2024/1366

24.5.2024 г.

ДЕЛЕГИРАН РЕГЛАМЕНТ (ЕС) 2024/1366 НА КОМИСИЯТА

от 11 март 2024 година

за допълнение на Регламент (ЕС) 2019/943 на Европейския парламент и на Съвета чрез установяване на мрежов кодекс относно специфични за сектора правила за свързаните с киберсигурността аспекти на трансграничните потоци на електроенергия

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) 2019/943 на Европейския парламент и на Съвета от 5 юни 2019 г. относно вътрешния пазар на електроенергия ([1]), и по-специално член 59, параграф 2, буква д) от него,

като има предвид, че:

(1) Управлението на рисковете за киберсигурността е от решаващо значение за поддържане на сигурността на електроснабдяването и за осигуряване на високо равнище на киберсигурност в електроенергетиката.

(2) Цифровизацията и киберсигурността имат решаващо значение за предоставянето на основни услуги и следователно са от стратегическо значение за критичната енергийна инфраструктура.

(3) В Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета ([2]) са определени мерки за високо общо ниво на киберсигурност в Съюза. С Регламент (ЕС) 2019/941 на Европейския парламент и на Съвета ([3]) се допълва Директива (ЕС) 2022/2555, като се гарантира, че киберинцидентите в електроенергетиката правилно се определят като риск и че на мерките, предприети за справяне с тях, се обръща достатъчно внимание в плановете за готовност за справяне с рисковете. С Регламент (ЕС) 2019/943 се допълват Директива (ЕС) 2022/2555 и Регламент (ЕС) 2019/941, като се определят специфични правила, засягащи електроенергетиката на равнището на Съюза. Освен това с настоящия делегиран регламент се допълват разпоредбите на Директива (ЕС) 2022/2555 по отношение на електроенергетиката, когато става въпрос за трансгранични потоци на електроенергия.

(4) В контекста на взаимосвързаните цифровизирани електроенергийни системи предотвратяването и управлението на криза в електроснабдяването, свързана с кибератаки, не може да се счита за задача, която може да бъде изпълнявана единствено на национално равнище. Необходимо е да се разгърне пълният потенциал на по-ефективни и не толкова скъпи мерки чрез регионално сътрудничество и сътрудничество в рамките на Съюза. Ето защо са необходими обща рамка от правила и по-добре координирани процедури, за да се гарантира, че държавите членки и другите участници са в състояние да си сътрудничат ефективно през границите в условията на засилена прозрачност, доверие и солидарност между държавите членки и компетентните органи, отговарящи за електроенергията и киберсигурността.

(5) Управлението на рисковете за киберсигурността в обхвата на настоящия регламент изисква структуриран процес, включващ, наред с другото, установяване на рисковете за трансграничните потоци на електроенергия, произтичащи от кибератаки, свързаните с тях оперативни процеси и периметри, съответните мерки за контрол във връзка с киберсигурността и механизми за проверка. Макар че графикът на целия процес е разпределен в продължение на години, всяка стъпка от него следва да допринася за високо общо ниво на киберсигурност в сектора и за намаляване на рисковете за киберсигурността. Всички участници в процеса следва да положат максимални усилия за разработване и съгласуване на методиките възможно най-скоро, без неоправдано забавяне, и във всички случаи не по-късно от крайните срокове, определени в настоящия регламент.

([1]) ОВ L 158, 14.6.2019 г., стр. 54.

([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 МИС 2) (ОВ L 333, 27.12.2022 г., стр. 80).

([3]) Регламент (ЕС) 2019/941 на Европейския парламент и на Съвета от 5 юни 2019 г. за готовност за справяне с рискове в електроенергийния сектор и за отмяна на Директива 2005/89/ЕО (ОВ L 158, 14.6.2019 г., стр. 1).

(6) Оценките на рисковете за киберсигурността на равнището на Съюза, на държавите членки, на регионите и на субектите в настоящия регламент може да бъдат ограничени до рисковете, произтичащи от кибератаки съгласно определението в Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета ([4]), като по този начин се изключват например физическите атаки, природните бедствия и прекъсвания на електроснабдяването поради загуба на съоръжения или човешки ресурси. Общоевропейските и регионалните рискове, свързани с физически атаки или природни бедствия в сферата на електроенергетиката, вече са обхванати от друго съществуващо законодателство на Съюза, включително член 5 от Регламент (ЕС) 2019/941 или Регламент (ЕС) 2017/1485 на Комисията ([5]) за установяване на насоки относно експлоатацията на системата за пренос на електроенергия. По подобен начин Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета ([6]) за устойчивостта на критичните субекти има за цел да намали уязвимостите и да укрепи физическата устойчивост на критичните субекти и обхваща всички съответни природни и антропогенни рискове, които може да засегнат предоставянето на основни услуги, включително произшествия, природни бедствия, извънредни ситуации, свързани с общественото здраве, например пандемии и хибридни заплахи или други враждебни заплахи, включително терористични престъпления, проникване на престъпни елементи и саботаж.

(7) Понятието „субекти с голямо въздействие и с критично въздействие“ в настоящия регламент е от основно значение за определяне на обхвата на субектите, които ще подлежат на задълженията, описани в регламента. Основаният на риска подход, изложен в различните разпоредби, има за цел да установи процесите, спомагателните активи и субектите, които ги управляват и които оказват влияние върху трансграничните потоци на електроенергия. В зависимост от степента на въздействие на евентуалните кибератаки върху техните операции, свързани с трансграничните потоци на електроенергия, те може да се разглеждат като субекти „с голямо въздействие“ или като такива „с критично въздействие“. В член 3 от Директива (ЕС) 2022/2555 се определят понятията за съществени и важни субекти, както и критериите за определяне на субектите от тези категории. Въпреки че много от тях ще бъдат разглеждани и определяни едновременно като „съществени“ по смисъла на член 3 от Директива (ЕС) 2022/2555 и като такива с голямо или с критично въздействие съгласно член 24 от настоящия регламент, критериите, изложени в настоящия регламент, се отнасят само до тяхната роля и въздействие в процесите в сферата на електроенергията, засягащи трансграничните потоци, без да се вземат предвид критериите, определени в член 3 от Директива (ЕС) 2022/2555.

(8) Субектите в обхвата на настоящия регламент, считани за субекти с голямо или с критично въздействие съгласно член 24 от настоящия регламент и подлежащи на предвидените в него задължения, са предимно тези, които оказват пряко въздействие върху трансграничните потоци на електроенергия в ЕС.

(9) В настоящият регламент се използват съществуващите механизми и инструменти, които вече са установени в други законодателни актове, за да се осигури ефективност и да се избегне дублиране при постигането на целите.

(10) При прилагането на настоящия регламент държавите членки, съответните органи и системните оператори следва да вземат предвид договорените европейски стандарти и техническите спецификации на европейските организации за стандартизация и да действат в съответствие със законодателството на Съюза, свързано с пускането на пазара или пускането в експлоатация на продукти, попадащи в обхвата на това законодателство на Съюза.

([4]) Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 (ОВ L 333, 27.12.2022 г., стр. 1).

([5]) Регламент (ЕС) 2017/1485 на Комисията от 2 август 2017 година за установяване на насоки относно експлоатацията на системата за пренос на електроенергия (ОВ L 220, 25.8.2017 г., стр. 1).

([6]) Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14 декември 2022 година за устойчивостта на критичните субекти и за отмяна на Директива 2008/114/ЕО на Съвета (ОВ L 333, 27.12.2022 г., стр. 164).

(11) С оглед на намаляването на рисковете за киберсигурността е необходимо да се създаде подробен правилник, който да урежда действията и сътрудничеството между съответните заинтересовани страни, чиито дейности се отнасят до свързаните с киберсигурността аспекти на трансграничните потоци на електроенергия, с цел да се гарантира сигурността на системата. Тези организационни и технически правила следва да гарантират, че повечето произшествия в електроснабдяването с първопричини, свързани с киберсигурността, се отстраняват ефективно на оперативно равнище. Необходимо е да се определи какво трябва да направят тези съответни заинтересовани страни, за да предотвратят такива кризи, и какви мерки могат да предприемат, ако правилата за експлоатация на системата сами по себе си вече не са достатъчни. Ето защо е необходимо да се създаде обща рамка от правила за това как да се предотвратяват едновременни кризи в електроснабдяването, чиято първопричина е киберсигурността, как да се изгради подготвеност за тях и как те да бъдат управлявани. По този начин се постига по-голяма прозрачност на етапа на подготовка и по време на едновременна криза в електроснабдяването и се гарантира, че мерките се предприемат по координиран и ефективен начин заедно с компетентните органи по киберсигурността в държавите членки. От държавите членки и съответните субекти следва да се изисква да си сътрудничат в дух на солидарност на регионално равнище и, когато е приложимо, на двустранен принцип. Целта на това сътрудничество и правила е да се постигне по-добра готовност за справяне с рискове за киберсигурността на по-ниска цена, което е в съответствие и с целите на Директива (ЕС) 2022/2555. Необходимо е също така да се укрепи вътрешният пазар на електроенергия, като се повиши доверието между държавите членки, и по-специално да се намали рискът от неоправдано ограничаване на трансграничните потоци на електроенергия, като по този начин се намали рискът от разпространение на отрицателни последици върху съседните държави членки.

(12) Сигурността на електроснабдяването предполага ефективно сътрудничество между държавите членки, институциите, органите, бюрата и агенциите на Съюза, както и съответните заинтересовани страни. Операторите на разпределителни системи и операторите на преносни системи играят ключова роля в осигуряването на сигурна, надеждна и ефективна електроенергийна система в съответствие с член 31 и член 40 от Директива (ЕС) 2019/944 на Европейския парламент и на Съвета ([7]). Различните регулаторни органи и други съответни компетентни национални органи също играят важна роля в осигуряването и наблюдението на киберсигурността в рамките на електроснабдяването като част от задачите им, възложени с Директива (ЕС) 2019/944 и Директива (ЕС) 2022/2555. Държавите членки следва да определят съществуващ или нов субект като свой компетентен национален орган за прилагането на настоящия регламент, с цел да се гарантират прозрачното и приобщаващо участие на всички заинтересовани страни, ефективната подготовка и правилното му прилагане, сътрудничеството между различните заинтересовани страни и компетентни органи в областта на електроенергетиката и киберсигурността, както и да се улеснят предотвратяването и последващото оценяване на електроенергийни кризи с първопричини в областта на киберсигурността и обменът на информация във връзка с тях.

(13) Когато субект с голямо или с критично въздействие предоставя услуги в повече от една държава членка или има седалище, друго място на стопанска дейност или представител в една държава членка, но неговата мрежа и информационните му системи се намират в една или повече други държави членки, тези държави членки следва да насърчават съответните си компетентни органи да положат максимални усилия да си сътрудничат и да си оказват взаимно необходимото съдействие.

(14) Държавите членки следва да гарантират, че компетентните органи разполагат с необходимите правомощия по отношение на субекти с голямо въздействие и с критично въздействие, за да насърчават спазването на настоящия регламент. Тези правомощия следва да позволяват на компетентните органи да извършват проверки на място или надзор от разстояние. Това може да включва случайни проверки, извършване на редовни одити, целенасочени одити на сигурността въз основа на оценки на риска или налична информация, свързана с риска, и сканиране на сигурността въз основа на обективни, недискриминационни, справедливи и прозрачни критерии за оценка на рисковете, които включват искане на информация, необходима за оценка на мерките в областта на киберсигурността, приети от субекта. Тази информация следва да включва документирани политики за киберсигурност, данни за достъп, документи или всякаква друга информация, необходима за изпълнението на надзорните им задачи, както и доказателства за изпълнението на политиките за киберсигурност, като например резултатите от одити на сигурността, извършени от квалифициран одитор, и съответните доказателства, на които те се основават.

([7]) Директива (ЕС) 2019/944 на Европейския парламент и на Съвета от 5 юни 2019 г. относно общите правила за вътрешния пазар на електроенергия и за изменение на Директива 2012/27/ЕС (ОВ L 158, 14.6.2019 г., стр. 125).

(15) За да се избегнат празнини в задълженията за управление на рисковете за киберсигурността, наложени на субекти с голямо въздействие и с критично въздействие, или тяхното дублиране, националните органи съгласно Директива (ЕС) 2022/2555 и компетентните органи съгласно настоящия регламент следва да си сътрудничат във връзка с прилагането на мерки за управление на рисковете за киберсигурността и надзора на спазването на тези мерки на национално равнище. Съответствието на даден субект с изискванията за управление на рисковете за киберсигурността, установени в настоящия регламент, може да се счита от компетентните органи съгласно Директива (ЕС) 2022/2555 за спазване на съответните изисквания, установени в посочената директива, или обратното.

(16) Общият подход към предотвратяването и управлението на едновременни кризи в електроснабдяването изисква общо разбиране между държавите членки за това какво представлява едновременната криза в електроснабдяването и кога кибератаката е важен фактор за нея. По-специално, следва да се улесни координацията между държавите членки и съответните субекти с цел справяне със ситуация, при която съществува или непосредствено предстои потенциален риск от значителен недостиг на електроенергия или невъзможност за електроснабдяване на потребителите, и то поради кибератака.

(17) В съображение 1 от Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета ([8]) се признава жизненоважната роля на мрежите и информационните системи и на електронните съобщителни мрежи и услуги за поддържане на функционирането на икономиката в ключови сектори като енергетиката, а в съображение 44 се обяснява, че Агенцията на Европейския съюз за киберсигурност (ENISA) следва да поддържа връзка с Агенцията на Европейския съюз за сътрудничество между регулаторите на енергия (ACER).

(18) С Регламент (ЕС) 2019/943 на операторите на преносни системи (ОПС) и на операторите на разпределителни системи (ОРС) се възлагат конкретни отговорности по отношение на киберсигурността. Техните европейски сдружения, а именно Европейската мрежа на операторите на преносни системи за електроенергия („ЕМОПС за електроенергия“) и Организацията на операторите на разпределителни системи в Европейския съюз („ООРСЕС“) съгласно съответно членове 30 и 55 от посочения регламент насърчават киберсигурността в сътрудничество със съответните органи и регулирани субекти.

(19) Общият подход към предотвратяването и управлението на едновременни кризи в електроснабдяването с първопричини, свързани с киберсигурността, изисква също така всички съответни заинтересовани страни да използват хармонизирани методи и определения за установяване на рисковете, свързани с киберсигурността на електроснабдяването. Подходът изисква също така възможност за ефективна съпоставка как те и техните съседи се справят в тази област. Поради това е необходимо да се установят процесите, ролите и отговорностите за разработване и актуализиране на методиките за управление на риска, скалите за класифициране на инциденти и мерките в областта на киберсигурността, адаптирани към рисковете за киберсигурността, които оказват влияние върху трансграничните потоци на електроенергия.

(20) Държавите членки чрез компетентния орган, определен за целите на настоящия регламент, отговарят за определянето на субектите, които отговарят на критериите за квалифициране като субекти с голямо въздействие и с критично въздействие. За да се отстранят различията сред държавите членки в това отношение и да се гарантира правна сигурност по отношение на мерките за управление на рисковете за киберсигурността и задълженията за докладване по отношение на всички относими субекти, следва да се установи набор от критерии за определяне на субектите, попадащи в обхвата на настоящия регламент. Този набор от критерии следва да бъде установен и редовно актуализиран през целия процес на разработване и приемане на общите условия и методиките, предвидени в настоящия регламент.

(21) Разпоредбите на настоящия регламент не следва да засягат правото на Съюза, в което се предвиждат специфични правила за сертифициране на продукти на информационните и комуникационните технологии („ИКТ продукти“), ИКТ услуги и ИКТ процеси, по-специално без да се засяга Регламент (ЕС) 2019/881 по отношение на рамката за създаване на европейски схеми за сертифициране на киберсигурността. В контекста на настоящия регламент ИКТ продуктите следва да включват и технически устройства и програмно осигуряване, които позволяват пряко взаимодействие с електротехническата мрежа, по-специално промишлени системи за управление, които могат да се използват за пренос, разпределение и производство на енергия, както и за събиране и предаване на съответната информация. Разпоредбите следва да гарантират, че съответните цели по отношение на сигурността, посочени в член 51 от Регламент (ЕС) 2019/881, се изпълняват от ИКТ продуктите, ИКТ услугите и ИКТ процесите, които ще се закупуват.

([8]) 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).

(22) Неотдавнашните кибератаки показват, че субектите все по-често стават обект на атаки по веригата на доставките. Такива атаки по веригата на доставките оказват въздействие не само върху отделни субекти в обхвата ѝ, но могат да имат и каскаден ефект върху по-големи атаки срещу субекти, с които те са свързани в електроенергийната мрежа. Поради това бяха добавени разпоредби и препоръки, които да спомогнат за намаляване на рисковете за киберсигурността, засягащи процесите, свързани с веригата на доставките, по-специално с обществените поръчки, които оказват влияние върху трансграничните потоци на електроенергия.

(23) Тъй като използването на уязвимости в мрежите и информационните системи може да доведе до значителни енергийни смущения и вреди за икономиката и потребителите, тези уязвимости следва да бъдат бързо установявани и отстранявани, за да се намалят рисковете. За да се улесни ефективното прилагане на настоящия регламент, съответните субекти и компетентните органи следва да си сътрудничат за упражняване и изпробване на дейности, които се считат за подходящи за тази цел, включително обмен на информация относно киберзаплахи, кибератаки, уязвимости, инструменти и методи, тактики, техники и процедури, готовност за управление на кризи в областта на киберсигурността и други учения. Тъй като технологиите се развиват непрекъснато и цифровизацията на електроенергетиката напредва с бързи темпове, прилагането на приетите разпоредби не следва да бъде в ущърб на иновациите и да представлява пречка за достъпа до пазара на електроенергия и последващото използване на иновативни решения, които допринасят за ефективността и устойчивостта на електроенергийната система.

(24) Информацията, събирана с оглед на наблюдението на прилагането на настоящия регламент, следва да бъде разумно ограничена въз основа на принципа „необходимост да се знае“. На заинтересованите страни следва да се предоставят постижими и ефективни крайни срокове за предоставяне на такава информация. Трябва да се избягва двойното уведомяване.

(25) Защитата на киберсигурността се простира отвъд границите на Съюза. За сигурна система се изисква участието на съседни трети държави. Съюзът и неговите държави членки следва да се стремят да подкрепят съседните трети държави, чиято електроенергийна инфраструктура е свързана с европейската електроенергийна мрежа, в прилагането на правила за киберсигурност, подобни на установените в настоящия регламент.

(26) За да се подобри координацията на сигурността на ранен етап и за да се изпробват бъдещите обвързващи правила, общи условия и методики, ЕМОПС за електроенергия, ООРСЕС и компетентните органи следва да започнат да разработват необвързващи насоки веднага след влизането в сила на настоящия регламент. Тези насоки ще послужат като отправна точка за разработването на бъдещите общи условия и методики. Успоредно с това компетентните органи следва да определят субекти, които да кандидатстват за позицията на субекти с голямо и с критично въздействие, за да започнат доброволно да изпълняват предвидените задължения.

(27) Настоящият регламент беше разработен в тясно сътрудничество с ACER, ENISA, ЕМОПС за електроенергия, ООРСЕС и други заинтересовани страни, за да се приемат ефективни, балансирани и пропорционални правила по прозрачен и приобщаващ начин.

