоменост на Съюза по отношение на киберпространството в тясно сътрудничество с ENISA.

е) координира управлението на съществени инциденти;

ж) действа от страна на субектите на Съюза като еквивалент на координатора, определен за целите на координираното оповестяване на уязвимости съгласно член 12, параграф 1 от Директива (ЕС) 2022/2555;

з) извършва, по искане на субект на Съюза, изпреварващо неинвазивно сканиране на публично достъпните мрежови и информационни системи на субект на Съюза.

Информацията, посочена в първа алинея, буква д), се споделя с МСК, мрежата на ЕРИКС и Центъра на Европейския съюз за анализ на информация (EU INTCEN), когато е приложимо и целесъобразно, и при спазване на подходящи условия за поверителност.

4. CERT-EU може в съответствие с член 17 или 18, в зависимост от случая, да си сътрудничи със съответните общности в областта на киберсигурността в рамките на Съюза и неговите държави членки, включително в следните области:

а) готовност, координация при инциденти, обмен на информация и реагиране на техническо равнище при кризи в случаи, свързани със субекти на Съюза;

б) оперативно сътрудничество във връзка с мрежата на ЕРИКС, включително по отношение на взаимопомощта;

в) разузнавателни данни за киберзаплахи, включително ситуационна осведоменост;

г) по всяка тема, за която се изисква експертният технически опит на CERT-EU в областта на киберсигурността.

5. В рамките на своята област на компетентност CERT-EU участва в структурирано сътрудничество с ENISA с цел изграждане на капацитет, оперативно сътрудничество и дългосрочни стратегически анализи на киберзаплахите в съответствие с Регламент (ЕС) 2019/881. CERT-EU може да си сътрудничи и да обменя информация с Европейския център за борба с киберпрестъпността на Европол.

6. CERT-EU може да предоставя следните услуги, които не са описани в неговия каталог на услугите (услуги, за които се събира такса):

а) услуги за оказване на подкрепа във връзка с киберсигурността на ИКТ средата на субекти на Съюза, различни от посочените в параграф 3, въз основа на споразумения за нивото на обслужване и в зависимост от наличните ресурси, по-специално многостранен мониторинг на мрежите, включително 24-часов мониторинг 7 дни в седмицата на първа линия за киберзаплахи със сериозни последици;

б) услуги за оказване на подкрепа във връзка със свързани с киберсигурността операции или проекти на субекти на Съюза, различни от насочените към защитата на тяхната ИКТ среда, въз основа на писмени споразумения и с предварителното одобрение на МСК;

в) при поискване – изпреварващо сканиране на мрежовите и информационните системи на съответния субект на Съюза с цел откриване на уязвимости с възможно значително въздействие;

г) услуги за оказване на подкрепа във връзка със сигурността на ИКТ средата на организации, различни от субектите на Съюза, които си сътрудничат тясно със субектите на Съюза, например чрез възлагане на задачи или отговорности съгласно правото на Съюза, въз основа на писмени споразумения и с предварителното одобрение на МСК.

По отношение на първа алинея, буква г) CERT-EU може по изключение да сключва споразумения за нивото на обслужване с образувания, различни от субектите на Съюза, с предварително одобрение от МСК.

7. CERT-EU организира и може да участва в учения в областта на киберсигурността или да препоръчва участие в съществуващи учения, когато е целесъобразно - в тясно сътрудничество с ENISA, с цел проверка на нивото на киберсигурност на субектите на Съюза.

8. CERT-EU може да предоставя помощ на субектите на Съюза във връзка с инциденти в мрежови и информационни системи, работещи с КИЕС, когато съответните субекти на Съюза изрично поискат това съгласно своите съответни процедури. Предоставянето на помощ от CERT-EU съгласно настоящия параграф не засяга приложимите правила относно защитата на класифицирана информация.

9. CERT-EU уведомява субектите на Съюза за своите процедури и протоколи за действия при инциденти.

10. CERT-EU представя, с висока степен на поверителност и надеждност и чрез подходящи механизми за сътрудничество и канали на докладване, относима и анонимизирана информация за съществените инциденти и начина, по който са третирани. Тази информация се включва в доклада, посочен в член 10, параграф 14.