(28) С настоящия регламент се допълват и надграждат мерките за управление на кризи, установени в Механизма на ЕС за реакция при кризи в областта на киберсигурността, както е посочено в Препоръка (ЕС) 2017/1584 на Комисията ([9]). Кибератаката може също така да предизвика, да допринесе за или да съвпадне с криза в електроснабдяването съгласно определението в член 2, точка 9 от Регламент (ЕС) 2019/941, като окаже въздействие върху трансграничните потоци на електроенергия. Тази криза в електроснабдяването може да доведе до едновременна криза в електроснабдяването съгласно определението в член 2, точка 10 от Регламент (ЕС) 2019/941. Подобен инцидент би могъл да окаже въздействие и върху други сектори, зависещи от сигурността на електроснабдяването. В случай че подобен инцидент прерасне в мащабен киберинцидент по смисъла на член 16 от Директива (ЕС) 2022/2555, следва да се прилагат разпоредбите на посочения член за създаване на Европейска мрежа за връзка на организациите при киберкризи (EU-CyCLONe). По отношение на управлението на кризи на равнището на Съюза съответните страни следва да разчитат на интегрирани договорености на ЕС за реакция на политическо равнище при криза („договорености за IPCR“) съгласно Решение за изпълнение (ЕС) 2018/1993 на Съвета ([10]).

(29) Настоящият регламент не засяга компетентността на всяка държава членка да предприема необходимите мерки, с които да гарантира защитата на основните интереси на своята сигурност, да опазва реда и обществената сигурност и да създава условия за разследването, разкриването и наказателното преследване на престъпления, в съответствие с правото на Съюза. В съответствие с член 346 от ДФЕС нито една държава членка не може да бъде задължавана да предоставя информация, чието разкриване тя счита за противоречащо на основните интереси на нейната сигурност.

([9]) 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).

([10]) Решение за изпълнение (ЕС) 2018/1993 на Съвета от 11 декември 2018 година относно договорености за интегрирана реакция на ЕС при политическа криза (ОВ L 320, 17.12.2018 г., стр. 28).

(30) Въпреки че настоящият регламент по принцип се прилага за субекти, извършващи дейности по производство на електроенергия от ядрени електроцентрали, някои от тези дейности могат да бъдат свързани с националната сигурност.

(31) За всяко обработване на лични данни съгласно настоящия регламент следва да се прилагат правото на Съюза в областта на защитата на данните и правото на Съюза в областта на неприкосновеността на личния живот. По-специално настоящият регламент не засяга Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([11]), Директива 2002/58/ЕО на Европейския парламент и на Съвета ([12]) и Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([13]). Поради това настоящият регламент не следва да засяга, наред с другото, задачите и правомощията на органите, компетентни да следят за спазването на приложимото правото на Съюза в областта на защитата на данните и правото на Съюза в областта на неприкосновеността на личния живот.

(32) Предвид значението на международното сътрудничество в областта на киберсигурността определените от държавите членки компетентни органи, отговарящи за изпълнението на задачите, възложени им съгласно настоящия регламент, следва да могат да участват в международни мрежи за сътрудничество. Поради това за целите на изпълнението на своите задачи компетентните органи следва да могат да обменят информация, включително лични данни, с компетентните органи на трети държави, при условие че са изпълнени условията съгласно правото на Съюза в областта на защитата на данните за предаването на лични данни на трети държави и наред с другото, условията по член 49 от Регламент (ЕС) 2016/679.

(33) Обработването на лични данни — в степента, необходима и пропорционална за гарантиране на сигурността на мрежовите и информационните системи от субекти с голямо въздействие или с критично въздействие, може да се счита за законосъобразно въз основа на факта, че това обработване е в съответствие с правно задължение, което се прилага спрямо администратора, в съответствие с изискванията на член 6, параграф 1, буква в) и член 6, параграф 3 от Регламент (ЕС) 2016/679. Обработването на лични данни може да бъде необходимо и за основателните интереси, преследвани от субекти с голямо въздействие или с критично въздействие, както и от доставчици на технологии и услуги в областта на сигурността, действащи от името на тези субекти, в съответствие с член 6, параграф 1, буква е) от Регламент (ЕС) 2016/679, включително когато това обработване е необходимо за споразумения за обмен на информация в областта на киберсигурността или за доброволно съобщаване на съответната информация в съответствие с настоящия регламент. Мерки, свързани с предотвратяването, разкриването, идентифицирането, ограничаването, анализирането и реакцията на кибератаки, мерки за повишаване на осведомеността във връзка с конкретни киберзаплахи, обмен на информация в контекста на отстраняване на уязвимостите и координирано разкриване на уязвимостите, доброволен обмен на информация за тези кибератаки и за киберзаплахи и уязвимости, показатели за нарушена сигурност, тактики, техники и процедури, предупреждения във връзка с киберсигурността и инструменти за конфигуриране може да изискват обработването на определени категории лични данни, като например IP адреси, единни ресурсни локатори (URL адреси), имена на домейни, адреси на електронна поща и, когато те разкриват лични данни, електронни времеви печати. Обработването на лични данни от компетентните органи, единните звена за контакт и ЕРИКС може да съставлява правно задължение или да се счита за необходимо за изпълнението на задача от обществен интерес или за упражняването на официалните правомощия, които са предоставени на администратора съгласно член 6, параграф 1, буква в) или д) и член 6, параграф 3 от Регламент (ЕС) 2016/679, или за преследване на основателен интерес на субектите с голямо въздействие или с критично въздействие, както е посочено в член 6, параграф 1, буква е) от посочения регламент. Освен това в националното право може да се определят правила, позволяващи на компетентните органи, единните звена за контакт и ЕРИКС, доколкото това е необходимо и пропорционално за целите на гарантирането на сигурността на мрежите и информационните системи на субектите с голямо въздействие или с критично въздействие, да обработват специални категории лични данни в съответствие с член 9 от Регламент (ЕС) 2016/679, по-специално чрез предвиждане на подходящи и конкретни мерки за защита на основните права и интереси на физическите лица, включително технически ограничения за повторното използване на такива данни и използването на най-съвременни мерки за сигурност и опазване на неприкосновеността на личния живот, като псевдонимизация или криптиране, когато анонимизирането може значително да засегне преследваната цел.

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

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

([13]) Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 година 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).

(34) В много случаи вследствие на кибератаки се засягат лични данни. В този контекст компетентните органи следва да си сътрудничат и да обменят информация относно всички съответни въпроси с органите, посочени в Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО.

(35) Беше проведена консултация с Европейския надзорен орган по защита на данните в съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725, който представи становище на 17 ноември 2023 г.,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Глава I

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет

С настоящия регламент се създава мрежов кодекс, в който се определят специфични за сектора правила за свързаните с киберсигурността аспекти на трансграничните потоци на електроенергия, включително правила за общи минимални изисквания, планиране, наблюдение, докладване, както и за управление на кризи.

Член 2

Приложно поле

1. Настоящият регламент се прилага по отношение на свързаните с киберсигурността аспекти на трансграничните потоци на електроенергия в дейностите на следните субекти, ако те са определени като субекти с голямо въздействие или с критично въздействие в съответствие с член 24:

а) електроенергийни предприятия съгласно определението в член 2, точка 57 от Директива (ЕС) 2019/944;

б) номинирани оператори на пазара на електроенергия („НОПЕ“) съгласно определението в член 2, точка 8 от Регламент (ЕС) 2019/943;

в) „организирани пазари“ съгласно определението в член 2, точка 4 от Регламент за изпълнение (ЕС) № 1348/2014 на Комисията ([14]), които уреждат сделки с продукти, свързани с трансграничните потоци на електроенергия;

г) доставчици на ИКТ услуги с критично въздействие, посочени в член 3, точка 9 от настоящия регламент;

д) ЕМОПС за електроенергия, създадена в съответствие с член 28 от Регламент (ЕС) 2019/943;

е) ООРСЕС, създадена в съответствие с член 52 от Регламент (ЕС) 2019/943;

ж) отговарящи за баланса лица съгласно определението в член 2, точка 14 от Регламент (ЕС) 2019/943;

з) оператори на зарядна точка съгласно определението в приложение I към Директива (ЕС) 2022/2555;

и) регионални координационни центрове („РКЦ“), създадени съгласно член 35 от Регламент (ЕС) 2019/943;

й) доставчици на управлявани услуги за сигурност („ДУУС“) съгласно определението в член 6, точка 40 от Директива (ЕС) 2022/2555;

к) всеки друг субект или трета страна, на които са делегирани или възложени отговорности съгласно настоящия регламент.

2. За изпълнението на задачите, възложени с настоящия регламент, са отговорни следните органи, като част от настоящите им правомощия:

а) Агенцията на Европейския съюз за сътрудничество между регулаторите на енергия (ACER), създадена с Регламент (ЕС) 2019/942 на Европейския парламент и на Съвета ([15]);

б) националните компетентни органи, които отговарят за изпълнението на задачите, възложени им по силата на настоящия регламент, и са определени от държавите членки по силата на член 4, наричани още „компетентни органи“;

в) националните регулаторни органи („НРО“), определени от всяка държава членка в съответствие с член 57, параграф 1 от Директива (ЕС) 2019/944;

([14]) Регламент за изпълнение (ЕС) № 1348/2014 на Комисията от 17 декември 2014 г. за прилагане на член 8, параграфи 2 и 6 от Регламент (ЕС) № 1227/2011 на Европейския парламент и на Съвета относно интегритета и прозрачността на пазара за търговия на едро с енергия по отношение на докладването на данни (ОВ L 363, 18.12.2014 г., стр. 121).

([15]) Регламент (ЕС) 2019/942 на Европейския парламент и на Съвета от 5 юни 2019 година за създаване на Агенция на Европейския съюз за сътрудничество между регулаторите на енергия (преработен текст) (ОВ L 158, 14.6.2019 г., стр. 22).

г) компетентните органи, отговарящи за готовността за справяне с рискове („КО — ГСР“), създадени съгласно член 3 от Регламент (ЕС) 2019/941;

д) екипите за реагиране при инциденти с компютърната сигурност („ЕРИКС“), определени или създадени в съответствие с член 10 от Директива (ЕС) 2022/2555;

е) компетентни органи, отговарящи за киберсигурността („КООКС“), определени или създадени съгласно член 8 от Директива (ЕС) 2022/2555;

ж) Агенцията на Европейския съюз за киберсигурност, създадена съгласно Регламент (ЕС) 2019/881;

з) всички други органи или трети страни, на които са делегирани или възложени отговорности съгласно член 4, параграф 3.

3. Настоящият регламент се прилага и за всички субекти, които не са установени в Съюза, но предоставят услуги на субекти в Съюза, при условие че компетентните органи са ги определили като субекти с голямо въздействие или с критично въздействие в съответствие с член 24, параграф 2.

4. Настоящият регламент не засяга отговорността на държавите членки да опазват националната сигурност и правомощието им да гарантират други основни функции на държавата, включително да осигуряват нейната териториална цялост и да поддържат законността и реда.

5. Настоящият регламент не засяга отговорността на държавите членки да опазват националната сигурност по отношение на дейностите по производство на електроенергия от ядрени електроцентрали, включително дейностите в рамките на веригата за създаване на стойност в сектора на ядрената енергия, в съответствие с Договорите.

6. Субектите, компетентните органи, единните звена за контакт на равнище субект и ЕРИКС обработват лични данни, доколкото това е необходимо за целите на настоящия регламент и в съответствие с Регламент (ЕС) 2016/679, като по-специално това обработване се основава на член 6 от него.

Член 3

Определения

Прилагат се следните определения:

1) „актив“ означава всяка информация, програмно осигуряване или апаратна част в мрежите и информационните системи, независимо дали са материални или нематериални, който или която има стойност за дадено лице, организация или правителство;

2) „компетентен орган, отговарящ за готовността за справяне с рискове“, означава компетентният орган, определен съгласно член 3 от Регламент (ЕС) 2019/941;

3) „екип за реагиране при инциденти с компютърната сигурност“ означава екип, отговарящ за справянето с рискове и предприемането на действия при инциденти в съответствие с член 10 от Директива (ЕС) 2022/2555;

4) „актив с критично въздействие“ означава актив, който е необходим за осъществяването на процес с критично въздействие;

5) „субект с критично въздействие“ означава субект, който осъществява процес с критично въздействие и който е определен от компетентните органи в съответствие с член 24;

6) „периметър на критично въздействие“ означава периметър, определен от субекта, посочен в член 2, параграф 1, обхващащ всички активи с критично въздействие, в който може да се контролира достъпът до тези активи и с който се определя обхватът на прилагане на разширените мерки за контрол във връзка с киберсигурността;

7) „процес с критично въздействие“ означава работен процес, осъществяван от субект, по отношение на който показателите за въздействието върху киберсигурността в електроенергетиката са над прага на критично въздействие;

8) „праг на критично въздействие“ означава стойностите на показателите за въздействието върху киберсигурността в електроенергетиката, посочени в член 19, параграф 3, буква б), при надвишаването на които кибератака срещу работен процес ще доведе до критично смущение в трансграничните потоци на електроенергия;

9) „доставчик на ИКТ услуги с критично въздействие“ означава субект, който предоставя ИКТ услуга или ИКТ процес, които са необходими за процес с критично въздействие или с голямо въздействие, засягащ свързаните с киберсигурността аспекти на трансграничните потоци на електроенергия, и които, ако бъдат изложени на риск, могат да доведат до кибератака с въздействие над прага на критично или на голямо въздействие;

10) „трансграничен поток на електроенергия“ означава трансграничен поток по смисъла на член 2, точка 3 от Регламент (ЕС) 2019/943;

11) „кибератака“ означава инцидент съгласно определението в член 3, точка 14 от Регламент (ЕС) 2022/2554;

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

13) „мерки за контрол във връзка с киберсигурността“ означава действия или процедури, извършвани с цел избягване, откриване, противодействие или свеждане до минимум на рисковете за киберсигурността;

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

15) „система за управление на киберсигурността“ означава политиките, процедурите, насоките и свързаните с тях ресурси и дейности, управлявани колективно от даден субект с цел защита на неговите информационни активи от киберзаплахи чрез системно създаване, внедряване, прилагане, наблюдение, преразглеждане, поддържане и подобряване на сигурността на мрежите и информационните системи на организацията;

16) „оперативен център за киберсигурност“ означава специализиран център, в който технически екип, състоящ се от един или повече експерти, подпомаган от информационни системи за киберсигурност, изпълнява задачи, свързани със сигурността (услуги на оперативен център за киберсигурност („ОЦКС“), като например предприемане на действия при кибератаки и при грешки в конфигурацията на сигурността, следене на сигурността, анализ на регистри и установяване на кибератаки;

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

18) „управление на уязвимостите в киберсигурността“ означава практиката на установяване и отстраняване на уязвимости;

19) „субект“ означава субект съгласно определението в член 6, точка 38 от Директива (ЕС) 2022/2555;

20) „ранно предупреждение“ означава информацията, необходима, за да се посочи дали има съмнение, че значимият инцидент е причинен от неправомерни или злонамерени действия, или че може да има трансгранично въздействие;

21) „показател за въздействието върху киберсигурността в електроенергетиката“ („ЕСП“) означава показател или скала за класификация, според която се класифицират възможните последици от кибератаки върху работните процеси, засягащи трансграничните потоци на електроенергия;

22) „европейска схема за сертифициране на киберсигурността“ означава схема съгласно определението в член 2, точка 9 от Регламент (ЕС) 2019/881;

23) „субект с голямо въздействие“ означава субект, който осъществява процес с голямо въздействие и който е определен от компетентните органи в съответствие с член 24;

24) „процес с голямо въздействие“ означава всеки работен процес, осъществяван от субект, по отношение на който показателите за въздействието върху киберсигурността в електроенергетиката са над прага на голямо въздействие;

25) „актив с голямо въздействие“ означава актив, който е необходим за осъществяването на процес с голямо въздействие;

26) „праг на голямо въздействие“ означава стойностите на показателите за въздействието върху киберсигурността в електроенергетиката, посочени в член 19, параграф 3, буква б), при надвишаването на които успешна кибератака срещу даден процес ще доведе до съществено смущение в трансграничните потоци на електроенергия;

27) „периметър на голямо на въздействие“ означава периметър, определен от всеки субект, посочен в член 2, параграф 1, обхващащ всички активи с голямо въздействие, в който може да се контролира достъпът до тези активи и с който се определя обхватът на прилагане на минималните мерки за контрол във връзка с киберсигурността;

28) „ИКТ продукт“ означава ИКТ продукт съгласно определението в член 2, точка 12 от Регламент (ЕС) 2019/881;

29) „ИКТ услуга“ означава услуга в областта на ИКТ съгласно определението в член 2, точка 13 от Регламент (ЕС) 2019/881;

30) „ИКТ процес“ означава ИКТ процес съгласно определението в член 2, точка 14 от Регламент (ЕС) 2019/881;

31) „наследена система“ означава наследена ИКТ система съгласно определението в член 3, точка 3 от Регламент (ЕС) 2022/2554;

32) „национално единно звено за контакт“ означава единното звено за контакт, определено или създадено от всяка държава членка в съответствие с член 8, параграф 3 от Директива (ЕС) 2022/2555;

33) „органи, отговорни за управление на киберкризи в МИС“, означава органите, определени или създадени съгласно член 9, параграф 1 от Директива (ЕС) 2022/2555;

34) „първоизточник на информация“ означава субект, който инициира събитието за обмен на информация, споделяне на информация или запаметяване на информация;

35) „спецификации за възлагане на обществени поръчки“ означава спецификациите, които субектите определят за възлагането на обществени поръчки за нови или актуализирани ИКТ продукти, ИКТ процеси или ИКТ услуги;

36) „представител“ означава физическо или юридическо лице, установено в Съюза, което е изрично определено да действа от името на субект с голямо въздействие или субект с критично въздействие, който не е установен в Съюза, но предоставя услуги на субекти в Съюза, и към което компетентен орган или ЕРИКС може да се обръща — вместо към самия субект с голямо въздействие или с критично въздействие — по отношение на задълженията на въпросния субект, предвидени в настоящия регламент;

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

38) „матрица на въздействието на риска“ означава матрица, използвана по време на оценката на риска за определяне на полученото при тази оценка равнище на въздействие на риска за всеки оценен риск;

39) „едновременна криза в електроснабдяването“ означава криза в електроснабдяването съгласно определението в член 2, точка 10 от Регламент (ЕС) 2019/941;

40) „единно звено за контакт на равнище субект“ означава единно звено за контакт на равнището на съответния субект, както е посочено в член 38, параграф 1, буква в);

41) „заинтересована страна“ означава всяка страна, която има интерес от успеха и продължаващото функциониране на дадена организация или процес, като например служители, директори, акционери, регулаторни органи, сдружения, доставчици и клиенти;

42) „стандарт“ означава стандарт съгласно определението в член 2, точка 1 от Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета ([16]);

43) „регион на експлоатация на системата“ означава регионите на експлоатация на системата, както са определени в приложение I към Решение 05-2022 на ACER относно определянето на регионите на експлоатация на системата, както е установено съгласно член 36 от Регламент (ЕС) 2019/943;

44) „оператори на системи“ означава „оператор на разпределителна система“ (ОРС) и „оператор на преносна система“ (ОПС), както са определени в член 2, точки 29 и 35 от Директива (ЕС) 2019/944;

45) „процес с критично въздействие в целия Съюз“ означава всеки процес в електроенергетиката, евентуално включващ множество субекти, по отношение на който при извършването на оценката на рисковете за киберсигурността в целия Съюз възможното въздействие на кибератака може да бъде счетено за критично;

46) „процес с голямо въздействие в целия Съюз“ означава всеки процес в електроенергетиката, евентуално включващ множество субекти, по отношение на който при извършването на оценката на рисковете за киберсигурността в целия Съюз възможното въздействие на кибератака може да бъде счетено за голямо;

47) „некоригирана активно използвана уязвимост“ означава уязвимост, която все още не е публично оповестена и не е коригирана и за която има надеждни доказателства, че е извършено изпълнение на злонамерен програмен код от участник в система без разрешението на собственика на системата;

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

Член 4

Компетентен орган

1. Във възможно най-кратък срок и във всички случаи до 13 декември 2024 г. всяка държава членка определя национален правителствен или регулаторен орган, отговорен за изпълнението на задачите, които му се възлагат с настоящия регламент („компетентен орган“). До момента, в който на компетентния орган бъде възложено изпълнението на задачите съгласно настоящия регламент, регулаторният орган, определен от всяка държава членка съгласно член 57, параграф 1 от Директива (ЕС) 2019/944, изпълнява задачите на компетентния орган в съответствие с настоящия регламент.