11. CERT-EU, в сътрудничество с ЕНОЗД, оказва подкрепа на съответните субекти на Съюза при справянето с инциденти, водещи до нарушаване на сигурността на личните данни, без да се засягат компетентността и задачите на ЕНОЗД като надзорен орган съгласно Регламент (ЕС) 2018/1725.

12. CERT-EU може, ако това е изрично поискано от съответните отговарящи за политиката отдели на субектите на Съюза, да предоставя технически консултации или информация във връзка със съответните въпроси на политиката.

Член 14

Насоки, препоръки и призиви за действие

1. CERT-EU оказва подкрепа при прилагането на настоящия регламент, като отправя:

а) призиви за действие, в които се описват спешни мерки за сигурност, които субектите на Съюза настоятелно се призовават да предприемат в рамките на определен срок;

б) предложения до МСК за насоки, насочени към всички субекти на Съюза или към част от тях;

в) предложения до МСК за препоръки, насочени към отделни субекти на Съюза.

По отношение на първа алинея, буква а) след получаване на призива за действие съответният субект на Съюза без необосновано забавяне информира CERT-EU за начина, по който са приложени спешните мерки за сигурност.

2. Насоките и препоръките може да включват:

а) общи методики и модел за оценка на зрелостта по отношение на киберсигурността на субектите на Съюза, включително съответните скали или КПЕ, които служат като отправна точка в подкрепа на постоянното подобряване на киберсигурността във всички субекти на Съюза и улесняват определянето на приоритета на областите и мерките за киберсигурност, като се взема предвид състоянието на киберсигурността на субектите;

б) правилата или подобренията във връзка с управлението на риска за киберсигурността, както и мерките за управление на рисковете за киберсигурността;

в) правилата за оценките на зрелостта по отношение на киберсигурността и плановете за киберсигурност;

г) когато е целесъобразно, използването на обща технология, отворен код и архитектура и свързаните с тях най-добри практики с цел постигане на оперативна съвместимост и общи стандарти, включително координиран подход към сигурността на веригите за доставка;

д) когато е целесъобразно, информация за улесняване на използването на инструменти за съвместно възлагане на поръчки за закупуването на съответните услуги и продукти в областта на киберсигурността от доставчици, които са трети лица;

е) правила за обмен на информация съгласно член 20.

Член 15

Ръководител на CERT-EU

1. Комисията назначава ръководителя на CERT-EU, след като получи одобрението на мнозинство от две трети от членовете на МСК. На всички етапи на процедурата по назначаване на ръководителя на CERT-EU се провеждат консултации с МСК, по-специално по отношение на изготвянето на обявленията за свободна длъжност, разглеждането на кандидатурите и назначаването на комисии за подбор във връзка с длъжността. Процедурата за подбор, включително окончателният списък с кандидати, от който ще бъде назначен ръководителят на CERT-EU, трябва да гарантира справедлива представеност на всеки пол, като се вземат предвид подадените кандидатури.

2. Ръководителят на CERT-EU отговаря за правилното функциониране на CERT-EU и действа в рамките на функциите си и под ръководството на МСК. Ръководителят на CERT-EU докладва редовно на председателя на МСК и представя ad hoc доклади на МСК по негово искане.

3. Ръководителят на CERT-EU подпомага отговорния оправомощен разпоредител с бюджетни кредити при изготвянето на годишния отчет за дейността, съдържащ финансова информация и информация за управлението, включително резултатите от контрола, изготвян съгласно член 74, параграф 9 от Регламент (ЕС, Евратом) 2018/1046 на Европейския парламент и на Съвета ([9]), и редовно докладва на оправомощения разпоредител с бюджетни кредити за изпълнението на мерките, по отношение на които са били делегирани правомощия на ръководителя на CERT-EU.

4. Ръководителят на CERT-EU изготвя ежегодно финансов план на административните приходи и разходи за дейностите му, предложение за годишна работна програма, предложение за каталог на услугите на CERT-EU, предложения за преразглеждане на каталога на услугите, предложение за правила за споразуменията за нивото на обслужване и предложение за КПЕ за CERT-EU, които се одобряват от МСК в съответствие с член 11. При преразглеждането на списъка на услугите в каталога на услугите на CERT-EU ръководителят на CERT-EU взема предвид разпределените на CERT-EU ресурси.