2. Държавите членки незабавно уведомяват Комисията, ACER, ENISA, групата за сътрудничество за МИС, създадена съгласно член 14 от Директива (ЕС) 2022/2555, и Групата за координация в областта на електроенергетиката, създадена съгласно член 1 от Решение на Комисията от 15 ноември 2012 г. ([17]), и им съобщават наименованието и данните за контакт на своя компетентен орган, определен съгласно параграф 1 от настоящия член, както и всички последващи промени в тях.

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

([17]) Решение на Комисията от 15 ноември 2012 г. за създаване на Група за координация в областта на електроенергетиката (2012/C 353/02) (ОВ C 353, 17.11.2012 г., стр. 2).

3. Държавите членки може да разрешат на своя компетентен орган да делегира задачите, възложени му по силата на настоящия регламент, на други национални органи, с изключение на задачите, изброени в член 5. Всеки компетентен орган следи за прилагането на настоящия регламент от страна на органите, на които е делегирал задачи. Компетентният орган съобщава на Комисията, на ACER, на Групата за координация в областта на електроенергетиката, на ENISA и на групата за сътрудничество за МИС наименованието и данните за контакт на органите, на които е делегирана задача, както и възложените им задачи и всички последващи промени в посочените данни.

Член 5

Сътрудничество между съответните органи и структури на национално равнище

Компетентните органи координират и осигуряват подходящо сътрудничество между компетентните органи, отговарящи за киберсигурността, органите, отговорни за управлението на киберкризи, НРО, компетентните органи, отговарящи за готовността за справяне с рискове, и ЕРИКС за целите на изпълнението на съответните задължения, установени в настоящия регламент. Компетентните органи също така се координират с всички други структури или органи, определени от всяка държава членка, за да се осигурят ефикасни процедури и да се избегне дублиране на задачи и задължения. Компетентните органи могат да дадат указания на съответните НРО да поискат становище от ACER съгласно член 8, параграф 3.

Член 6

Общи условия или методики, или планове

1. ОПС в сътрудничество с ООРСЕС разработват предложения за общите условия или методиките в съответствие с параграф 2 или за плановете в съответствие с параграф 3.

2. На одобрение от всички компетентни органи подлежат следните общи условия или методики и техните изменения:

а) методиките за оценка на рисковете за киберсигурността по смисъла на член 18, параграф 1;

б) докладът за цялостна оценка на трансграничните рискове за киберсигурността в електроенергетиката в съответствие с член 23;

в) минималните и разширените мерки за контрол във връзка с киберсигурността в електроенергетиката в съответствие с член 29, съпоставянето на мерките за контрол във връзка с киберсигурността в електроенергетиката със стандартите съгласно член 34, включително на минималните и на разширените мерки за контрол във връзка с киберсигурността във веригата на доставките в съответствие с член 33;

г) препоръка относно обществените поръчки в областта на киберсигурността в съответствие с член 35;

д) методиката на скалата за класификация на кибератаките в съответствие с член 37, параграф 8.

3. Предложенията за регионални планове за намаляване на рисковете за киберсигурността в съответствие с член 22 подлежат на одобрение от всички компетентни органи на съответния регион на експлоатация на системата.

4. Предложенията за общи условия, за методиките, изброени в параграф 2, или за плановете, посочени в параграф 3, включват предложения график за тяхното прилагане и описание на очакваното им въздействие върху целите на настоящия регламент.

5. ООРСЕС може да предостави мотивирано становище на съответните ОПС до три седмици преди крайния срок за представяне на компетентните органи на предложението за общи условия или методики, или за планове. ОПС, които са отговорни за предложението за общи условия или методики, или за планове, вземат предвид мотивираното становище на ООРСЕС, преди да представят предложението за одобрение от компетентните органи. ОПС предоставят обосновка, когато не са се съобразили със становището на ООРСЕС.

6. Участващите ОПС си сътрудничат тясно при съвместното разработване на общи условия и методики, и планове. ОПС, със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС, редовно информират компетентните органи и ACER за напредъка по разработването на общи условия или методики, или на планове.

Член 7

Правила за гласуване в рамките на ОПС

1. Когато ОПС, приемащи решения по предложенията за общи условия или методики, не могат да постигнат съгласие, те приемат решението чрез гласуване с квалифицирано мнозинство. Квалифицираното мнозинство за такива предложения се изчислява, както следва:

а) ОПС, представляващи най-малко 55 % от държавите членки; и

б) ОПС, представляващи държави членки, съставляващи най-малко 65 % от населението на Съюза.

2. Блокиращото малцинство за решенията по предложения за условията или методиките по член 6, параграф 2 трябва да включва ОПС, представляващи най-малко четири държави членки, а ако липсва такова, квалифицираното мнозинство се счита за постигнато.

3. Когато ОПС от даден регион на експлоатация на системата, приемащи решения по предложения за плановете, посочени в член 6, параграф 2, не могат да постигнат съгласие и когато засегнатият регион на експлоатация на системата е съставен от над пет държави членки, ОПС приемат решението чрез гласуване с квалифицирано мнозинство. За постигане на квалифицирано мнозинство за предложенията по член 6, параграф 2 се изисква следното мнозинство:

а) ОПС, представляващи най-малко 72 % от засегнатите държави членки; и

б) ОПС, представляващи държави членки, съставляващи най-малко 65 % от населението на засегнатия регион.

4. Блокиращото малцинство при вземането на решения по предложенията за планове включва поне минимален брой ОПС, представляващи повече от 35 % от населението на участващите държави членки, плюс ОПС, представляващи най-малко още една засегната държава членка, а ако липсва такова блокиращо малцинство, квалифицираното мнозинство се счита за постигнато.

5. За решенията на ОПС по предложения за общите условия или методиките по член 6, параграф 2 всяка държава членка има един глас. Ако на територията на държава членка има повече от един ОПС, държавата членка разпределя правата на глас между тези ОПС.

6. Ако ОПС, в сътрудничество с ООРСЕС, не успеят да представят на съответните компетентни органи първоначално или изменено предложение за общи условия или методики, или за планове, в сроковете, определени в настоящия регламент, те предоставят на засегнатите компетентни органи и на ACER съответните проекти на общите условия или методики, или на плановете. Те обясняват какво е попречило на постигането на съгласие. Компетентните органи съвместно предприемат подходящите стъпки за приемане на изискваните общи условия или методики, или на изискваните планове. Това може да стане например чрез искане на изменения на проектите съгласно настоящия параграф, чрез преразглеждане и допълване на тези проекти или, когато не са предоставени проекти, чрез определяне и одобряване на изискваните общи условия или методики, или на изискваните планове.

Член 8

Представяне на предложения на компетентните органи

1. ОПС представят на засегнатите компетентни органи предложенията за общи условия или методики, или за планове за одобрение в рамките на съответните срокове, посочени в членове 18, 23, 29, 33, 34, 35 и 37. Компетентните органи може съвместно да удължат тези срокове при извънредни обстоятелства, по-специално в случаите, когато даден срок не може да бъде спазен поради обстоятелства, които са извън сферата на ОПС или на ООРСЕС.

2. Предложенията за общи условия или методики, или за планове съгласно параграф 1 се представят за информация на ACER едновременно с представянето им на компетентните органи.

3. По съвместно искане от страна на НРО ACER издава становище по предложението за общи условия или методики, или за планове в рамките на шест месеца след получаването на предложенията за общи условия или методики, или за планове и уведомява НРО и компетентните органи за становището. НРО, КООКС и всички други органи, определени като компетентни органи, се координират помежду си, преди НРО да поискат становище от ACER. ACER може да включи в това становище препоръки. ACER се консултира с ENISA, преди да предостави становище по предложенията, изброени в член 6, параграф 2.

4. Компетентните органи се консултират взаимно, сътрудничат си тясно и се координират помежду си, за да постигнат съгласие по предложените общи условия, методики или планове. Преди да одобрят общите условия или методиките, или плановете, те преразглеждат и допълват предложенията, когато е необходимо, след консултация с ЕМОПС за електроенергия и с ООРСЕС, за да се гарантира, че предложенията са в съответствие с настоящия регламент и допринасят за постигането на високо общо ниво на киберсигурност в целия Съюз.

5. Компетентните органи приемат решение по общите условия или методиките, или по плановете в рамките на шест месеца след получаването на общите условия или методиките, или на плановете от съответния компетентен орган или, когато е приложимо, от последния засегнат съответен компетентен орган.

6. Когато ACER предостави становище, съответните компетентни органи вземат предвид това становище и приемат своите решения в рамките на шест месеца от получаването на становището на ACER.

7. Когато компетентните органи съвместно изискват изменение на предложените общи условия или методики, или планове, за да ги одобрят, ОПС в сътрудничество с ООРСЕС разработват предложение за такова изменение на общите условия или методиките, или на плановете. ОПС представят измененото предложение за одобрение в рамките на два месеца след искането на компетентните органи. Компетентните органи приемат решение относно изменените общи условия или методики, или планове, в рамките на два месеца след представянето им.

8. Когато компетентните органи не са успели да постигнат съгласие в рамките на срока, посочен в параграф 5 или 7, те информират Комисията. Комисията може да предприеме подходящи стъпки, за да направи възможно приемането на изискваните общи условия или методики, или планове.

9. ОПС, със съдействието на ЕМОПС за електроенергия и на ООРСЕС, оповестяват общите условия или методиките, или плановете на своите уебсайтове след одобряването им от съответните компетентни органи, освен когато тази информация се счита за поверителна в съответствие с член 47.

10. Компетентните органи може съвместно да поискат от ОПС и ООРСЕС предложения за изменения на одобрените общи условия или методики или на одобрените планове и да определят краен срок за подаване на тези предложения. ОПС, в сътрудничество с ООРСЕС, може да предлагат на компетентните органи изменения и по собствена инициатива. Предложенията за изменение на общите условия или на методиките, или за изменение на плановете се разработват и одобряват в съответствие с процедурата, посочена в настоящия член.

11. Най-малко веднъж на всеки три години след първоначалното приемане на съответните общи условия или методики, или на съответните приети планове ОПС, в сътрудничество с ООРСЕС, правят преглед на ефективността на приетите общи условия или методики, или на приетите планове и докладват без неоправдано забавяне констатациите от прегледа на компетентните органи и на ACER.

Член 9

Консултации

1. ОПС, със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС, се консултират със заинтересованите страни, включително ACER, ENISA и компетентния орган на всяка държава членка, относно проектопредложенията за общи условия или методики, изброени в член 6, параграф 2, или за плановете, посочени в член 6, параграф 3. Консултацията продължава не по-малко от един месец.

2. Предложенията за общи условия или методики, изброени в член 6, параграф 2, представени от ОПС в сътрудничество с ООРСЕС, се оповестяват и се подлагат на консултация на равнището на Съюза. Предложенията за плановете, посочени в член 6, параграф 3, представени от съответните ОПС в сътрудничество с ООРСЕС на регионално равнище, се подлагат на консултации най-малко на регионално равнище.

3. ОПС, със съдействието на ЕМОПС за електроенергия, и ООРСЕС, отговаряща за предложението за общи условия или методики или за планове, надлежно вземат предвид становищата на заинтересованите страни, изразени при проведените съгласно параграф 1 консултации, преди да представят това предложение за регулаторно одобрение. Във всички случаи при представянето на предложението се прилага солидна обосновка за причините за включването или невключването на становищата, изразени при консултацията, и тази обосновка се оповестява своевременно преди или едновременно с оповестяването на предложението за общите условия или методиките.

Член 10

Участие на заинтересованите страни

ACER, в тясно сътрудничество с ЕМОПС за електроенергия и ООРСЕС, организира участието на заинтересованите страни, включително редовни срещи със заинтересованите страни за установяване на проблеми и предлагане на подобрения, свързани с прилагането на настоящия регламент.

Член 11

Възстановяване на разходите

1. Разходите, понесени от ОПС и ОРС, които са обект на регулиране на мрежовите тарифи, и произтичащи от задълженията, предвидени в настоящия регламент, включително разходите, понесени от ЕМОПС за електроенергия и от ООРСЕС, се оценяват от съответния НРО на всяка държава членка.

2. Разходите, оценени като приемливи, ефективни и пропорционални, се възстановяват чрез мрежови тарифи или други подходящи механизми, определени от съответния НРО.

3. ОПС и ОРС, посочени в параграф 1, предоставят в приемлив срок, определен от НРО, информацията, необходима за улесняване на оценката на направените разходи, ако такава бъде поискана от съответните НРО.

Член 12

Наблюдение

1. ACER наблюдава изпълнението на настоящия регламент в съответствие с член 32, параграф 1 от Регламент (ЕС) 2019/943 и член 4, параграф 2 от Регламент (ЕС) 2019/942. При извършването на това наблюдение ACER може да си сътрудничи с ENISA и да поиска подкрепа от ЕМОПС за електроенергия и от ООРСЕС. ACER редовно информира Групата за координация в областта на електроенергетиката и групата за сътрудничество за МИС относно прилагането на настоящия регламент.

2. Най-малко на всеки три години след влизането в сила на настоящия регламент ACER публикува доклад с цел:

а) преглед на състоянието на изпълнението на приложимите мерки за управление на рисковете за киберсигурността по отношение на субектите с голямо въздействие и субектите с критично въздействие;

б) установяване дали са необходими допълнителни правила относно общи изисквания, планиране, наблюдение, докладване и управление на кризи, за да се предотвратят рисковете за електроенергетиката; и

в) установяване на областите с възможности за подобрение за целите на преразглеждането на настоящия регламент или определяне на необхванати области и на нови приоритети, които може да възникнат поради развитието на технологиите.

3. До 13 юни 2025 г. ACER, в сътрудничество с ENISA и след консултация с ЕМОПС за електроенергия и ООРСЕС, може да издаде насоки относно съответната информация, която трябва да се съобщава на ACER за целите на наблюдението, както и относно процеса и честотата на събирането ѝ, въз основа на показателите за изпълнението, определени в съответствие с параграф 5.

4. Компетентните органи може да разполагат с достъп до съответната информация, съхранявана от ACER, която агенцията е събрала в съответствие с настоящия член.

5. ACER, в сътрудничество с ENISA и с подкрепата на ЕМОПС за електроенергия и на ООРСЕС, издава необвързващи показатели за изпълнението за оценка на експлоатационната надеждност, които се отнасят до свързаните с киберсигурността аспекти на трансграничните потоци на електроенергия.

6. Субектите, изброени в член 2, параграф 1 от настоящия регламент, предоставят на ACER информацията, необходима на агенцията за изпълнението на задачите, изброени в параграф 2.

Член 13

Сравнителен анализ

1. До 13 юни 2025 г. ACER, в сътрудничество с ENISA, изготвя ръководство с незадължителен характер за сравнителен анализ на киберсигурността. В ръководството на НРО се обясняват принципите за сравнителен анализ на прилаганите мерки за контрол във връзка с киберсигурността съгласно параграф 2 от настоящия член, като се вземат предвид разходите за прилагане на мерките за контрол и ефективността на функцията, изпълнявана от процесите, продуктите, услугите, системите и решенията, използвани за прилагането на такива мерки за контрол. При изготвянето на ръководството с незадължителен характер за сравнителен анализ на киберсигурността ACER взема предвид съществуващите доклади за сравнителен анализ. ACER предоставя на НРО за информация ръководството с незадължителен характер за сравнителен анализ на киберсигурността.

2. В рамките на 12 месеца след създаването на ръководството за сравнителен анализ съгласно параграф 1 НРО извършват сравнителен анализ, за да оценят дали с настоящите инвестиции в киберсигурността:

а) се намаляват рисковете, които оказват влияние върху трансграничните потоци на електроенергия;

б) се постигат желаните резултати и се способства за по-голяма ефективност при развитието на електроенергийните системи;

в) дали посочените инвестиции в киберсигурността са ефикасни и интегрирани в цялостното снабдяване с активи и услуги.

3. За целите на сравнителния анализ НРО може да вземат предвид ръководството с незадължителен характер за сравнителен анализ на киберсигурността, изготвено от ACER, и по-специално да оценяват:

а) средните свързани с киберсигурността разходи за намаляване на рисковете, оказващи влияние върху трансграничните потоци на електроенергия, особено по отношение на субектите с голямо въздействие и субектите с критично въздействие;

б) в сътрудничество с ЕМОПС за електроенергия и ООРСЕС, средните цени на услугите, системите и продуктите за киберсигурност, които допринасят в голяма степен за подобряването и поддържането на мерките за управление на рисковете за киберсигурността в различните региони на експлоатация на системата;

в) наличието и степента на съпоставимост на разходите и функциите, свързани с услугите, системите и решенията в областта на киберсигурността, подходящи за прилагането на настоящия регламент, като се набелязват възможни мерки, необходими за насърчаване на ефективността на разходите, особено в случаите, когато може да са необходими инвестиции в технологии в областта на киберсигурността.

4. Всяка информация, свързана със сравнителния анализ, се обработва и преработва в съответствие с изискванията за класификация на данните в настоящия регламент, с минималните мерки за контрол във връзка с киберсигурността и с доклада за оценка на трансграничните рискове за киберсигурността в електроенергетиката. Сравнителният анализ, посочен в параграфи 2 и 3, не се оповестява публично.

5. Без да се засягат изискванията за поверителност, посочени в член 47, и необходимостта от опазване на сигурността на субектите, за които се прилагат разпоредбите на настоящия регламент, сравнителният анализ, посочен в параграфи 2 и 3 от настоящия член, се предоставя на всички НРО, всички компетентни органи, ACER, ENISA и Комисията.

Член 14

Споразумения с ОПС от държави извън Съюза

1. В рамките на 18 месеца след влизането в сила на настоящия регламент ОПС от регион на експлоатация на система, който е съседен на трета държава, полагат усилия да сключат споразумения с ОПС от съседната трета държава, които са в съответствие с приложимото право на Съюза и в които се определят основата за сътрудничество в областта на защитата на киберсигурността и договореностите за сътрудничество в областта на киберсигурността с тези ОПС.

2. ОПС информират компетентния орган за споразуменията, сключени съгласно параграф 1.

Член 15

Законни представители

1. Субекти, които нямат място на стопанска дейност в Съюза, но предоставят услуги на субекти в Съюза и за които е постъпило уведомление, че са определени като субекти с голямо или с критично въздействие в съответствие с член 24, параграф 6, в срок от три месеца след уведомяването определят писмено свой представител в Съюза и информират с оглед на това уведомяващия компетентен орган.

2. Този представител разполага с правомощия, позволяващи към него да се обръща всеки компетентен орган или ЕРИКС в Съюза, вместо към или в допълнение към субекта с голямо въздействие или субекта с критично въздействие по отношение на задълженията на въпросния субект съгласно настоящия регламент. Субектът с голямо въздействие или субектът с критично въздействие предоставя на своя законен представител необходимите правомощия и достатъчно ресурси, за да се гарантира ефективното и своевременно сътрудничество със съответните компетентни органи или ЕРИКС.

3. Представителят трябва да е установен в една от държавите членки, в които субектът предлага своите услуги. Приема се, че субектът е под юрисдикцията на държавата членка, в която е установен представителят. Субектите с голямо въздействие или с критично въздействие съобщават името, пощенския адрес, адреса на електронната поща и телефонния номер на своя законен представител на компетентния орган в държавата членка, в която пребивава или е установен законният представител.

4. Възможно е определеният законен представител да бъде подведен под отговорност за неспазване на задълженията по настоящия регламент, без да се засягат отговорността и правните действия, които биха могли да бъдат предприети срещу самия субект с голямо или с критично въздействие.

5. При липсата на представител в Съюза, определен съгласно настоящия член, всяка държава членка, в която субектът предоставя услуги, може да предприеме правни действия срещу него за неизпълнение на задълженията съгласно настоящия регламент.

6. Определянето на представител в Съюза съгласно параграф 1 не представлява установяване в Съюза.

Член 16

Сътрудничество между ЕМОПС за електроенергия и ООРСЕС

1. ЕМОПС за електроенергия и ООРСЕС си сътрудничат при извършването на оценки на рисковете за киберсигурността съгласно член 19 и член 21, и по-специално при изпълнението на следните задачи:

а) разработването на методиките за оценка на рисковете за киберсигурността съгласно член 18, параграф 1;

б) изготвянето на доклад за цялостна оценка на трансграничните рискове за киберсигурността в електроенергетиката в съответствие с член 23;

в) разработването на обща рамка в областта на киберсигурността в електроенергетиката в съответствие с глава III;

г) изготвянето на препоръка относно обществените поръчки в областта на киберсигурността в съответствие с член 35;

д) разработването на методиката на скалата за класификация на кибератаките в съответствие с член 37, параграф 8;

е) разработването на временен показател за въздействие върху киберсигурността в електроенергетиката (ECII) за показателя за въздействие върху киберсигурността в електроенергетиката в съответствие с член 48, параграф 1, буква а);

ж) изготвянето на консолидирания временен списък на субектите с голямо въздействие и с критично въздействие съгласно член 48, параграф 3;

з) изготвянето на временния списък на процесите с голямо въздействие и с критично въздействие в целия Съюз в съответствие с член 48, параграф 4;

и) изготвянето на временния списък на европейските и международните стандарти и мерки за контрол в съответствие с член 48, параграф 6;

й) извършването на оценката на рисковете за киберсигурността в целия Съюз в съответствие с член 19;

к) извършването на регионалните оценки на рисковете за киберсигурността в съответствие с член 21;

л) определянето на регионалните планове за намаляване на рисковете за киберсигурността в съответствие с член 22;

м) разработването на насоки относно европейските схеми за сертифициране на киберсигурността за ИКТ продукти, ИКТ услуги и ИКТ процеси в съответствие с член 36;

н) разработването, след консултации с ACER и ENISA, на насоки за прилагането на настоящия регламент.

2. Сътрудничеството между ЕМОПС за електроенергия и ООРСЕС може да се осъществява под формата на работна група относно рисковете за киберсигурността.

3. ЕМОПС за електроенергия и ООРСЕС редовно информират ACER, ENISA, групата за сътрудничество за МИС и Групата за координация в областта на електроенергетиката за напредъка по изпълнението на оценките в целия Съюз и регионалните оценки на рисковете за киберсигурността в съответствие с член 19 и член 21.

Член 17

Сътрудничество между ACER и компетентните органи

ACER, в сътрудничество с всеки компетентен орган:

1) наблюдава изпълнението на мерките за управление на рисковете за киберсигурността в съответствие с член 12, параграф 2, буква а) и на задълженията за докладване в съответствие с член 27 и член 39; и

2) наблюдава процеса на приемане, както и прилагането на общите условия, методиките или плановете в съответствие с член 6, параграфи 2 и 3. Сътрудничеството между ACER, ENISA и всеки компетентен орган може да се осъществява под формата на орган за наблюдение на рисковете за киберсигурността.

ГЛАВА II

ОЦЕНКА НА РИСКОВЕТЕ И ОПРЕДЕЛЯНЕ НА СЪОТВЕТНИТЕ РИСКОВЕ ЗА КИБЕРСИГУРНОСТТА

Член 18

Методики за оценка на рисковете за киберсигурността

1. До 13 март 2025 г. ОПС, със съдействието на ЕМОПС за електроенергия, в сътрудничество с ООРСЕС и след консултация с групата за сътрудничество за МИС, представят предложение за методиките за оценка на рисковете за киберсигурността на равнището на Съюза, на регионално равнище и на равнището на държавата членка.

2. Методиките за оценка на рисковете за киберсигурността на равнището на Съюза, на регионално равнище и на равнището на държавата членка включват:

а) списък на киберзаплахите, които трябва да бъдат разгледани, включително поне следните заплахи за веригата на доставките:

i) сериозно и непредвидено нарушаване на веригата на доставките;

ii) липса на наличност на ИКТ продукти, ИКТ услуги или ИКТ процеси във веригата на доставките;

iii) предприети кибератаки чрез участници във веригата на доставките;

iv) изтичане на чувствителна информация по веригата на доставките, включително проследяване по веригата на доставките;

v) въвеждане на слаби места или задни вратички в ИКТ продукти, ИКТ услуги или ИКТ процеси чрез участници във веригата на доставките;

б) критериите за оценка на въздействието на рисковете за киберсигурността като голямо или като критично, като се използват определени прагове за последиците и вероятността;

в) подход за анализиране на рисковете за киберсигурността, произтичащи от наследените системи, каскадните ефекти от кибератаки и естеството на системите, осигуряващи работата на електроенергийната мрежа, като действащи в реално време системи;

г) подход за анализ на рисковете за киберсигурността, произтичащи от зависимостта от един-единствен доставчик на ИКТ продукти, ИКТ услуги или ИКТ процеси.

3. С методиките за оценка на рисковете за киберсигурността на равнището на Съюза, на регионално равнище и на равнището на държавата членка се оценяват рисковете за киберсигурността, като се използва една и съща матрица на въздействието на риска. С матрицата на въздействието на риска:

а) се измерват последиците от кибератаките въз основа на следните критерии:

i) отпадане на товар;

ii) намаляване на генериращата мощност;

iii) отпадане на мощност в резерва за първично регулиране на честотата;

iv) загуба на способност за възстановяване на функционирането на електроенергийна мрежа, без да се разчита на възстановяването на външната преносна мрежа след пълно или частично изключване (наричана още „пускане без външно захранване“);

v) очакваната продължителност на прекъсване на електроснабдяването, което засяга клиентите, в комбинация с мащаба на прекъсването по отношение на броя на клиентите;

vi) всички други количествени или качествени критерии, които логично биха могли да служат за показатели за въздействието на кибератаката върху трансграничните потоци на електроенергия;

б) се измерва вероятността за инцидент като честота на кибератаките за една година.

4. В методиките за оценка на рисковете за киберсигурността на равнището на Съюза се описват начините за определяне на стойностите на ECII за праговете на голямо и на критично въздействие. ECII дава възможност на субектите да оценяват с помощта на критериите, посочени в параграф 2, буква б), въздействието на рисковете върху техния работен процес по време на оценките на въздействието върху дейността, които извършват съгласно член 26, параграф 4, буква в), подточка i).

5. ЕМОПС за електроенергия, в координация с ООРСЕС, информира Групата за координация в областта на електроенергетиката относно предложенията за методики за оценка на рисковете за киберсигурността, които са разработени в съответствие с параграф 1.

Член 19

Оценка на рисковете за киберсигурността в целия Съюз

1. В рамките на 9 месеца след одобряването на методиките за оценка на рисковете за киберсигурността в съответствие с член 8 и на всеки три години след това ЕМОПС за електроенергия, в сътрудничество с ООРСЕС и като се консултира с групата за сътрудничество за МИС, без да се засяга член 22 от Директива (ЕС) 2022/2555, извършва оценка на рисковете за киберсигурността в целия Съюз и изготвя проектодоклад за оценка на рисковете за киберсигурността в целия Съюз. За тази цел те ще използват методиките, разработени съгласно член 18 и одобрени съгласно член 8, за определяне, анализ и оценка на възможните последици от кибератаки, които засягат експлоатационната сигурност на електроенергийната система и нарушават трансграничните потоци на електроенергия. При оценката на рисковете за киберсигурността в целия Съюз не се вземат предвид правните и финансовите вреди или уронването на доброто име, дължащи се на кибератаки.

2. Докладът за оценка на рисковете за киберсигурността в целия Съюз включва следните елементи:

а) процесите с голямо въздействие и с критично въздействие в целия Съюз;

б) матрица на въздействието на риска, която субектите и компетентните органи използват за оценка на рисковете за киберсигурността, установени при оценката на рисковете за киберсигурността на равнището на държавата членка, извършена в съответствие с член 20, и при оценката на рисковете за киберсигурността на равнище субект, извършена в съответствие с член 26, параграф 2, буква б).

3. По отношение на процесите с голямо въздействие в целия Съюз и процесите с критично въздействие в целия Съюз докладът за оценка на рисковете за киберсигурността в целия Съюз включва:

а) оценка на възможните последици от кибератака, като се използват показателите, определени в методиката за оценка на рисковете за киберсигурността, разработена в съответствие с член 18, параграфи 2, 3 и 4 и одобрена в съответствие с член 8;

б) ЕСП и праговете на голямо и на критично въздействие, които компетентните органи използват съгласно член 24, параграфи 1 и 2, за да определят субектите с голямо въздействие и с критично въздействие, участващи в процесите с голямо въздействие в целия Съюз и в процесите с критично въздействие в целия Съюз.

4. ЕМОПС за електроенергия, в сътрудничество с ООРСЕС, предоставя на ACER за становище проектодоклада за оценка на рисковете за киберсигурността в целия Съюз, съдържащ резултатите от оценката на рисковете за киберсигурността в целия Съюз. ACER дава становище по проектодоклада в срок от три месеца след получаването му. При оформянето на окончателната редакция на този доклад ЕМОПС за електроенергия и ООРСЕС отчитат в максимална степен становището на ACER.

5. В рамките на три месеца след получаването на становището на ACER ЕМОПС за електроенергия, в сътрудничество с ООРСЕС, уведомява ACER, Комисията, ENISA и компетентните органи за окончателния доклад за оценка на рисковете за киберсигурността в целия Съюз.

Член 20

Оценка на рисковете за киберсигурността на равнище държава членка

1. Всеки компетентен орган извършва оценка на рисковете за киберсигурността на равнище държава членка за всички субекти с голямо въздействие и с критично въздействие в своята държава членка, като използва методиките, разработени съгласно член 18 и одобрени съгласно член 8. При оценката на рисковете за киберсигурността на равнище държава членка се определят и анализират рисковете от кибератаки, които засягат експлоатационната сигурност на електроенергийната система и нарушават трансграничните потоци на електроенергия. При оценката на рисковете за киберсигурността на равнище държава членка не се вземат предвид правните и финансовите вреди или уронването на доброто име, дължащи се на кибератаки.

2. В рамките на 21 месеца след уведомяването на субектите с голямо въздействие и с критично въздействие съгласно член 24, параграф 6 и на всеки три години след тази дата, и след консултация с КООКС, отговарящ за електроенергията, всеки компетентен орган, подпомаган от ЕРИКС, предоставя на ЕМОПС за електроенергия и на ООРСЕС доклад за оценка на рисковете за киберсигурността на равнище държава членка, съдържащ следната информация за всеки работен процес с голямо въздействие и с критично въздействие:

а) състоянието на изпълнението на минималните и разширените мерки за контрол във връзка с киберсигурността в съответствие с член 29;

б) списък на всички кибератаки, докладвани през предходните три години съгласно член 38, параграф 3;

в) обобщение на информацията за киберзаплахите, докладвана през предходните три години съгласно член 38, параграф 6;

г) оценка на рисковете от компрометиране на поверителността, почтеността и на наличността на информацията, както и на съответните активи, за всеки процес с голямо въздействие или с критично въздействие в целия Съюз;

д) когато е необходимо, списък на допълнителни субекти, определени като такива с голямо въздействие или с критично въздействие съгласно член 24, параграфи 1, 2, 3 и 5.

3. В доклада за оценка на рисковете за киберсигурността на равнище държава членка се взема предвид планът за готовност за справяне с рискове на държавата членка, изготвен съгласно член 10 от Регламент (ЕС) 2019/941.

4. Информацията, съдържаща се в доклада за оценка на рисковете за киберсигурността на равнище държава членка съгласно параграф 2, букви а)—г), не трябва да се свързва с конкретни субекти или активи. Докладът за оценка на рисковете за киберсигурността на равнище държава членка включва и оценка на риска, свързан с временните дерогации, издадени от компетентните органи в държавите членки съгласно член 30.

5. ЕМОПС за електроенергия и ООРСЕС може да поискат допълнителна информация от компетентните органи във връзка със задачите, посочени в параграф 2, букви а) и в).

6. Компетентните органи гарантират, че предоставената от тях информация е точна и вярна.

Член 21

Регионални оценки на рисковете за киберсигурността

1. ЕМОПС за електроенергия, в сътрудничество с ООРСЕС и като се консултира със съответния регионален координационен център, извършва регионална оценка на рисковете за киберсигурността за всеки регион на експлоатация на системата, като използва методиките, разработени съгласно член 19 и одобрени съгласно член 8, за да установи, анализира и оцени рисковете от кибератаки, засягащи експлоатационната сигурност на електроенергийната система и нарушаващи трансграничните потоци на електроенергия. При регионалните оценки на рисковете за киберсигурността не се вземат предвид правните и финансовите вреди или уронването на доброто име, дължащи се на кибератаки.

2. В рамките на 30 месеца след уведомяването на субектите с голямо въздействие и с критично въздействие съгласно член 24, параграф 6 и на всеки три години след това ЕМОПС за електроенергия, в сътрудничество с ООРСЕС и като се консултира с групата за сътрудничество за МИС, изготвя регионален доклад за оценка на рисковете за киберсигурността за всеки регион на експлоатация на системата.

3. В регионалния доклад за оценка на рисковете за киберсигурността се взема предвид съответната информация, съдържаща се в докладите за оценка на рисковете за киберсигурността в целия Съюз и в докладите за оценка на рисковете за киберсигурността на равнище държава членка.

4. При регионалната оценка на рисковете за киберсигурността се разглеждат сценариите при регионална криза в електроснабдяването, свързана с киберсигурността, определени съгласно член 6 от Регламент (ЕС) 2019/941.

Член 22

Регионални планове за намаляване на рисковете за киберсигурността

1. В рамките на 36 месеца след уведомяването на субектите с голямо и с критично въздействие съгласно член 24, параграф 6 и не по-късно от 13 юни 2031 г., както и на всеки три години след тази дата, ОПС, със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС, и като се консултират с регионалните координационни центрове и с групата за сътрудничество за МИС, разработват регионален план за намаляване на рисковете за киберсигурността за всеки регион на експлоатация на системата.

2. Регионалните планове за намаляване на рисковете за киберсигурността включват:

а) минималните и разширените мерки за контрол във връзка с киберсигурността, които субектите с голямо въздействие и с критично въздействие трябва да прилагат в региона на експлоатация на системата;

б) остатъчните рискове за киберсигурността в регионите на експлоатация на системата след прилагането на мерките за контрол, посочени в буква а).

3. ЕМОПС за електроенергия предоставя регионалните планове за намаляване на рисковете на съответните оператори на преносни системи, на компетентните органи и на Групата за координация в областта на електроенергетиката. Групата за координация в областта на електроенергетиката може да препоръча внасянето на изменения.

4. ОПС, със съдействието на ЕМОПС за електроенергия в сътрудничество с ООРСЕС и като се консултират с групата за сътрудничество за МИС, актуализират регионалните планове за намаляване на рисковете на всеки три години, освен ако обстоятелствата не налагат по-чести актуализации.

Член 23

Доклад за цялостна оценка на трансграничните рискове за киберсигурността в електроенергетиката

1. В рамките на 40 месеца след уведомяването на субектите с голямо въздействие и субектите с критично въздействие в съответствие с член 24, параграф 6 и на всеки три години след това ОПС, със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС, и като се консултират с групата за сътрудничество за МИС, предоставят на Групата за координация в областта на електроенергетиката доклад относно резултатите от оценката на рисковете за киберсигурността по отношение на трансграничните потоци на електроенергия („доклад за цялостна оценка на трансграничните рискове за киберсигурността в електроенергетиката“).

2. Докладът за цялостна оценка на трансграничните рискове за киберсигурността в електроенергетиката се основава на доклада за оценка на рисковете за киберсигурността в целия Съюз, на докладите за оценка на рисковете за киберсигурността на равнище държава членка и на регионалните доклади за оценка на рисковете за киберсигурността и включва следната информация:

а) списъка на процесите с голямо въздействие в целия Съюз и процесите с критично въздействие в целия Съюз, установени в доклада за оценка на рисковете за киберсигурността в целия Съюз в съответствие с член 19, параграф 2, буква а), включително оценката на вероятността и на въздействието на рисковете за киберсигурността, оценени по време на изготвянето на регионалните доклади за оценка на рисковете за киберсигурността в съответствие с член 21, параграф 2 и член 19, параграф 3, буква а);

б) настоящите киберзаплахи, със специално наблягане върху нововъзникващите заплахи и рискове за електроенергийната система;

в) кибератаките за предходния период на равнището на Съюза, като предоставя критичен преглед на това как тези кибератаки може да са оказали влияние върху трансграничните потоци на електроенергия;

г) общото състояние на изпълнението на мерките в областта на киберсигурността;

д) състоянието на изпълнението на информационните потоци съгласно членове 37 и 38;

е) списък на информацията или на специфичните критерии за класифициране на информация съгласно член 46;

ж) установените и откроените рискове, които може да произтекат от необезпеченото със сигурност управление на веригата на доставките;

з) резултатите и натрупания опит от регионалните и междурегионалните учения в областта на киберсигурността, организирани съгласно член 44;

и) анализ на развитието на цялостните трансгранични рискове за киберсигурността в електроенергетиката след последните регионални оценки на рисковете за киберсигурността;

й) всяка друга информация, която може да бъде полезна за определяне на възможни подобрения на настоящия регламент или на необходимостта от преразглеждане на настоящия регламент или на някой от неговите инструменти; и

к) обобщена и анонимизирана информация за дерогациите, предоставени съгласно член 30, параграф 3.