5. Най-малко веднъж годишно ръководителят на CERT-EU представя на МСК и на председателя на МСК доклади относно дейността и резултатите от дейността на CERT-EU по време на референтния период, включително относно изпълнението на бюджета, сключените споразумения за нивото на обслужване и писмени споразумения, сътрудничеството с различни партньори и предприетите от персонала задания, включително докладите, посочени в член 11. Тези доклади включват работна програма за следващия период, финансово планиране на приходите и разходите, включително щатното разписание, планирани актуализации на каталога с услуги на CERT-EU и оценка на очакваното въздействие, което тези актуализации могат да окажат по отношение на финансовите и човешките ресурси.

Член 16

Финансови въпроси и въпроси, свързани с персонала

1. CERT-EU се включва в административната структура на една от генералните дирекции на Комисията, за да се ползва от структурите на Комисията за подкрепа при административната дейност, финансовото управление и счетоводството, като същевременно запазва положението си на автономен междуинституционален доставчик на услуги за всички субекти на Съюза. Комисията информира МСК за мястото на CERT-EU в административната структура, както и за всички промени във връзка с това. Комисията прави редовен преглед на административните правила, свързани със CERT-EU, и във всеки случай преди установяването на всяка многогодишна финансова рамка съгласно член 312 ДФЕС, за да даде възможност за предприемане на подходящи действия. Прегледът включва разглеждане на възможността за учредяване на CERT-EU като служба на Съюза.

2. По отношение на прилагането на административните и финансовите процедури ръководителят на CERT-EU действа под ръководството на Комисията и под надзора на МСК.

([9]) 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).

3. Задачите и дейностите на CERT-EU, включително услугите, предоставяни на субектите на Съюза съгласно член 13, параграфи 3, 4, 5 и 7 и член 14, параграф 1, които се финансират по функцията на многогодишната финансова рамка, предназначена за европейската публична администрация, се финансират чрез отделен бюджетен ред от бюджета на Комисията. Определените за CERT-EU длъжности се описват подробно в бележка под линия към щатното разписание на Комисията.

4. Субектите на Съюза, различни от посочените в параграф 3, правят годишни финансови вноски за дейността на CERT-EU с цел покриване на услугите, предоставяни от CERT-EU съгласно този параграф. Вноските се правят въз основа на насоките, дадени от МСК и договорени между всеки субект на Съюза и CERT-EU в споразуменията за нивото на обслужване. Вноските представляват справедлив и пропорционален дял от общите разходи за предоставените услуги. Те се получават по отделния бюджетен ред, посочен в параграф 3 от настоящия член, като целеви приходи съгласно член 21, параграф 3, буква в) от Регламент (ЕС, Евратом) 2018/1046.

5. Разходите за услугите, предвидени в член 13, параграф 6, се възстановяват от субектите на Съюза, които използват услугите на CERT-EU. Приходите се разпределят по бюджетните редове в подкрепа на разходите.

Член 17

Сътрудничество между CERT-EU и партньори в държавите членки

1. CERT-EU без необосновано забавяне си сътрудничи и обменя информация с партньорите си в държавите членки, по-специално ЕРИКС, определени или създадени съгласно член 10 от Директива (ЕС) 2022/2555, или когато е приложимо, компетентните органи и единните звена за контакт, определени или създадени съгласно член 8 от посочената директива, по отношение на инциденти, киберзаплахи, уязвимости, ситуации, близки до инцидент, евентуални мерки за противодействие, както и най-добри практики, и по всички въпроси от значение за подобряването на защитата на ИКТ средите на субектите на Съюза, включително чрез мрежата на ЕРИКС, посочена в член 15 от Директива (ЕС) 2022/2555. CERT-EU оказва на Комисията подкрепа в мрежата EU-CyCLONe, създадена съгласно член 16 от Директива (ЕС) 2022/2555, във връзка с координираното управление на мащабни киберинциденти и киберкризи.

2. Когато CERT-EU узнае за настъпването на значим инцидент на територията на дадена държава членка, той без забавяне уведомява съответния партньор в тази държава членка в съответствие с параграф 1.