3. Субектите, изброени в член 2, параграф 1, може да допринасят за изготвянето на доклада за цялостна оценка на трансграничните рискове за киберсигурността в електроенергетиката, като съблюдават поверителността на информацията в съответствие с член 47. ОПС, със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС, се консултират на ранен етап с тези субекти.

4. Докладът за цялостна оценка на трансграничните рискове за киберсигурността в електроенергетиката е предмет на правилата за защита на обмена на информация съгласно член 46. Без да се засягат разпоредбите на член 10, параграф 4 и член 47, параграф 4, ЕМОПС за електроенергия и ООРСЕС публикуват публична версия на този доклад, която не съдържа информация, която може да причини вреда на субектите, изброени в член 2, параграф 1. Публичната версия на този доклад се публикува само със съгласието на групата за сътрудничество за МИС и Групата за координация в областта на електроенергетиката. ЕМОПС за електроенергия в координация с ООРСЕС отговаря за съставянето и публикуването на публичната версия на доклада.

Член 24

Определяне на субекти с голямо въздействие и субекти с критично въздействие

1. Всеки компетентен орган, като използва ЕСII и праговете на голямо и на критично въздействие, включени в доклада за оценка на рисковете за киберсигурността в целия Съюз в съответствие с член 19, параграф 3, буква б), определя субектите с голямо въздействие и субектите с критично въздействие в своята държава членка, които участват в процесите с голямо въздействие в целия Съюз и в процесите с критично въздействие в целия Съюз. Компетентните органи могат да поискат информация от даден субект в тяхната държава членка, за да определят стойностите на ЕСII за този субект. Ако определената стойност на ЕСII на даден субект е над прага на голямо или на критично въздействие, определеният субект бива включен в доклада за оценка на рисковете за киберсигурността на равнище държава членка, посочен в член 20, параграф 2.

2. Всеки компетентен орган, като използва ЕСII и праговете на голямо и на критично въздействие, включени в доклада за оценка на рисковете за киберсигурността в целия Съюз в съответствие с член 19, параграф 3, буква б), определя субектите с голямо въздействие и с критично въздействие, които не са установени в Съюза, доколкото те извършват дейност в рамките на Съюза. Компетентният орган може да поиска информация от субект, който не е установен в Съюза, за да определи стойностите на ЕСII за този субект.

3. Всеки компетентен орган може да определи допълнителни субекти в своята държава членка като субекти с голямо въздействие или с критично въздействие, ако са изпълнени следните критерии:

а) субектът е част от група субекти, за които съществува значителен риск да бъдат засегнати едновременно от кибератака;

б) ЕСII, обобщен за групата субекти, е над прага на голямо въздействие или на критично въздействие.

4. Ако компетентният орган определи допълнителни субекти в съответствие с параграф 3, всички процеси в тези субекти, за които ЕСII, обобщени за групата субекти, са над прага на голямо въздействие, се считат за процеси с голямо въздействие, а всички процеси в тези субекти, за които ЕСII, обобщени за групата субекти, са над праговете на критично въздействие, се считат за процеси с критично въздействие.

5. Ако компетентен орган определи посочени в параграф 3, буква а) субекти в повече от една държава членка, той информира за това другите компетентни органи, ЕМОПС за електроенергия и ООРСЕС. Въз основа на информацията, получена от всички компетентни органи, ЕМОПС за електроенергия, в сътрудничество с ООРСЕС, предоставя на компетентните органи анализ на съвкупностите от субекти в повече от една държава членка, които могат да създадат разпределени смущения в трансграничните потоци на електроенергия и могат да доведат до кибератака. Когато група субекти в няколко държави членки са определени като съвкупност, чийто ЕСII надвишава прага на голямо въздействие или на критично въздействие, всички засегнати компетентни органи определят субектите в такава група като субекти с голямо въздействие или с критично въздействие за своята съответна държава членка въз основа на обобщения индекс ЕСII за групата субекти, а определените субекти се описват в доклада за оценка на рисковете за киберсигурността в целия Съюз.

6. В рамките на девет месеца след получаването на уведомление от ЕМОПС за електроенергия и от ООРСЕС за доклада за оценка на рисковете за киберсигурността в целия Съюз по член 19, параграф 5, но във всички случаи не по-късно от 13 юни 2028 г., всеки компетентен орган уведомява субектите в списъка, че те са определени като субекти с голямо въздействие или с критично въздействие в неговата държава членка.

7. Когато на компетентен орган е докладвано за даден доставчик на услуги, че той е доставчик на ИКТ услуги с критично въздействие в съответствие с член 27, буква в), този компетентен орган уведомява за това компетентните органи на държавите членки, на чиято територия се намира седалището или представителството. Последният компетентен орган уведомява доставчика на услуги, че е бил определен като доставчик на критични услуги.

Член 25

Национални схеми за проверка

1. Компетентните органи може да създадат национална схема за проверки, за да се удостоверява, че субектите с критично въздействие, определени съгласно член 24, параграф 1, са приложили националната законодателна рамка, която е включена в матрицата на съответствията, посочена в член 34. Националната схема за проверка може да се основава на инспекция, извършвана от компетентния орган, на независими одити на сигурността или на взаимни партньорски проверки от субекти с критично въздействие в същата държава членка, контролирани от компетентния орган.

2. Ако даден компетентен орган реши да създаде национална схема за проверка, този компетентен орган гарантира, че проверката се извършва в съответствие със следните изисквания:

а) всяка страна, извършваща партньорска проверка, одит или инспекция, е независима от проверявания субект с критично въздействие и няма наличен конфликт на интереси;

б) персоналът, който извършва партньорската проверка, одита или инспекцията, трябва да има удостоверими познания в областта на:

i) киберсигурността в електроенергетиката;

ii) системи за управление на киберсигурността;

iii) принципите на одита;

iv) оценката на рисковете за киберсигурността;

v) общата рамка в областта на киберсигурността в електроенергетиката;

vi) националната законодателна и регулаторна рамка и европейските и международните стандарти в обхвата на проверката;

vii) процесите с критично въздействие в обхвата на проверката;

в) на страната, извършваща партньорската проверка, одита или инспекцията, се предоставя достатъчно време за извършване на тези дейности;

г) страната, извършваща партньорската проверка, одита или инспекцията, предприема подходящи мерки за защита на информацията, която събира по време на проверката, в съответствие с нейната степен на поверителност; и

д) партньорските проверки, одитите или инспекциите се извършват поне веднъж годишно и включват пълния обхват на проверката поне веднъж на всеки три години.

3. Ако даден компетентен орган реши да създаде национална схема за проверка, той докладва ежегодно на ACER колко често е извършвал проверки по тази схема.

Член 26

Управление на риска в областта на киберсигурността на равнището на отделните субекти

1. Всеки субект с голямо въздействие и с критично въздействие, определен от компетентните органи съгласно член 24, параграф 1, изпълнява дейности по управление на риска в областта на киберсигурността за всички свои активи в периметъра си на голямо въздействие и на критично въздействие. Всеки субект с голямо въздействие и с критично въздействие извършва управление на риска, съдържащо етапите, описани в параграф 2, на всеки три години.

2. Управлението на риска в областта на киберсигурността на всеки субект с голямо въздействие и с критично въздействие се основава на подход, целящ да предпази мрежите и информационните системи на този субекти и включващ следните етапи:

а) установяване на контекста;

б) оценка на рисковете за киберсигурността на равнище субект;

в) третиране на рисковете за киберсигурността;

г) приемане на рисковете за киберсигурността.

3. По време на етапа на установяване на контекста всеки субект с голямо въздействие и с критично въздействие:

а) определя обхвата на оценката на рисковете за киберсигурността, включително процесите с голямо въздействие и процесите с критично въздействие, определени от ЕМОПС за електроенергия и ООРСЕС, и други процеси, които може да бъдат обект на кибератаки с голямо въздействие или с критично въздействие върху трансграничните потоци на електроенергия; и

б) определя критериите за оценка на риска и за приемане на риска в съответствие с матрицата на въздействието на риска, която субектите и компетентните органи използват за оценка на рисковете за киберсигурността в методиките за оценка на рисковете за киберсигурността на равнището на Съюза, на регионално равнище и на равнището на държавите членки, разработена от ЕМОПС за електроенергия и ООРСЕС в съответствие с член 19, параграф 2.

4. По време на етапа на оценка на рисковете за киберсигурността всеки субект с голямо въздействие и с критично въздействие:

а) определя рисковете за киберсигурността, като взема предвид:

i) всички активи, поддържащи процесите с голямо въздействие и с критично въздействие в целия Съюз, като се прави оценка на възможното влияние върху трансграничните потоци на електроенергия, ако активът бъде компрометиран;

ii) възможните киберзаплахи, като се вземат предвид киберзаплахите, установени в последния доклад за цялостна оценка на трансграничните рискове за киберсигурността в електроенергетиката, посочен в член 23, параграф 1, и заплахите по веригата на доставките;

iii) уязвимостите, включително уязвимостите в наследените системи;

iv) възможните сценарии за кибератаки, включително кибератаки, които засягат експлоатационната сигурност на електроенергийната система и нарушават трансграничните потоци на електроенергия;

v) съответните оценки и анализи на рисковете, извършени на равнището на Съюза, включително координирани оценки на риска на критичните вериги на доставките в съответствие с член 22 от Директива (ЕС) 2022/2555, и

vi) съществуващите въведени мерки за контрол;

б) анализира вероятността и последиците от рисковете за киберсигурността, установени по буква а), и определя нивото на рисковете за киберсигурността, като прилага матрицата на въздействието на риска, използвана в методиките за оценка на рисковете за киберсигурността на равнището на Съюза, на регионално равнище и на равнището на държавите членки, разработени от ОПС със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС, в съответствие с член 19, параграф 2;

в) класифицира активите според възможните последствия при компрометиране на киберсигурността и определя периметъра на голямо въздействие и на критично въздействие, като използва следните стъпки:

i) извършване за всички процеси, попадащи в обхвата на оценката на рисковете за киберсигурността, на оценка на въздействието върху стопанската дейност, като се използва ЕСII;

ii) класифициране на даден процес като процес с голямо въздействие или с критично въздействие, ако неговият ЕСII надвишава прага съответно на голямо или на критично въздействие;

iii) определяне на всички активи с голямо въздействие и с критично въздействие като активите, необходими съответно за процесите с голямо въздействие и за тези с критично въздействие;

iv) определяне на периметрите на голямо въздействие и на критично въздействие, съдържащи съответно всички активи с голямо въздействие и активи с критично въздействие, така че да може да се контролира достъпът до периметрите;

г) оценява рисковете за киберсигурността, като ги степенува по приоритет с помощта на критериите за оценка на риска и критериите за приемане на риска, посочени в параграф 3, буква б).

5. По време на етапа на третиране на рисковете за киберсигурността всеки субект с голямо въздействие и с критично въздействие изготвя план за намаляване на рисковете за киберсигурността на равнище субект, като избира варианти за третиране на риска, подходящи за управление на рисковете, и определя остатъчните рискове.

6. По време на етапа на приемане на риска за киберсигурността всеки субект с голямо въздействие и с критично въздействие решава дали да приеме остатъчния риск въз основа на критериите за приемане на риска, установени в параграф 3, буква б).

7. Всеки субект с голямо въздействие и с критично въздействие регистрира активите, установени в параграф 1, в опис на активите. Този опис на активите не е част от доклада за оценка на риска.

8. Компетентният орган може да проверява активите в описа по време на проверките.

Член 27

Докладване относно оценката на рисковете на равнище субект

В рамките на 12 месеца след уведомяването на субектите с голямо въздействие и с критично въздействие съгласно член 24, параграф 6 и на всеки три години след това всеки субект с голямо въздействие и с критично въздействие предоставя на компетентния орган доклад, съдържащ следната информация:

1) списък на мерките за контрол, избрани за плана за намаляване на рисковете на равнище субект в съответствие с член 26, параграф 5, придружен от сведения за текущото състояние на изпълнението на всяка мярка за контрол;

2) за всеки процес с голямо въздействие в целия Съюз или процес с критично въздействие в целия Съюз — оценка на риска от компрометиране на поверителността, почтеността и на наличността на информацията, както и от компрометиране на съответните активи. Оценката на този риск се дава в съответствие с матрицата на въздействието на риска по член 19, параграф 2;

3) списък на доставчиците на ИКТ услуги с критично въздействие за неговите процеси с критично въздействие.

ГЛАВА III

ОБЩА РАМКА В ОБЛАСТТА НА КИБЕРСИГУРНОСТТА В ЕЛЕКТРОЕНЕРГЕТИКАТА

Член 28

Съдържание, функциониране и преразглеждане на общата рамка в областта на киберсигурността в електроенергетиката

1. Общата рамка в областта на киберсигурността в електроенергетиката се състои от следните мерки за контрол във връзка с киберсигурността и следната система за управление на киберсигурността:

а) минималните мерки за контрол във връзка с киберсигурността, разработени в съответствие с член 29;

б) разширените мерки за контрол във връзка с киберсигурността, разработени в съответствие с член 29;

в) матрицата на съответствията, разработена в съответствие с член 34, в която за мерките за контрол, посочени в букви а) и б), са дадени съответни връзки с избрани европейски и международни стандарти и национални законодателни или регулаторни рамки;

г) система за управление на киберсигурността, създадена в съответствие с член 32.

2. Всички субекти с голямо въздействие прилагат минималните мерки за контрол във връзка с киберсигурността в съответствие с параграф 1, буква а) в рамките на своя периметър на голямо въздействие.

3. Всички субекти с критично въздействие прилагат разширените мерки за контрол във връзка с киберсигурността в съответствие с параграф 1, буква б) в рамките на своя периметър на критично въздействие.

4. В рамките на 7 месеца след предаването на първия проектодоклад за оценка на рисковете за киберсигурността в целия Съюз в съответствие с член 19, параграф 4 общата рамка в областта на киберсигурността в електроенергетиката, посочена в параграф 1, се допълва от минималните и разширените мерки за контрол във връзка с киберсигурността по веригата на доставките, разработени в съответствие с член 33.

Член 29

Минимални и разширени мерки за контрол във връзка с киберсигурността

1. В рамките на 7 месеца след представянето на първия проектодоклад за оценка на рисковете за киберсигурността в целия Съюз съгласно член 19, параграф 4 ОПС, със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС, изготвят предложение за минимални и разширени мерки за контрол във връзка с киберсигурността.

2. В рамките на 6 месеца след изготвянето на всеки регионален доклад за оценка на рисковете за киберсигурността в съответствие с член 21, параграф 2 ОПС, със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС, предлагат на компетентния орган изменение на минималните и разширените мерки за контрол във връзка с киберсигурността. Предложението ще бъде направено в съответствие с член 8, параграф 10 и в него ще бъдат отчетени рисковете, установени при регионалната оценка на рисковете.

3. Минималните и разширените мерки за контрол във връзка с киберсигурността са проверими чрез участие в национална схема за проверка в съответствие с процедурата, посочена в член 31, или чрез провеждане на независими одити на сигурността от трети страни, извършени в съответствие с изискванията, изброени в член 25, параграф 2.

4. Първоначалните минимални и разширени мерки за контрол във връзка с киберсигурността, разработени съгласно параграф 1, се основават на рисковете, които са установени в доклада за оценка на рисковете за киберсигурността в целия Съюз, посочен в член 19, параграф 5. Изменените минимални и разширени мерки за контрол във връзка с киберсигурността, разработени в съответствие с параграф 2, се основават на регионалния доклад за оценка на рисковете за киберсигурността, посочен в член 21, параграф 2.

5. Минималните мерки за контрол във връзка с киберсигурността включват мерки за защита на информацията, обменяна съгласно член 46.

6. В рамките на 12 месеца след одобряването на минималните и на разширените мерки за контрол във връзка с киберсигурността съгласно член 8, параграф 5 или след всяка актуализация съгласно член 8, параграф 10 субектите, изброени в член 2, параграф 1 и определени като субекти с критично въздействие и субекти с голямо въздействие съгласно член 24, прилагат минималните мерки за контрол във връзка с киберсигурността в рамките на периметъра на голямо въздействие и разширените мерки за контрол във връзка с киберсигурността в рамките на периметъра на критично въздействие по време на изготвянето на плана за намаляване на рисковете за киберсигурността на равнище субект съгласно член 26, параграф 5.

Член 30

Дерогации от минималните и разширените мерки за контрол във връзка с киберсигурността

1. Изброените в член 2, параграф 1 субекти може да поискат от съответния компетентен орган да им предостави дерогация от задължението им да прилагат минималните и разширените мерки за контрол във връзка с киберсигурността, посочени в член 29, параграф 6. Компетентният орган може да предостави такава дерогация въз основа на едно от следните основания:

а) при изключителни обстоятелства, когато субектът може да докаже, че разходите за прилагане на подходящите мерки за контрол във връзка с киберсигурността значително надхвърлят ползите. С цел да се помогне на субектите, ACER и ЕМОПС за електроенергия в сътрудничество с ООРСЕС може да изготвят съвместно насоки за изчисляване на разходите за мерките за контрол във връзка с киберсигурността;

б) когато субектът предоставя план за третиране на рисковете на равнище субект, с който се намаляват рисковете за киберсигурността, като се използват алтернативни мерки за контрол до равнище, което е приемливо в съответствие с критериите за приемане на риска, посочени в член 26, параграф 3, буква б).

2. В срок от три месеца от получаването на посоченото в параграф 1 искане всеки компетентен орган решава дали трябва да предостави дерогация от минималните и разширените мерки за контрол във връзка с киберсигурността. Дерогациите от минималните или разширените мерки за контрол във връзка с киберсигурността се предоставят за максимален срок от три години, като е налице възможност за удължаване на срока.

3. Обобщена и анонимизирана информация за предоставените дерогации се включва като приложение към доклада за цялостна оценка на трансграничните рискове за киберсигурността в електроенергетиката, посочен в член 23. ЕМОПС за електроенергия и ООРСЕС актуализират съвместно списъка, когато това е необходимо.

Член 31

Проверка на общата рамка в областта на киберсигурността в електроенергетиката

1. Не по-късно от 24 месеца след приемането на мерките за контрол, посочени в член 28, параграф 1, букви а), б) и в), и създаването на системата за управление на киберсигурността, посочена в буква г) от въпросния член, всеки субект с критично въздействие, установен в съответствие с член 24, параграф 1, трябва да може да докаже, по искане на компетентния орган, че спазва системата за управление на киберсигурността и минималните или разширените мерки за контрол във връзка с киберсигурността.

2. Всеки субект с критично въздействие изпълнява задължението, посочено в параграф 1, като провежда независими одити на сигурността, извършвани от трета страна в съответствие с изискванията, посочени в член 25, параграф 2, или като участва в национална схема за проверка в съответствие с член 25, параграф 1.

3. Проверката, с която се установява спазване от страна на субект с критично въздействие на системата за управление на киберсигурността и на минималните или разширените мерки за контрол във връзка с киберсигурността, обхваща всички активи в рамките на периметъра на критично въздействие на субекта с критично въздействие.

4. Проверката, с която се установява спазване от страна на субект с критично въздействие на системата за управление на киберсигурността и на минималните или разширените мерки за контрол във връзка с киберсигурността, се повтаря периодично най-късно 36 месеца след края на първата проверка и на всеки 3 години след това.

5. Всеки субект с критично въздействие, определен в съответствие с член 24, доказва спазването от негова страна на мерките за контрол, посочени в член 28, параграф 1, букви а), б) и в), и създаването на система за управление на киберсигурността, посочена в буква г) от въпросния член, като докладва на компетентния орган резултатите от проверката на съответствието.

Член 32

Система за управление на киберсигурността

1. В срок от 24 месеца след уведомяването от компетентния орган за определянето му като субект с голямо въздействие или с критично въздействие в съответствие с член 24, параграф 6, всеки субект с голямо въздействие и с критично въздействие създава система за управление на киберсигурността и я преразглежда на всеки три години след това, за да:

а) определи обхвата на системата за управление на киберсигурността, като взема предвид интерфейсите и зависимостите с други субекти;

б) гарантира, че всички членове на висшето му ръководство са информирани за съответните правни задължения и активно допринасят за прилагането на системата за управление на киберсигурността чрез навременни решения и бързи реакции;

в) осигурява разполагаемост на ресурсите, необходими за системата за управление на киберсигурността;

г) въвежда политика за киберсигурност, която се документира и съобщава в рамките на субекта, както и на страните, засегнати от рисковете за сигурността;

д) възлага и съобщава отговорности във връзка с ролите, свързани с киберсигурността;

е) осъществява управлението на рисковете за киберсигурността на равнище субект, както е определено в член 26;

ж) определя и предоставя ресурсите, необходими за прилагането, поддръжката и непрекъснатото подобряване на системата за управление на киберсигурността, като се съобразява с необходимите компетентности и осведоменост за ресурсите в областта на киберсигурността;

з) определя вътрешната и външната комуникация, която е от значение за киберсигурността;

и) създава, актуализира и контролира документираната информация, свързана със системата за управление на киберсигурността;

й) оценява функционирането и ефективността на системата за управление на киберсигурността;

к) провежда вътрешни одити на планирани интервали с цел да се гарантира, че системата за управление на киберсигурността се прилага и поддържа ефективно;

л) преразглежда прилагането на системата за управление на киберсигурността на планирани интервали; и контролира и коригира несъответствието на ресурсите и дейностите с политиките, процедурите и насоките, засягащи системата за управление на киберсигурността.

2. Обхватът на системата за управление на киберсигурността включва всички активи в рамките на периметъра на голямо въздействие и на критично въздействие на субекта с голямо въздействие и с критично въздействие.

3. Компетентните органи, без да налагат употребата на определен тип технология или да упражняват дискриминация в нейна полза, насърчават използването на европейски или международни стандарти и спецификации, свързани със системите за управление, които са от значение за сигурността на мрежите и информационните системи.

Член 33

Минимални и разширени мерки за контрол във връзка с киберсигурността във веригата на доставките

1. В рамките на 7 месеца след представянето на първия проектодоклад за оценка на рисковете за киберсигурността в целия Съюз съгласно член 19, параграф 4 ОПС, със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС, разработват предложение за минимални и разширени мерки за контрол във връзка с киберсигурността по веригата на доставките, с което се намаляват рисковете за веригата на доставките, установени в оценките на рисковете за киберсигурността в целия Съюз, които да допълнят минималните и разширените мерки за контрол във връзка с киберсигурността, разработени в съответствие с член 29. Минималните и разширените мерки за контрол във връзка с киберсигурността във веригата на доставките се разработват заедно с минималните и разширените мерки за контрол във връзка с киберсигурността в съответствие с член 29. Минималните и разширените мерки за контрол във връзка с киберсигурността във веригата на доставките обхващат целия жизнен цикъл на всички ИКТ продукти, ИКТ услуги и ИКТ процеси в рамките на периметрите на критично въздействие и на голямо въздействие на субект с голямо въздействие или субект с критично въздействие. При разработването на предложението за минимални и разширени мерки за контрол във връзка с киберсигурността във веригата на доставките се провеждат консултации с групата за сътрудничество за МИС.

2. Минималните мерки за контрол във връзка с киберсигурността във веригата на доставките включват мерки за контрол за субекти с голямо въздействие и с критично въздействие, които:

а) включват препоръки за обществените поръчки за ИКТ продукти, ИКТ услуги и ИКТ процеси, посочени в спецификациите за киберсигурност, които обхващат най-малкото:

i) цялостни проверки на персонала на доставчика, който участва във веригата на доставките и работи с чувствителна информация, или който разполага с достъп до активите на субекта с голямо въздействие или с критично въздействие. Цялостната проверка може да включва проверка на самоличността и миналото на персонала или на изпълнителите на даден субект в съответствие с националното законодателство и процедури и съответното и приложимо право на Съюза, включително Регламент (ЕС) 2016/679 и Директива (ЕС) 2016/680 на Европейския парламент и на Съвета ([18]). Цялостните проверки са пропорционални и строго ограничени до това, което е необходимо. Те се извършват с единствената цел да се оцени възможен риск за сигурността на съответния субект. Проверките трябва да бъдат пропорционални на стопанските нужди, класификацията на информацията, до която се предоставя достъп, и усещането за рискове, и може да се извършват от самия субект, от външно дружество, извършващо скрининг, или чрез освобождаване от контрол на държавно равнище;

ii) процесите за сигурно и контролирано проектиране, разработване и производство на ИКТ продукти, ИКТ услуги и ИКТ процеси, насърчаване на проектирането и разработването на ИКТ продукти, ИКТ услуги и ИКТ процеси, които включват подходящи технически мерки за гарантиране на киберсигурността;

iii) проектирането на мрежи и информационни системи, в които устройствата са ненадеждни, дори когато са в рамките на защитен периметър, изискват се проверка на всички заявки, които се получават, и се прилага принципът на функциониране с най-малка привилегия;

iv) достъпа на доставчика до активите на субекта;

([18]) Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета (ОВ L 119, 4.5.2016 г., стр. 89).

v) договорните задължения по отношение на доставчика за защита и ограничаване на достъпа до чувствителна за субекта информация;

vi) основните спецификации за обществени поръчки в областта на киберсигурността за подизпълнители на доставчика;

vii) възможността за проследяване на прилагането на спецификациите за киберсигурност от разработването през производството до доставката на ИКТ продукти, ИКТ услуги или ИКТ процеси;

viii) поддръжката за актуализации във връзка със сигурността през целия експлоатационен срок на ИКТ продукти, ИКТ услуги или ИКТ процеси;

ix) правото на одит на киберсигурността в процесите на проектиране, разработване и производство на доставчика;

x) оценяването на рисковия профил на доставчика;

б) изисква се от такива субекти да вземат предвид посочените в буква а) препоръки за обществените поръчки при сключването на договори с доставчици, сътрудничещи партньори и други страни във веригата на доставките, които включват обичайни доставки на ИКТ продукти, ИКТ услуги и ИКТ процеси, както и нежелани събития и обстоятелства като прекратяване и промяна на договора в случай на небрежност от страна на договорния партньор;

в) изисква се от такива субекти да вземат предвид резултатите от съответните координирани оценки на риска за сигурността на критични вериги на доставките, извършвани в съответствие с член 22, параграф 1 от Директива (ЕС) 2022/2555;

г) включват се критерии за подбор и сключване на договори с доставчици, които могат да спазват спецификациите за киберсигурност, както е посочено в буква а), и които притежават равнище на киберсигурност, подходящо за рисковете за киберсигурността на ИКТ продукта, ИКТ услугата или ИКТ процесите, които доставя доставчикът;

д) включват се критерии за разнообразяване на източниците на доставка на ИКТ продукти, ИКТ услуги и ИКТ процеси и за намаляване на риска от зависимост от определен доставчик;

е) включват се критерии за редовно наблюдение, преразглеждане или одит на спецификациите за киберсигурност за вътрешни оперативни процеси на доставчика през целия експлоатационен срок на всеки ИКТ продукт, ИКТ услуга и ИКТ процес.

3. По отношение на спецификациите за киберсигурност в препоръката относно обществени поръчки в областта на киберсигурността, посочени в параграф 2, буква а), субектите с голямо въздействие или с критично въздействие използват принципите на обществените поръчки съгласно Директива 2014/24/ЕС на Европейския парламент и на Съвета ([19]), в съответствие с член 35, параграф 4, или определят свои собствени спецификации въз основа на резултатите от оценката на рисковете за киберсигурността на равнище субект.

4. Разширените мерки за контрол във връзка с киберсигурността във веригата на доставките включват мерки за контрол за субекти с критично въздействие, целящи по време на обществените поръчки да се провери дали ИКТ продуктите, ИКТ услугите и ИКТ процесите, които ще бъдат използвани като активи с критично въздействие, отговарят на спецификациите за киберсигурност. ИКТ продуктът, ИКТ услугата или ИКТ процесът се проверяват или чрез посочената в член 31 европейска схема за сертифициране на киберсигурността, или чрез дейности за проверка, избрани и организирани от субекта. Задълбочеността и обхватът на дейностите за проверка трябва да са достатъчни, за да осигурят увереност, че ИКТ продуктът, ИКТ услугата или ИКТ процесът може да се използва за намаляване на рисковете, установени в оценката на рисковете на равнище субект. Субектът с критично въздействие документира стъпките, предприети за намаляване на установените рискове.

5. Минималните и разширените мерки за контрол във връзка с киберсигурността във веригата на доставките се прилагат по отношение на обществени поръчки за съответните ИКТ продукти, ИКТ услуги и ИКТ процеси. Минималните и разширените мерки за контрол във връзка с киберсигурността по веригата на доставките ще се прилагат по отношение на процеси за обществени поръчки в субектите, установени като субекти с критично въздействие и с голямо въздействие в съответствие с член 24, като началото ще бъде поставено шест месеца след приемането или актуализирането на минималните и разширените мерки за контрол във връзка с киберсигурността, посочени в член 29.

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

6. В срок от 6 месеца след изготвянето на всеки регионален доклад за оценка на рисковете за киберсигурността в съответствие с член 21, параграф 2 ОПС, със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС, предлагат на компетентния орган изменение на минималните и разширените мерки за контрол във връзка с киберсигурността по веригата на доставките. Предложението ще бъде направено в съответствие с член 8, параграф 10 и в него ще бъдат отчетени рисковете, установени при регионалната оценка на рисковете.

Член 34

Матрица на съответствията между мерките за контрол във връзка с киберсигурността в електроенергетиката и съществуващи стандарти

1. В рамките на 7 месеца след представянето на първия проектодоклад за оценка на рисковете за киберсигурността в целия Съюз съгласно член 19, параграф 4 ОПС, със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС и като се консултират с ENISA, разработват предложение за матрица за съпоставяне на мерките за контрол, определени в член 28, параграф 1, букви а) и б) с избрани европейски и международни стандарти, както и съответните технически спецификации („матрица на съответствията“). ЕМОПС за електроенергия и ООРСЕС документират еквивалентността на различните мерки за контрол с мерките за контрол, определени в член 28, параграф 1, букви а) и б).

2. Компетентните органи може да предоставят на ЕМОПС за електроенергия и на ООРСЕС съпоставяне на мерките за контрол, определени в член 28, параграф 1, букви а) и б), като се позоват на съответните национални законодателни или регулаторни рамки, включително относимите национални стандарти на държавите членки в съответствие с член 25 от Директива (ЕС) 2022/2555. Ако компетентният орган на държава членка предостави такова съпоставяне, ЕМОПС за електроенергия и ООРСЕС интегрират това съпоставяне на национално равнище в матрицата на съответствията.

3. В рамките на 6 месеца след изготвянето на всеки регионален доклад за оценка на рисковете за киберсигурността в съответствие с член 21, параграф 2 ОПС, със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС и като се консултират с ENISA, предлагат на компетентния орган изменение във връзка с матрицата на съответствията. Предложението ще бъде направено в съответствие с член 8, параграф 10 и в него ще бъдат отчетени рисковете, установени при регионалната оценка на рисковете.

ГЛАВА IV

ПРЕПОРЪКИ ОТНОСНО ОБЩЕСТВЕНИ ПОРЪЧКИ В ОБЛАСТТА НА КИБЕРСИГУРНОСТТА

Член 35

Препоръки относно обществени поръчки в областта на киберсигурността

1. ОПС, със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС, разработват в рамките на работна програма, която трябва да се изготви и актуализира всеки път при приемането на регионален доклад за оценка на рисковете за киберсигурността, набор от необвързващи препоръки относно обществени поръчки в областта на киберсигурността, които субекти с критично въздействие или с голямо въздействие може да използват като основа за обществените поръчки за ИКТ продукти, ИКТ услуги и ИКТ процеси в рамките на периметрите на голямо въздействие и на критично въздействие. Тази работна програма включва следното:

а) описание и класификация на видовете ИКТ продукти, ИКТ услуги и ИКТ процеси, използвани от субекти с голямо въздействие и с критично въздействие в рамките на периметъра на голямо въздействие и на критично въздействие;

б) списък на видовете ИКТ продукти, ИКТ услуги и ИКТ процеси, за които се разработва набор от необвързващи препоръки относно обществени поръчки в областта на киберсигурността, който се основава на съответните регионални доклади за оценка на рисковете за киберсигурността и на приоритетите на субектите с голямо въздействие и субектите с критично въздействие.

2. в рамките на 6 месеца след приемането или актуализирането на регионалния доклад за оценка на рисковете за киберсигурността ЕМОПС за електроенергия, в сътрудничество с ООРСЕС, предоставя на ACER обобщение на тази работна програма.

3. ОПС, със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС, се стремят да гарантират, че необвързващите препоръки относно обществени поръчки в областта на киберсигурността, разработени въз основа на съответната регионална оценка на рисковете за киберсигурността, са подобни или сравними между отделните региони на експлоатация на системата. Наборите от препоръки относно обществени поръчки в областта на киберсигурността обхващат най-малкото спецификациите, посочени в член 33, параграф 2, буква а). Когато е възможно, спецификациите се избират от европейски и международни стандарти.

4. ОПС, със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС, гарантират, че наборите от препоръки за обществени поръчки в областта на киберсигурността:

а) са съобразени с принципите на обществените поръчки съгласно Директива 2014/24/ЕС; и

б) са съвместими и съобразени с най-новите налични европейски схеми за сертифициране на киберсигурността, относими към съответния ИКТ продукт, ИКТ услуга или ИКТ процес.

Член 36

Насоки относно европейските схеми за сертифициране на киберсигурността за обществени поръчки за ИКТ продукти, ИКТ услуги или ИКТ процеси.

1. Необвързващите препоръки относно обществени поръчки в областта на киберсигурността, разработени съгласно член 35, може да включват специфични за сектора насоки относно използването на европейски схеми за сертифициране на киберсигурността, когато за използвания от субекти с критично въздействие тип ИКТ продукт, ИКТ услуга или ИКТ процес е налице подходяща схема, без да се засяга рамката за установяване на европейски схеми за сертифициране на киберсигурността съгласно член 46 от Регламент (ЕС) 2019/881.

2. ОПС, със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС, си сътрудничат тясно с ENISA при предоставяне на специфични за сектора насоки, включени в необвързващите препоръки относно обществени поръчки в областта на киберсигурността, посочени в параграф 1.

ГЛАВА V

ИНФОРМАЦИОННИ ПОТОЦИ, КИБЕРАТАКИ И УПРАВЛЕНИЕ НА КРИЗИ

Член 37

Правила относно обмена на информация

1. Ако компетентен орган получава информация, свързана с подлежаща на докладване кибератака, този компетентен орган:

а) оценява степента на поверителност на тази информация и информира субекта за резултата от своята оценка без ненужно забавяне и не по-късно от 24 часа след получаване на информацията;

б) прави опит да намери всяка друга подобна кибератака в Съюза, докладвана на други компетентни органи, за да съпостави информацията, получена в контекста на подлежащата на докладване кибератака, с информацията, предоставена в контекста на други кибератаки, и да обогати съществуващата информация, да укрепи и да координира реакциите в областта на киберсигурността;

в) носи отговорност за заличаването на търговските тайни и анонимизирането на информацията в съответствие със съответните национални правила и правилата на Съюза;

г) без ненужно забавяне и не по-късно от 24 часа след приемането на информация за подлежаща на докладване кибератака обменя информацията с националните единни звена за контакт, ЕРИКС и всички компетентни органи, определени съгласно член 4 в други държави членки и редовно предоставя актуализирана информация на тези органи или структури;

д) без ненужно забавяне и не по-късно от 24 часа след получаване на информацията съгласно параграф 1, буква а) разпространява информацията за кибератаката, след анонимизирането и заличаването на търговските тайни съгласно параграф 1, буква в), до субекти с критично въздействие и с голямо въздействие в своята държава членка и редовно предоставя актуализирана информация, позволяваща на субектите да организират ефективно защитата си;

е) може да поиска от докладващия субект с голямо въздействие или с критично въздействие да разпространи допълнително и по сигурен начин до други субекти, които може да бъдат засегнати, информацията за подлежаща на докладване кибератака, за да получи от сектора на електроенергетиката осведоменост за състоянието и да предотврати проявлението на риск, който може да ескалира при трансграничен киберинцидент, свързан с електроенергия;

ж) споделя с ENISA обобщаващ доклад, след анонимизирането и заличаването на търговските тайни, който съдържа информация за кибератаката.

2. Ако ЕРИКС разбере за некоригирана активно използвана уязвимост, той:

а) споделя информацията незабавно с ENISA чрез подходящ защитен канал за обмен на информация, освен ако не е посочено друго в правото на Съюза;

б) подпомага съответния субект да получи от производителя или доставчика ефективно, координирано и бързо управление на некоригираната активно експлоатирана уязвимост или на ефективни и ефикасни мерки за намаляване на рисковете;

в) обменя наличната информация с оператор и иска от производителя или доставчика, когато това е възможно, да определи списък на ЕРИКС в държавите членки, засегнати от некоригираната активно използвана уязвимост, като за това трябва да бъде съобщено;

г) споделя наличната информация с набелязаните съгласно предходната буква ЕРИКС въз основа на принципа „необходимост да се знае“;

д) споделя, когато са налични, стратегии за намаляване на рисковете и мерки за докладваната некоригирана активно използвана уязвимост.

3. Ако компетентен орган узнае за некоригирана активно използвана уязвимост, този компетентен орган:

а) споделя, когато са налични, стратегии и мерки за намаляване на рисковете за докладваната некоригирана активно използвана уязвимост в координация с другите ЕРИКС в неговата държава членка;

б) споделя информацията с ЕРИКС в държавата членка, в която е докладвана некоригираната активно използвана уязвимост.

4. Ако компетентният орган узнае за некоригирана уязвимост, без да са налице доказателства, че тя вече се използва активно, той се координира без ненужно забавяне с ЕРИКС за целите на координираното оповестяване на уязвимости, определено в член 12, параграф 1 от Директива (ЕС) 2022/2555.

5. Ако ЕРИКС получи информация, свързана с киберзаплахи от един или от няколко субекта с голямо въздействие или с критично въздействие в съответствие с член 38, параграф 6, той разпространява тази информация или всяка друга информация, която е от значение за предотвратяване, откриване, оттоваряне или намаляване на съответните рискове за субекти с критично въздействие и с голямо въздействие в своята държава членка и, когато е целесъобразно, до всички съответни ЕРИКС и до своето национално единно звено за контакт, без ненужно забавяне и не по-късно от четири часа след получаването на информацията.

6. Ако компетентен орган узнае информация, свързана с киберзаплахи от един или от няколко субекта с голямо въздействие или с критично въздействие, той препраща тази информация на ЕРИКС за целите на параграф 5.