3. При условие че личните данни са защитени в съответствие с приложимото право на Съюза за защита на данните, CERT-EU без необосновано забавяне обменя относима информация за конкретен инцидент с партньорите в държавите членки, за да се улесни откриването на подобни киберзаплахи или инциденти или за да допринесе за анализа на инцидента, без разрешението на засегнатия субект на Съюза. CERT-EU обменя информация за конкретен инцидент, от която става ясна мишената на инцидента, само в някой от следните случаи:

а) засегнатият субект на Съюза дава съгласието си;

б) засегнатият субект на Съюза не е дал съгласие съгласно буква а), но разкриването на това кой е засегнатият субект на Съюза би увеличило вероятността инцидентите другаде да бъдат избегнати или смекчени;

в) засегнатият субект на Съюза вече е оповестил публично, че е бил засегнат.

Решенията за обмен на информация за конкретен инцидент, от която става ясна мишената на инцидента съгласно първа алинея, буква б), се одобряват от ръководителя на CERT-EU. Преди да приеме такова решение, CERT-EU се свързва писмено със засегнатия субект на Съюза, като обяснява ясно как разкриването на това кой е засегнатият субект на Съюза би спомогнало да бъдат избегнати или смекчени инцидентите другаде. Ръководителят на CERT-EU предоставя обяснението и изрично изисква от субекта на Съюза да посочи дали дава съгласието си в рамките на определен срок. Ръководителят на CERT-EU също така информира субекта на Съюза, че с оглед на предоставеното обяснение си запазва правото да разкрие информацията дори при липсата на съгласие. Засегнатият субект на Съюза се уведомява преди разкриването на информацията.

Член 18

Сътрудничество между CERT-EU и други партньори

1. CERT-EU може да си сътрудничи с партньори в Съюза, различни от посочените в член 17, за които се прилагат изискванията на Съюза относно киберсигурността, включително с партньори от конкретни промишлени отрасли, във връзка с инструменти и методи, например техники, тактики, процедури и добри практики, както и във връзка с киберзаплахи и уязвимости. За всяко сътрудничество с такива партньори CERT-EU иска предварително одобрение от МСК във всеки отделен случай. Когато CERT-EU установява сътрудничество с такива партньори, той информира съответните посочени в член 17, параграф 1 партньори в държавата членка, в която се намира партньорът. Когато е приложимо и целесъобразно, това сътрудничество и съответните условия, включително по отношение на киберсигурността, защитата на данните и работата с информация, се установяват в специални договорености за поверителност, като например договори или административни договорености. За договореностите за поверителност не е необходимо предварително одобрение от МСК, но неговият председател трябва да бъде информиран за тях. В случай на спешна и непосредствена нужда от обмен на информация в областта на киберсигурността в интерес на субектите на Съюза или на друго лице, CERT-EU може да извърши такъв обмен със субект, от чиято специфична компетентност, капацитет и експертен опит съществува оправдана необходимост с оглед на получаване на помощ във връзка с такава спешна и непосредствена нужда, дори ако CERT-EU не е постигнал договореност за поверителност с този субект. В такива случаи CERT-EU незабавно информира председателя на МСК и докладва на МСК чрез редовни доклади или заседания.

2. CERT-EU може да си сътрудничи с партньори, като например търговски субекти, включително субекти от конкретни промишлени отрасли, международни организации, национални субекти от държави извън Съюза или отделни експерти, с цел събиране на информация относно общи и конкретни киберзаплахи, ситуации, близки до инцидент, уязвимости и възможни мерки за противодействие. За по-широкообхватно сътрудничество с такива партньори CERT-EU иска предварително одобрение от МСК във всеки отделен случай.

3. CERT-EU може, със съгласието на субекта на Съюза, който е засегнат от инцидент, и при условие че е налице договореност или договор за неразкриване на информация със съответния партньор или сътрудник, да предоставя информация във връзка с конкретния инцидент на различните партньори, посочени в параграфи 1 и 2, единствено с цел да допринесат за неговия анализ.

ГЛАВА V

ЗАДЪЛЖЕНИЯ ЗА СЪТРУДНИЧЕСТВО И ДОКЛАДВАНЕ

Член 19

Работа с информация

1. Субектите на Съюза и CERT-EU спазват задължението за професионална тайна в съответствие с член 339 ДФЕС или равностойни приложими уредби.

2. Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета ([10]) се прилага по отношение на исканията за публичен достъп до документи, съхранявани от CERT-EU, включително предвиденото в посочения регламент задължение за консултация с други субекти на Съюза или, когато е приложимо, с държави членки, когато дадено искане се отнася до техни документи.