7. Компетентните органи може да делегират изцяло или частично отговорностите по параграфи 3 и 4, засягащи един или повече субекти с голямо въздействие или с критично въздействие, които работят в повече от една държава членка, на друг компетентен орган в една от тези държави членки след споразумение между засегнатите компетентни органи.

8. ОПС, със съдействието на ЕМОПС за електроенергия и в сътрудничество с ООРСЕС, разработват методика за скала за класификация на кибератаките до 13 юни 2025 г. ОПС, със съдействието на ЕМОПС за електроенергия и ООРСЕС, може да поискат от компетентните органи да проведат консултации с ENISA и с техните компетентни органи, отговарящи за киберсигурността, във връзка с помощта при разработването на такава скала за класификация. С методиката се предоставя класификация за тежестта на кибератака в 5 степени, като двете най-високи степени са „голяма“ и „критична“. Класификацията се основава на оценката на следните параметри:

а) потенциалното въздействие, като се вземат предвид изложените активи и периметри, определени в съответствие с член 26, параграф 4, буква в); и

б) сериозността на кибератаката.

9. До 13 юни 2026 г. ЕМОПС за електроенергия, в сътрудничество с ООРСЕС, извършва проучване за осъществимост, за да оцени възможността и финансовите разходи, необходими за разработването на общ инструмент, позволяващ на всички субекти да обменят информация със съответните национални органи.

10. В проучването за осъществимост се разглежда възможността такъв общ инструмент:

а) да се ползва за подкрепяне на субектите с критично въздействие и с голямо въздействие чрез съответната свързана със сигурността информация за операции на трансгранични потоци на електроенергия, чрез докладване почти в реално време за кибератаки, чрез ранни предупреждения, свързани с въпроси на киберсигурността и неразкрити уязвимости на използваното в електроенергийната система оборудване;

б) да бъде поддържан в подходяща и високо надеждна среда;

в) да позволява събиране на данни от субекти с критично въздействие и с голямо въздействие и да улеснява заличаването на поверителна информация и анонимизирането на данните и бързото им разпространение до субекти с критично въздействие и с голямо въздействие.

11. ЕМОПС за електроенергия, в сътрудничество с ООРСЕС:

а) се консултира с ENISA и групата за сътрудничество за МИС, националните единни звена за контакт и представителите на основните заинтересовани страни при оценката на осъществимостта;

б) представя резултатите от проучването за осъществимост на ACER и на групата за сътрудничество за МИС.

12. ЕМОПС за електроенергия, в сътрудничество с ООРСЕС, може да анализира и да улесни предлаганите от субекти с критично въздействие и с голямо въздействие инициативи, за да се оценят и изпитат такива инструменти за обмен на информация.

Член 38

Роля на субектите с голямо въздействие и с критично въздействие по отношение на обмена на информация

1. Всеки субект с голямо въздействие и с критично въздействие:

а) установява за всички активи в рамките на своя периметър на киберсигурност, определен съгласно член 26, параграф 4, буква в), най-малкото способностите на ОЦКС:

i) да гарантира, че съответните мрежи и информационни системи и приложения предоставят регистри за сигурност за следене на сигурността, за да се даде възможност за откриване на аномалии и събиране на информация относно кибератаки;

ii) да извършва следене на сигурността, включително откриване на прониквания и оценка на уязвимостите на мрежите и информационните системи;

iii) да анализира и, когато е необходимо, да предприема всички необходими действия съгласно собствената си отговорност и способност да защитава субекта;

iv) да участва в посочените в настоящия член събиране и обмен на информация;

б) има право да закупува чрез ДУУС всички тези способности или части от тях съгласно буква а). Субектите с критично въздействие и с голямо въздействие продължават да носят отговорност за ДУУС и осъществяват контрол върху техните усилия;

в) определят единно звено за контакт на равнище субект за целите на обмена на информация.

2. ENISA може да издава необвързващи насоки за установяване на такива способности или за възлагане на услугата на ДУУС като подизпълнители като част от задачата, определена в член 6, параграф 2 от Регламент (ЕС) 2019/881.

3. Всеки субект с критично въздействие и с голямо въздействие обменя със своя ЕРИКС и със своя компетентен орган съответната информация, свързана с подлежаща на докладване кибератака, без ненужно забавяне и не по-късно от четири часа след като е узнал, че инцидентът подлежи на докладване.

4. Свързана с кибератака информация се счита за подлежаща на докладване, когато кибератаката се оценява от засегнатия субект с ниво на критичност, вариращо от „голямо“ до „критично“ въздействие, като се следва методиката за скала за класификация на кибератаките съгласно член 37, параграф 8. Единното звено за контакт на равнище субект, определено съгласно параграф 1, буква в), съобщава класификацията на инцидента.

5. Когато субекти с критично въздействие и с голямо въздействие уведомяват ЕРИКС за съответната информация, свързана с некоригирани активно използвани уязвимости, ЕРИКС може да препрати тази информация на своя компетентен орган. С оглед на степента на чувствителност на нотифицираната информация, ЕРИКС може да задържи информацията или да забави нейното препращане поради основателни причини, свързани с киберсигурността.

6. Всеки субект с критично въздействие и с голямо въздействие предоставя без ненужно забавяне на своите ЕРИКС всяка информация, свързана с подлежаща на докладване киберзаплаха, която може да има трансгранично въздействие. Свързаната с киберзаплаха информация се счита за подлежаща на докладване, когато е изпълнено поне едно от следните условия:

а) тя предоставя подходящи сведения за други субекти с критично въздействие и с голямо въздействие във връзка с предотвратяване, откриване, реагиране или намаляване на въздействието на риска;

б) в резултат на използваните в контекста на дадена атака установени техники, тактики и процедури се придобива информация като компрометирани URL адреси или IP адреси, хеш кодове или всеки друг атрибут, който е от полза за даване на контекст и за установяване на връзката с атаката;

в) киберзаплаха може да бъде допълнително оценена и да бъде поставена в контекст с допълнителна информация, предоставена от доставчици на услуги или трети страни, които не са предмет на настоящия регламент.

7. Когато обменя информация съгласно настоящия член, всеки субект с критично въздействие и с голямо въздействие уточнява следното:

а) че информацията се предоставя съгласно настоящия регламент;

б) дали информацията се отнася до:

i) подлежаща на докладване кибератака, посочена в параграф 3;

ii) некоригирани активно използвани уязвимости, които не са публично известни, както са посочени в параграф 4;

iii) подлежаща на докладване киберзаплаха, посочена в параграф 5;

в) в случай на подлежаща на докладване киберзаплаха — степента на кибератаката според методиката за скала за класификация на кибератаките, посочена в член 37, параграф 8, и информацията, водеща до тази класификация, включително най-малко критичността на кибератаката.

8. Когато субект с критично въздействие или с голямо въздействие уведоми за значителен инцидент съгласно член 23 от Директива (ЕС) 2022/2555 и докладването на инцидент съгласно посочения член съдържа съответната информация, изисквана съгласно параграф 3 от настоящия член, докладването от страна на субекта съгласно член 23, параграф 1 от тази директива представлява докладване на информация съгласно параграф 3 от настоящия член.

9. Всеки субект с критично въздействие или с голямо въздействие докладва на своя компетентен орган или ЕРИКС, като ясно определя конкретна информация, която може да бъде обменена само с компетентния орган или с ЕРИКС в случаи, в които обменяната информация може да бъда източник на кибератака. Всеки субект с критично въздействие или с голямо въздействие има правото да предоставя на компетентния ЕРИКС неповерителна версия на информацията.

Член 39

Установяване на кибератаки и обработване на свързана с тях информация

1. Субектите с критично въздействие и с голямо въздействие изграждат необходимите способности за справяне с откритите кибератаки, заедно с необходимата подкрепа от страна на съответния компетентен орган, ЕМОПС за електроенергия и ООРСЕС. Субектите с критично въздействие и с голямо въздействие може да бъдат подкрепени от ЕРИКС, определен в съответната им държава членка, като част от възложената на ЕРИКС задача по член 11, параграф 5, буква а) от Директива (ЕС) 2022/2555. Субектите с критично въздействие и с голямо въздействие изпълняват ефективно процесите за установяване, класифициране и реагиране на киберзаплахи, които ще засегнат или може да засегнат трансграничните потоци на електроенергия с цел да се сведе до минимум тяхното въздействие.

2. Ако трансграничните потоци на електроенергия бъдат засегнати от кибератака, единните звена за контакт на равнище субект на засегнатите субекти с критично въздействие и с голямо въздействие си сътрудничат, за да обменят помежду си информация, координирана от компетентния орган на държавата членка, в която е докладвано за първи път за кибератаката.

3. Субектите с критично въздействие и с голямо въздействие:

а) гарантират, че тяхното собствено единно звено за контакт на равнище субект има достъп въз основа на принципа „необходимост да се знае“ до информацията, която са получили от националното единно звено за контакт чрез неговия компетентен орган;

б) освен ако вече не е направено съгласно член 3, параграф 4 от Директива (ЕС) 2022/2555, уведомяват компетентния орган на държавата членка, в която са установени, и националното единно звено за контакт за списъка на техните единни звена за контакт, отговорни за киберсигурността, на равнище субект:

i) от които този компетентен орган и националното единно звено за контакт може да очакват да получат информация за подлежащи на докладване кибератаки;

ii) на които може да се наложи компетентните органи и националните единни звена за контакт да предоставят информация;

в) установяват процедури за управление на кибератаки във връзка с кибератаки, включително роли и отговорности, задачи и реакции въз основа на наблюдаваното развитие на кибератаката в рамките на периметъра на критично въздействие и на голямо въздействие;

г) изпробват цялостните процедури за управление на кибератаки поне веднъж годишно, като изпробват поне един сценарий, засягащ пряко или косвено трансграничните потоци на електроенергия. Това ежегодно изпробване може да се провежда от субекти с критично въздействие и с голямо въздействие по време на редовните учения, посочени в член 43. Всяка дейност за реагиране на кибератаки на живо с последствия, класифицирани най-малко в скала 2 съгласно методиката за скала за класификация на кибератаките, посочена в член 37, параграф 8 и чиято първопричина е киберсигурността, може да служи за годишно изпробване на плана за реакция при кибератака.

4. Изброените в параграф 1 задачи може да бъдат делегирани от държавите членки също и на регионалните координационни центрове в съответствие с член 37, параграф 2 от Регламент (ЕС) 2019/943.

Член 40

Управление на кризи

1. Когато компетентният орган установи, че дадена криза в електроснабдяването е свързана с кибератака, която оказва въздействие върху повече от една държава членка, компетентните органи от засегнатите държави членки, КООКС, КО — ГСР и органите за управление на киберкризи в МИС от засегнатите държави членки създават съвместно *ad hoc* група за координация при трансгранични кризи.

2. Ad hoc групата за координация при трансгранични кризи:

а) координира ефикасното извличане и по-нататъшното разпространение на цялата съответна свързана с киберсигурността информация до субектите, участващи в процеса на управление на кризи;

б) организира комуникацията между всички засегнати от кризата субекти и компетентните органи с цел да се намалят припокриванията и да се повиши ефикасността на анализите и техническите реакции за отстраняване на едновременните кризи в електроснабдяването, чиято първопричина е киберсигурността;

в) предоставя на засегнати от инцидента субекти, в сътрудничество с компетентните ЕРИКС, необходимия експертен опит, включително оперативни съвети относно прилагането на възможни мерки за намаляване на рисковете;

г) уведомява и предоставя редовни актуализации относно състоянието на инцидента на Комисията и на Групата за координация в областта на електроенергетиката, като следва принципите на защита, определени в член 46;

д) търси съвет от съответните органи, агенции или субекти, които може да бъдат от помощ за смекчаването на кризата в електроснабдяването.

3. Когато кибератаката се квалифицира или се очаква да се квалифицира като мащабен киберинцидент, *ad hoc* групата за координация при трансгранични кризи незабавно информира националните органи за управление на киберкризи в съответствие с член 9, параграф 1 от Директива (ЕС) 2022/2555 в засегнатите от инцидента държави членки, както и Комисията и EU-CyCLONe. В тази ситуация *ad hoc* групата за координация при трансгранични кризи подпомага EU-CyCLONe по отношение на секторните особености.

4. Субектите с критично въздействие и с голямо въздействие разработват и притежават способности, вътрешни насоки, планове за готовност за справяне с рисковете и персонал, който да участва в откриването и ограничаването на трансгранични кризи. Субектът с критично въздействие или с голямо въздействие, засегнат от едновременна криза в електроснабдяването, проучва първопричината за такава криза в сътрудничество със своя компетентен орган с цел да се определи степента, в която кризата е свързана с кибератака.

5. Задачите в параграф 4 може да бъдат делегирани от държавите членки и на регионалните координационни центрове в съответствие с член 37, параграф 2 от Регламент (ЕС) 2019/943.

Член 41

Планове за управление и реакция при кризи в областта на киберсигурността

1. В срок от 24 месеца след уведомяването на ACER за доклада за оценка на рисковете в целия Съюз ACER, в тясно сътрудничество с ENISA, ЕМОПС за електроенергия, ООРСЕС, КООКС, компетентните органи, КО — ГСР, НРО и националните органи, отговорни за управлението на киберкризи в МИС, разработват план за управление и реакция при кризи в областта на киберсигурността на равнището на Съюза във връзка с електроенергетиката.

2. В срок от 12 месеца след разработването от ACER на план за управление и реакция при кризи в областта на киберсигурността на равнището на Съюза във връзка с електроенергетиката съгласно параграф 1, всеки компетентен орган разработва национален план за управление и реакция при кризи в областта на киберсигурността за трансгранични потоци на електроенергия, като взема предвид плана за управление на кризи в областта на киберсигурността на равнището на Съюза и националния план за готовност за справяне с рисковете, създаден в съответствие с член 10 от Регламент (ЕС) 2019/941. Този план е в съответствие с плана за реакция при мащабни киберинциденти и кризи съгласно член 9, параграф 4 от Директива (ЕС) 2022/2555. Компетентният орган координира дейността си със субектите с критично въздействие и с голямо въздействие и с КО — ГСР в своята държава членка.

3. Изискваният съгласно член 9, параграф 4 от Директива (ЕС) 2022/2555 национален план за реакция при мащабни киберинциденти и кризи се счита за национален план за управление на кризи в областта на киберсигурността при кризи съгласно посочения член, ако включва разпоредби за управление и реакция при кризи във връзка с трансграничните потоци на електроенергия.

4. Изброените в параграфи 1 и 2 задачи може да бъдат делегирани от държавите членки и на регионалните координационни центрове в съответствие с член 37, параграф 2 от Регламент (ЕС) 2019/943.

5. Субектите с критично въздействие и с голямо въздействие гарантират, че техните процеси за управление на кризи, свързани с киберсигурността:

а) имат съвместими процедури за предприемане на действия при трансгранични инциденти, свързани с киберсигурността, както е определено в член 6, точка 8 от Директива (ЕС) 2022/2555, официално включени в техните планове за управление на кризи;

б) са част от общите дейности за управление на кризи.

6. В срок от 12 месеца след уведомяването на субектите с голямо въздействие и с критично въздействие съгласно член 24, параграф 6 и на всеки три години след това субектите с критично въздействие и с голямо въздействие разработват план за управление на кризи на равнище субект за свързана с киберсигурността криза, който се включва в техните общи планове за управление на кризи. Този план включва най-малкото следното:

а) правила за обявяване на криза, както е посочено в член 14, параграфи 2 и 3 от Регламент (ЕС) 2019/941;

б) ясни роли и отговорности за управление на кризи, включително ролята на други съответни субекти с критично въздействие и с голямо въздействие;

в) актуална информация за контакт, както и правила за комуникация и обмен на информация по време на кризисна ситуация, включително връзка с ЕРИКС.

7. Мерките за управление на кризи в съответствие с член 21, параграф 2, буква в) от Директива (ЕС) 2022/2555 се считат за план за управление на кризи на равнище субект във връзка с електроенергетиката съгласно настоящия член, ако той включва всички изисквания, изброени в параграф 6.

8. Плановете за управление на кризи се изпробват по време на ученията в областта на киберсигурността, посочени в членове 43, 44 и 45.

9. Субектите с критично и с голямо въздействие включват плановете си за управление на кризи на равнище субект в своите планове за непрекъснатост на дейността във връзка с процесите с критично въздействие и с голямо въздействие. Плановете за управление на кризи на равнище субект включват:

а) процеси в зависимост от разполагаемостта, стабилността и надеждността на ИТ услугите;

б) всички местоположения за непрекъснатост на дейността, включително местоположенията за апаратна част и програмно осигуряване;

в) всички вътрешни роли и отговорности, свързани с процесите на непрекъснатост на дейността.

10. Субектите с критично въздействие и с голямо въздействие актуализират своите планове за управление на кризи на равнище субект поне на всеки три години и когато това е необходимо.

11. ACER актуализира плана за управление и реакция при кризи в областта на киберсигурността на равнището на Съюза във връзка с електроенергетиката, разработен съгласно параграф 1, поне на всеки три години и когато това е необходимо.

12. Всеки компетентен орган актуализира националния план за управление и реакция при кризи в областта на киберсигурността във връзка с трансграничните потоци на електроенергия, разработен съгласно параграф 2, поне на всеки три години и когато това е необходимо.

13. Субектите с критично въздействие и с голямо въздействие изпробват своите планове за непрекъснатост на дейността поне веднъж на всеки три години или след големи промени в процес с критично въздействие. Резултатът от изпробванията на плана за непрекъснатост на дейността се документират. Субектите с критично въздействие и с голямо въздействие може да включват в ученията в областта на киберсигурността изпробването на своя план за непрекъснатост на дейността.

14. Субектите с критично въздействие и с голямо въздействие актуализират своя план за непрекъснатост на дейността винаги когато е необходимо и поне веднъж на всеки три години, като вземат предвид резултата от изпробването.

15. Ако при изпробване са установени недостатъци в плана за непрекъснатост на дейността, субектът с критично въздействие и с голямо въздействие коригира тези недостатъци в срок от 180 календарни дни след изпробването и провежда ново изпробване, за да предостави доказателства за ефективността на коригиращите мерки.

16. Когато субект с критично въздействие или с голямо въздействие не може да коригира недостатъците в срок от 180 календарни дни, той включва причините в доклада, който трябва да бъде предоставен на неговия компетентен орган в съответствие с член 27.

Член 42

Възможности за ранно предупреждение във връзка с киберсигурността за електроенергетиката

1. Компетентните органи си сътрудничат с ENISA за разработването на възможности за ранно предупреждение за киберсигурността в електроенергетиката (ECEAC) като част от помощта за държавите членки съгласно член 6, параграфи 2 и 7 от Регламент (ЕС) 2019/881.

2. ECEAC дават възможност на ENISA при изпълнение на задачите, изброени в член 7, параграф 7 от Регламент (ЕС) 2019/881:

а) да събира доброволно обменената информация от:

i) ЕРИКС, компетентните органи;

ii) субектите, изброени в член 2 от настоящия регламент;

iii) всеки друг субект, който желае да обмени доброволно съответната информация;

б) да събира и класифицира събраната информация;

в) да оценява информацията, до която ENISA има достъп, за да се установят условията на киберриск и съответните показатели във връзка с аспекти на трансграничните потоци на електроенергия;

г) да установи условията и показателите, които често са свързани с кибератаки в рамките на електроенергетиката;

д) да определя дали следва да се предприемат допълнителни анализи и превантивни действия чрез оценка и установяване на рискови фактори;

е) да информира компетентните органи относно установените рискове и препоръчаните превантивни действия, специфични за съответните субекти;

ж) да информира всички съответни изброени в член 2 субекти за резултатите от информацията, оценена в съответствие с букви б), в) и г) от настоящия параграф;

з) периодично да включва съответната информация в доклада за осведоменост за състоянието, изготвен в съответствие с член 7, параграф 6 от Регламент (ЕС) 2019/881;

и) да извлича, когато е възможно, от събраната информация приложими данни, които показват потенциално нарушение на сигурността или кибератака („показатели за компрометиране на системите“).

3. ЕРИКС разпространяват незабавно получената от ENISA информация до съответните субекти в рамките на своите задачи, определени в член 11, параграф 3, буква б) от Директива (ЕС) 2022/2555.

4. ACER наблюдава ефективността на ECEAC. ENISA оказва помощ на ACER чрез предоставяне на цялата необходима информация съгласно член 6, параграф 2 и член 7, параграф 1 от Регламент (ЕС) 2019/881. Анализът на настоящата дейност за наблюдение е част от наблюдението съгласно член 12 от настоящия регламент.

ГЛАВА VI

РАМКА ЗА УЧЕНИЯ В ОБЛАСТТА НА КИБЕРСИГУРНОСТТА

Член 43

Учения в областта на киберсигурността на равнище субект и на равнище държава членка

1. До 31 декември на годината след уведомяването на субектите с критично въздействие и на всеки три години след това всеки субект с критично въздействие провежда учения в областта на киберсигурността, които включват един или повече сценарии с кибератаки, засягащи пряко или косвено трансграничните потоци на електроенергия и свързани с рисковете, установени по време на оценките на рисковете за киберсигурността на равнище държава членка и на равнище субект в съответствие с член 20 и член 27.

2. Чрез дерогация от параграф 1 КО — ГСР, след консултация с компетентния орган и съответния орган за управление на киберкризи, определен или създаден съгласно член 9 от Директива (ЕС) 2022/2555, може да реши, вместо да провежда учения в областта на киберсигурността на равнище субект, да организира учения в областта на киберсигурността на равнище държава членка, както е посочено в параграф 1. Във връзка с това компетентният орган информира:

а) всички субекти с критично въздействие на своята държава членка, НРО, ЕРИКС и КООКС — най-късно до 30 юни на годината, предхождаща ученията в областта на киберсигурността на равнище субект;

б) всеки субект, който ще участва в ученията в областта на киберсигурността на равнище държава членка — най-късно 6 месеца преди провеждането на ученията.

3. КО — ГСР с техническата подкрепа на своите ЕРИКС организира посочените в параграф 2 учения в областта на киберсигурността на равнище държава членка, независимо или в контекста на друго учение в областта на киберсигурността във въпросната държава членка. За да може да групира тези учения, КО — ГСР може да отложи посочените в параграф 1 учения в областта на киберсигурността на равнище държава членка с една година.

4. Ученията в областта на киберсигурността на равнище субект и на равнище държава членка са в съответствие с националните рамки за управление на кризи в областта на киберсигурността в съответствие с член 9, параграф 4, буква г) от Директива (ЕС) 2022/2555.

5. До 31 декември 2026 г. и на всеки три години след това ЕМОПС за електроенергия, в сътрудничество с ООРСЕС, предоставя образец за сценарий на учения за провеждането на учения в областта на киберсигурността на равнище субект и на равнище държава членка, посочени в параграф 1. В този образец се вземат предвид резултатите от най-скорошната оценка на рисковете за киберсигурността на равнище субект и на равнище държава членка и се съдържат ключови критерии за успех. ЕМОПС за електроенергия и ООРСЕС включват ACER и ENISA в разработването на такъв образец.

Член 44

Регионални или междурегионални учения в областта на киберсигурността

1. До 31 декември 2029 г. и на всеки три години след това във всеки регион на експлоатация на системата ЕМОПС за електроенергия, в сътрудничество с ООРСЕС, организира регионално учение в областта на киберсигурността. В регионалното учение в областта на киберсигурността участват субектите с критично въздействие в региона на експлоатация на системата. ЕМОПС за електроенергия, в сътрудничество с ООРСЕС, може вместо да организира учение в областта на киберсигурността, да организира междурегионално учение в областта на киберсигурността в повече от един регион на експлоатация на системата в рамките на същия период. При учението следва да се вземат предвид други съществуващи оценки на рисковете за киберсигурността и сценарии, разработени на равнището на Съюза.

2. ENISA подкрепя ЕМОПС за електроенергия и ООРСЕС при подготовката и организирането на ученията в областта на киберсигурността на регионално или на междурегионално равнище.

3. ЕМОПС за електроенергия, в сътрудничество с ООРСЕС, информира субектите с критично въздействие, че ще участват в учение в областта на киберсигурността на регионално или на междурегионално равнище, шест месеца преди провеждане на учението.

4. Организаторът на редовно учение в областта на киберсигурността на равнището на Съюза съгласно член 7, параграф 5 от Регламент (ЕС) 2019/881 или на всяко задължително учение в областта на киберсигурността, свързано с електроенергетиката в рамките на същия географски периметър, може да покани ЕМОПС за електроенергия и ООРСЕС да участват. В такива случаи задължението по параграф 1 не се прилага, при условие че всички субекти с критично въздействие в региона на експлоатация на системата участват в едно и също учение.

5. В случай че ЕМОПС за електроенергия и ООРСЕС участват в учение в областта на киберсигурността, посочено в параграф 4, те може да отложат посоченото в параграф 1 регионално или междурегионално учение в областта на киберсигурността с една година.

6. До 31 декември 2027 г. и на всеки три години след тази дата ЕМОПС за електроенергия, в сътрудничество с ООРСЕС, предоставя образец на учение за провеждане на регионални и междурегионални учения в областта на киберсигурността. В този образец се вземат предвид резултатите от най-скорошната оценка на рисковете за киберсигурността на регионално равнище и се съдържат ключови критерии за успех. ЕМОПС за електроенергия се консултира с Комисията и може да поиска съвет от ACER, ENISA и Съвместния изследователски център относно организацията и провеждането на регионалните и междурегионалните учения в областта на киберсигурността.

Член 45

Резултат от ученията в областта на киберсигурността на равнище субект, държава членка, на регионално или междурегионално равнище

1. По искане от субект с критично въздействие доставчиците на критични услуги участват в ученията в областта на киберсигурността, посочени в член 43, параграфи 1 и 2 и в член 44, параграф 1, когато предоставят услуги за субекта с критично въздействие в областта, съответстваща на обхвата на съответното учение в областта на киберсигурността.

2. Организаторите на ученията в областта на киберсигурността, посочени в член 43, параграфи 1 и 2 и в член 44, параграф 1, като се консултират с ENISA по тяхно искане и съгласно член 7, параграф 5 от Регламент (ЕС) 2019/881, анализират и приключват съответното учение в областта на киберсигурността чрез доклад, обобщаващ изводите, който е предназначен за всички участници. Докладът включва:

а) сценариите за ученията, докладите от срещите, основните позиции, успехите и направените изводи на всяко равнище от веригата на стойността на електроенергията;

б) сведения дали са изпълнени ключовите критерии за успех;

в) списък с препоръки за субектите, участващи в съответното учение в областта на киберсигурността, за коригиране, адаптиране или промяна на свързаните с киберкризи процеси, процедури, съответни модели на управление и всички съществуващи договорни ангажименти с доставчици на критични услуги.

3. По искане на мрежата на ЕРИКС или групата за сътрудничество за МИС, или на EU-CyCLONe организаторите на ученията в областта на киберсигурността, посочени в член 43, параграфи 1 и 2 и в член 44, параграф 1, споделят резултата от съответните учения в областта на киберсигурността. Организаторите споделят с всеки субект, участващ в ученията, информацията, посочена в параграф 2, букви а) и б) от настоящия член. Организаторите споделят списъка с препоръки, посочен в същия параграф, буква в), изключително със субектите, към които се отнасят препоръките.

4. Организаторите на ученията в областта на киберсигурността, посочени в член 43, параграфи 1 и 2 и в член 44, параграф 1, редовно проследяват субектите, участващи в ученията, относно изпълнението на препоръките съгласно параграф 2, точка в) от настоящия член.

ГЛАВА VII

ЗАЩИТА НА ИНФОРМАЦИЯТА

Член 46

Принципи относно защитата на обменената информация

1. Изброените в член 2, параграф 1 субекти гарантират, че предоставената, получената, обменената или предадената съгласно настоящия регламент информация е достъпна само въз основа на принципа „необходимост да се знае“ и в съответствие със съответните правила на Съюза и национални правила за сигурност на информацията.

2. Изброените в член 2, параграф 1 субекти гарантират, че предоставената, получената, обменената или предадената съгласно настоящия регламент информация се разглежда и проследява през целия жизнен цикъл на тази информация и че може да бъде оповестена в края на жизнения си цикъл само след като бъде анонимизирана.

3. Изброените в член 2, параграф 1 субекти гарантират, че са въведени всички необходими мерки за защита от организационно и техническо естество с цел опазване и защитаване на поверителността, цялостността и наличността на информацията и невъзможността за отричане на предоставената, получената, обменената или предадената съгласно настоящия регламент информация, независимо от използваните средства. Мерките за защита:

а) са пропорционални;

б) са съобразени с рисковете за киберсигурността, свързани с известни минали и нововъзникващи заплахи, на които тази информация може да бъде обект в контекста на настоящия регламент;

в) доколкото е възможно, се основават на национални, европейски или международни стандарти и най-добри практики;

г) са документирани.

4. Изброените в член 2, параграф 1 субекти гарантират, че всяко лице, на което е предоставен достъп до предоставената, получената, обменената или предадената съгласно настоящия регламент информация, е информирано за правилата за сигурност, приложими на равнище субект, и за мерките и процедурите, свързани със защитата на информацията. Тези субекти гарантират, че съответното лице признава отговорността за защитата на информацията съгласно указанията по време на инструктажа.

5. Изброените в член 2, параграф 1 субекти гарантират, че достъпът до предоставената, получената, обменената или предадената съгласно настоящия регламент информация е ограничен до лица:

а) които имат право на достъп до тази информация въз основа на своите функции и в границите на изпълнение на възложените им задачи;

б) по отношение на които субектът е успял да оцени спазването на етичните принципи и принципите на почтеност, както и за които няма доказателства за отрицателен резултат от цялостната проверка за оценка на надеждността на лицето в съответствие с най-добрите практики и стандартните изисквания за сигурност на субекта, и, когато е необходимо, с националните законови и подзаконови разпоредби.

6. Изброените в член 2, параграф 1 субекти получават писменото съгласие на физическото или юридическото лице, което първоначално е създало или предоставило информацията, преди да предоставят тази информация на трета страна, която попада извън обхвата на настоящия регламент.

7. Посоченият в член 2, параграф 1 субект може да прецени, че тази информация ще бъде обменена, без да се спазват параграфи 1 и 4 от настоящия член, с цел да се предотврати едновременна криза в електроснабдяването, чиято първопричина е киберсигурността, или всяка трансгранична криза в рамките на Съюза в друг сектор. В този случай той:

а) се консултира с компетентния орган и получава от него правомощия да обменя такава информация;

б) анонимизира такава информация, без да се губят елементите, необходими за информиране на обществеността за непосредствен и сериозен риск за трансграничните потоци на електроенергия и възможните мерки за намаляване на рисковете;

в) защитава самоличността на първоизточника на информация и на субектите, които са обработвали такава информация съгласно настоящия регламент.

8. Чрез дерогация от параграф 6 от настоящия член компетентните органи може да предоставят предоставената, получената, обменената или предадената съгласно настоящия регламент информация на трета страна, която не е изброена в член 2, параграф 1, без предварителното писмено съгласие на първоизточника на информацията, но като информират последния при първа възможност. Преди да оповести каквато и да е предоставена, получена, обменена или предадена съгласно настоящия регламент информация на трета страна, която не е посочена в член 2, параграф 1, съответният компетентен орган гарантира в приемлива степен, че въпросната трета страна е запозната с действащите правила за сигурност и получава достатъчна гаранция, че въпросната трета страна може да защити получената информация в съответствие с параграфи 1—5 от настоящия член. Компетентният орган анонимизира такава информация, без да се губят елементите, необходими за информиране на обществеността за непосредствен и сериозен риск за трансграничните потоци на електроенергия и възможните мерки за намаляване на рисковете и защитава самоличността на първоизточника на информацията. В този случай третата страна, която не е посочена в член 2, параграф 1, защитава получената информация в съответствие с разпоредбите, които вече са в сила на равнище субект, или когато това не е възможно, с разпоредбите и указанията, предоставени от съответния компетентен орган.

9. Настоящият член не се прилага за субекти, които не са изброени в член 2, параграф 1, на които е предоставена информация съгласно параграф 6 от настоящия член. В този случай се прилага параграф 7 от настоящия член или компетентният орган може да предостави на субекта писмени разпоредби, които да се прилагат в случаите, когато информацията е получена съгласно настоящия регламент.

Член 47

Поверителност на информацията

1. Всяка предоставена, получена, обменена или предадена съгласно настоящия регламент информация е предмет на условията за опазване на професионалната тайна, посочени в параграфи 2—5 от настоящия член от настоящия регламент, и на изискванията, определени в член 65 от Регламент (ЕС) 2019/943. Всяка информация, предоставена, получена, обменена или предадена между изброените в член 2 от настоящия регламент субекти за целите на прилагането на настоящия регламент, се защитава, като се взема предвид прилаганата от първоизточника на информация степен на поверителност на информацията.

2. Задължението за професионална тайна се прилага по отношение на субектите, изброени в член 2.

3. КООКС, НРО, КО — ГСР и ЕРИКС обменят цялата необходима информация за изпълнение на своите задачи.

4. Всяка информация, получена, обменена или предадена между изброените в член 2, параграф 1 субекти за целите на прилагането на член 23, се анонимизира и обобщава.

5. Информация, която всеки субект или орган, предмет на настоящия регламент, е получил в хода на изпълнение на своите задължения, не може да се разкрива на друг субект или орган, като това правило не засяга случаите, уредени от националното право, другите разпоредби на настоящия регламент или друго съответно законодателство на Съюза.

6. Без да се засяга националното законодателство или законодателството на Съюза, орган, субект или физическо лице, което получава информация съгласно настоящия регламент, не може да я използва за цел, различна от изпълнението на своите задължения съгласно настоящия регламент.

7. ACER, след консултация с ENISA, всички компетентни органи, ЕМОПС за електроенергия и ООРСЕС, до 13 юни 2025 г. издава насоки относно механизмите за обмен на информация за всички изброени в член 2, параграф 1 субекти, и по-специално предвидените комуникационни потоци и методи за анонимизиране и обобщаване на информация за целите на прилагането на настоящия член.

8. Информация, която е поверителна съгласно правилата на Съюза и националните правила, се обменя с Комисията и другите съответни органи само когато такъв обмен е необходим за прилагането на настоящия регламент. Обменяната информация е ограничена до информацията, която е необходима и пропорционална за целите на този обмен. Обменът на информация се извършва при зачитане на нейната поверителност и на сигурността и търговските интереси на субектите с критично въздействие или с голямо въздействие.

ГЛАВА VIII

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 48

Временни разпоредби

1. До одобрението на общите условия или методиките, посочени в член 6, параграф 2, или плановете, посочени в член 6, параграф 3, ЕМОПС за електроенергия, в сътрудничество с ООРСЕС, разработва необвързващи насоки по следните въпроси:

а) временен показател за въздействието върху киберсигурността в електроенергетиката („ECII“) в съответствие с параграф 2 от настоящия член;

б) временен списък на процесите с голямо въздействие и с критично въздействие в целия Съюз в съответствие с параграф 4 от настоящия член; и

в) временен списък на европейските и международните стандарти и мерки за контрол, изисквани съгласно националното законодателство, които са от значение за свързаните с киберсигурността аспекти на трансграничните потоци на електроенергия в съответствие с параграф 6 от настоящия член.

2. До 13 октомври 2024 г. ЕМОПС за електроенергия, в сътрудничество с ООРСЕС, разработва препоръка за временен ECII. ЕМОПС за електроенергия, в сътрудничество с ООРСЕС, уведомява компетентните органи за препоръчания временен ECII.

3. Четири месеца след получаване на препоръчания временен ECII или най-късно до 13 февруари 2025 г. компетентните органи определят кандидати за субекти с голямо въздействие и с критично въздействие в своята държава членка въз основа на препоръчания ECII и разработват временен списък на субекти с голямо въздействие и с критично въздействие. Определените във временния списък субекти с голямо въздействие и с критично въздействие може доброволно да изпълняват определените им с настоящия регламент задължения въз основа на принципа на предохранителните мерки. До 13 март 2025 г. компетентните органи уведомяват субектите, посочени във временния списък, че са определени като субекти с голямо въздействие или с критично въздействие.

4. До 13 декември 2024 г. ЕМОПС за електроенергия, в сътрудничество с ООРСЕС, разработва временен списък на процеси с голямо въздействие и с критично въздействие в целия Съюз. Уведомените съгласно параграф 3 субекти, които доброволно решат да изпълнят определените им с настоящия регламент задължения въз основа на принципа на предохранителните мерки, използват временния списък на процеси с голямо въздействие и с критично въздействие, за да определят временните периметри на голямо въздействие и на критично въздействие и да определят активите, които да бъдат включени в първата оценка на рисковете за киберсигурността на равнище субект.

5. До 13 септември 2024 г. всеки компетентен орган съгласно член 4, параграф 1 предоставя на ЕМОПС за електроенергия и на ООРСЕС списък на своето национално законодателство, което е от значение за свързаните с киберсигурността аспекти на трансграничните потоци на електроенергия.

6. До 13 юни 2025 г. ЕМОПС за електроенергия, в сътрудничество с ООРСЕС, изготвя временен списък на европейски и международни стандарти и мерки за контрол, изисквани от националното законодателство, които са приложими за свързаните с киберсигурността аспекти на трансграничните потоци на електроенергия, като взема предвид предоставената от компетентните органи информация.

7. Временният списък на европейските и международните стандарти и мерки за контрол включва:

а) европейски и международни стандарти и национално законодателство, които предоставят насоки относно методиките за управление на рисковете за киберсигурността на равнище субект; и

б) еквивалент на мерките за контрол във връзка с киберсигурността, които се очаква да бъдат част от минималните и разширените мерки за контрол във връзка с киберсигурността.

8. При окончателното оформяне на временния списък на стандартите ЕМОПС за електроенергия и ООРСЕС вземат предвид предоставените от ENISA и ACER мнения. ЕМОПС за електроенергия и ООРСЕС публикуват временния списък на европейски и международни стандарти и мерки за контрол на своите уебсайтове.

9. ЕМОПС за електроенергия и ООРСЕС провеждат консултация с ENISA и ACER относно предложенията за необвързващи насоки, разработени съгласно параграф 1.

10. До разработването на минималните и разширените мерки за контрол във връзка с киберсигурността в съответствие с член 29 и приемането им в съответствие с член 8 всички изброени в член 2, параграф 1 субекти се стремят към постепенно прилагане на необвързващите насоки, разработени съгласно параграф 1.

Член 49

Влизане в сила

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

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

Съставено в Брюксел на 11 март 2024 година.

За Комисията
Председател
Ursula VON DER LEYEN