3. При работата с информация от страна на субектите на Съюза и CERT-EU се спазват приложимите правила относно информационната сигурност.

([10]) 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).

Член 20

Правила за обмен на информация в областта на киберсигурността

1. Субектите на Съюза могат на доброволна основа да уведомяват CERT-EU и да му предоставят информация за инциденти, киберзаплахи, ситуации, близки до инциденти, и уязвимости, които ги засягат. CERT-EU осигурява наличието на ефикасни средства за комуникация с високо равнище на проследимост, поверителност и надеждност с цел улесняване на споделянето на информация със субектите на Съюза. При обработването на уведомленията CERT-EU може да обработва задължителните уведомления с предимство пред доброволните уведомления. Без да се засяга член 12, доброволното уведомяване не води до налагането на никакви допълнителни задължения за подалия уведомлението субект на Съюза, които той не би имал, ако не беше подал уведомлението.

2. За да изпълнява мисията и задачите си, възложени съгласно член 13, CERT-EU може да поиска от субектите на Съюза да му предоставят информация от регистрите на съответните си ИКТ системи, включително информация, свързана с киберзаплахи, ситуации, близки до инциденти, уязвимости, показатели за нарушаване на сигурността, предупреждения във връзка с киберсигурността и препоръки относно конфигурацията на инструментите за киберсигурност за откриване на инциденти. Субектът на Съюза, към който е отправено искането, предава исканата информация и всички нейни последващи актуализации без необосновано забавяне.

3. CERT-EU може да обменя със субектите на Съюза информация за конкретен инцидент, която разкрива кой е субектът на Съюза, засегнат от инцидента, при условие че засегнатият субект е дал съгласие за това. Когато субект на Съюза откаже да даде съгласието си, той представя на CERT-EU мотивите, обосноваващи това решение.

4. При поискване субектите на Съюза споделят информация с Европейския парламент и Съвета относно изготвянето на плановете за киберсигурност.

5. При поискване МСК или CERT-EU, в зависимост от случая, споделят насоки, препоръки и призиви за действие с Европейския парламент и Съвета.

6. Задълженията за споделяне, предвидени в настоящия член, не обхващат:

а) КИЕС;

б) информация, чието по-нататъшно разпространение е изключено чрез видима маркировка, освен ако споделянето ѝ със CERT-EU не е било изрично разрешено.

Член 21

Задължения за докладване

1. За значим се счита инцидент, който:

а) е причинил или може да причини сериозно оперативно смущение във функционирането на съответния субект на Съюза или финансови щети за посочения субект;

б) е засегнал или може да засегне други физически или юридически лица, като причини значителни имуществени или неимуществени вреди.

2. Всички субекти на Съюза подават до CERT-EU:

а) без необосновано забавяне и при всички случаи в рамките на 24 часа след узнаването за значимия инцидент – ранно предупреждение, в което, когато е приложимо, се посочва предположението, че значимият инцидент се дължи на незаконосъобразни или злонамерени действия или би могъл да има въздействие върху различни субекти или трансгранично въздействие;

б) без необосновано забавяне и при всички случаи в рамките на 72 часа след узнаването за значимия инцидент – уведомление за инцидент, в което, когато е приложимо, се актуализира информацията, посочена в буква а), и се съдържа първоначална оценка на значимия инцидент, включително неговата тежест и въздействие, както и, когато има такива, показателите за нарушение на сигурността;

в) по искане на CERT-EU – междинен доклад за съответните актуализации на положението;

г) окончателен доклад не по-късно от един месец след подаването на уведомлението за инцидента по буква б), включващ следното:

i) подробно описание на инцидента, включително неговата тежест и въздействие;

ii) вида на заплахата или причината, която вероятно е породила инцидента;

iii) приложените и текущите мерки за ограничаване;

iv) когато е приложимо, трансграничното въздействие на инцидента или въздействието му върху различни субекти;

д) в случай на продължаващ инцидент към момента на представяне на окончателния доклад, посочен в буква г), доклад за текущия напредък и окончателен доклад в рамките на един месец от предприемането на действия във връзка с инцидента.

3. Без необосновано забавяне и при всички случаи в рамките на 24 часа от узнаването за значим инцидент субектът на Съюза информира всички съответни партньори в държавата членка, посочени в член 17, параграф 1, в държавата членка, в която се намира, че е възникнал значим инцидент.

4. Субектите на Съюза уведомяват, наред с другото, за всяка информация, която дава възможност на CERT-EU да определи въздействието върху различните субекти, въздействието върху държавата членка домакин или трансграничното въздействие след значим инцидент. Без да се засяга член 12, актът на уведомяване сам по себе си не води до повишена отговорност за субекта на Съюза.

5. Когато е приложимо, субектите на Съюза съобщават без необосновано забавяне на ползвателите на засегнатите мрежови и информационни системи или на други компоненти на ИКТ средата, че е възможно да са засегнати от значим инцидент или значителна киберзаплаха, и когато е целесъобразно, че трябва да предприемат смекчаващи мерки, всякакви други мерки или корективни мерки, които могат да предприемат в отговор на този инцидент или заплаха. Когато е целесъобразно, субектите на Съюза информират тези ползватели за самата значителна киберзаплаха.

6. Когато значим инцидент или значителна киберзаплаха засяга мрежова и информационна система или компонент от ИКТ средата на субект на Съюза, за която е известно, че е свързана с ИКТ средата на друг субект на Съюза, CERT-EU отправя съответно предупреждение във връзка с киберсигурността.

7. Субектите на Съюза предоставят на CERT-EU, по негово искане и без необосновано забавяне, цифрова информация, създадена чрез използването на електронните устройства, засегнати от съответните инциденти. CERT-EU може да предостави допълнителни подробни сведения за видовете информация, която му е необходима за постигане на ситуационна осведоменост и за реагиране при инциденти.

8. На всеки три месеца CERT-EU представя на МСК, ENISA, EU INTCEN и мрежата на ЕРИКС обобщен доклад, включващ анонимизирани и обобщени данни относно значимите инциденти, инциденти, киберзаплахи, ситуации, близки до инциденти, и уязвимости съгласно член 20, и значимите инциденти, за които е уведомен съгласно параграф 2 от настоящия член. Обобщеният доклад представлява част от материалите за двугодишния доклад за състоянието на киберсигурността в Съюза, който се приема съгласно член 18 от Директива (ЕС) 2022/2555.

9. До 8 юли 2024 г. МСК отправя насоки или препоръки, в които допълнително се конкретизират правилата, както и формата и съдържанието на докладването съгласно настоящия член. При изготвянето на тези насоки или препоръки МСК взема предвид всички актове за изпълнение, приети съгласно член 23, параграф 11 от Директива (ЕС) 2022/2555, в които се определят видът на информацията, форматът и процедурата за уведомленията. CERT-EU разпространява подходящите технически подробни сведения, които дават възможност за изпреварващо откриване и реагиране на инциденти или за предприемане на смекчаващи мерки от страна на субектите на Съюза.

10. Задълженията за докладване, предвидени в настоящия член, не обхващат:

а) КИЕС;

б) информация, чието по-нататъшно разпространение е изключено чрез видима маркировка, освен ако споделянето ѝ със CERT-EU не е било изрично разрешено.

Член 22

Координация и сътрудничество при реагиране на инциденти

1. При извършването на дейността му като координационен център за обмен на информация и реагиране при инциденти в областта на киберсигурността CERT-EU улеснява обмена на информация по отношение на инциденти, киберзаплахи, уязвимости и ситуации, близки до инциденти, между:

а) субектите на Съюза;

б) партньорите, посочени в членове 17 и 18.

2. CERT-EU, когато е целесъобразно – в тясно сътрудничество с ENISA, улеснява координацията между субектите на Съюза във връзка с реагирането при инциденти, което включва:

а) принос за съгласувани външни комуникации;

б) взаимна подкрепа, като например споделяне на информация, която е от значение за субектите на Съюза, или предоставяне на помощ, когато е целесъобразно - пряко на място;

в) оптимално използване на оперативните ресурси;

г) координация с други механизми за реакция при кризи на равнището на Съюза.

3. В тясно сътрудничество с ENISA CERT-EU оказва подкрепа на субектите на Съюза по отношение на ситуационната осведоменост във връзка с инциденти, киберзаплахи, уязвимости и ситуации, близки до инцидент, както и при споделяне на съответните промени в областта на киберсигурността.

4. До 8 януари 2025 г., въз основа на предложение от CERT-EU, МСК приема насоки или препоръки относно координацията и сътрудничеството при реагиране на значими инциденти. Когато се подозира, че даден инцидент е престъпен по своя характер, CERT-EU предоставя консултации във връзка с начина за подаване на сигнал във връзка с инцидента на правоприлагащите органи без необосновано забавяне.

5. След конкретно искане от държава членка и с одобрението на съответните субекти на Съюза CERT-EU може да се обърне към експертите от списъка, посочен в член 23, параграф 4, за да допринесат за реакцията при съществен инцидент с въздействие в тази държава членка или мащабен киберинцидент в съответствие с член 15, параграф 3, буква ж) от Директива (ЕС) 2022/2555. Специалните правила за достъп и използване на технически експерти от субектите на Съюза се одобряват от МСК въз основа на предложение на CERT-EU.

Член 23

Управление на съществени инциденти

1. За да окаже подкрепа на оперативно равнище при координираното управление на съществени инциденти, засягащи субекти на Съюза, и да допринесе за редовния обмен на относима информация между субектите на Съюза и с държавите членки, МСК разработва съгласно член 11, буква р) план за управление на киберкризи въз основа на дейностите, описани в член 22, параграф 2, в тясно сътрудничество със CERT-EU и ENISA. Планът за управление на киберкризи включва най-малко следните елементи:

а) правила относно координацията и информационния поток между субектите на Съюза за управлението на съществени инциденти на оперативно равнище;

б) общи стандартни оперативни процедури (СОП);

в) обща таксономия за тежестта на съществените инциденти и за точките, които могат да доведат до криза;

г) редовни учения;

д) сигурни канали за комуникация, които да се използват.

2. В съответствие с плана за управление на киберкризи, изготвен съгласно параграф 1 от настоящия член, и без да се засяга член 16, параграф 2, първа алинея от Директива (ЕС) 2022/2555, представителят на Комисията в МСК е звеното за контакт за споделяне на относима информация във връзка със съществени инциденти с EU-CyCLONe.

3. CERT-EU координира управлението на съществени инциденти от субектите на Съюза. Той поддържа опис на наличния технически експертен опит, който би бил необходим при реагиране на инциденти в случай на съществени инциденти, и подпомага МСК при координирането на плановете на субектите на Съюза за управление на киберкризи в случай на съществени инциденти, посочени в член 9, параграф 2.

4. Субектите на Съюза допринасят за изготвянето на описа на техническия експертен опит, като предоставят ежегодно актуализиран списък на наличните в техните организации експерти с подробно описание на техните специфични технически умения.

ГЛАВА VI

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 24

Първоначално преразпределяне на бюджета

За да се гарантира правилното и стабилно функциониране на CERT-EU, Комисията може да предложи преразпределяне на персонал и финансови ресурси към бюджета на Комисията, които да се използват за операции на CERT-EU. Преразпределянето се извършва едновременно с първия годишен бюджет на Съюза, който се приема след влизането в сила на настоящия регламент.

Член 25

Преглед

1. До 8 януари 2025 г. и ежегодно след това МСК, със съдействието на CERT-EU, докладва на Комисията за прилагането на настоящия регламент. МСК може да отправя препоръки към Комисията във връзка с прегледа на настоящия регламент.

2. До 8 януари 2027 г. и на всеки две години след това Комисията оценява прилагането на настоящия регламент и представя на Европейския парламент и на Съвета доклад за прилагането на настоящия регламент и за опита, придобит на стратегическо и оперативно равнище.

В доклада, посочен в първа алинея от настоящия параграф, се включват резултатите от прегледа, посочен в член 16, параграф 1, относно възможността за учредяване на CERT-EU като служба на Съюза.

3. В срок до 8 януари 2029 г. Комисията извършва оценка на функционирането на настоящия регламент и докладва на Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите. Комисията оценява също така целесъобразността в обхвата на настоящия регламент да бъдат включени мрежовите и информационните системи, работещи с КИЕС, като взема предвид други законодателни актове на Съюза, приложими за тези системи. Ако е необходимо, докладът се придружава от законодателно предложение.

Член 26

Влизане в сила

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

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

Съставено в Страсбург на 13 декември 2023 година.

За Европейския парламент	*За Съвета*
Председател	*Председател*
R. METSOLA	P. NAVARRO RÍOS