Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2024/1366

24.5.2024.

# KOMISIJAS DELEĢĒTĀ REGULA (ES) 2024/1366

**(2024. gada 11. marts),**

**ar ko papildina Eiropas Parlamenta un Padomes Regulu (ES) 2019/943, izveidojot tīkla kodeksu par nozarspecifiskiem noteikumiem attiecībā uz pārrobežu elektroenerģijas plūsmu kiberdrošības aspektiem**

**(Dokuments attiecas uz EEZ)**

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2019/943 (2019. gada 5. jūnijs) par elektroenerģijas iekšējo tirgu ([1]) un jo īpaši tās 59. panta 2. punkta e) apakšpunktu,

tā kā:

(1) Kiberdrošības risku pārvaldība ir būtiska, lai uzturētu elektroapgādes drošību un nodrošinātu augstu kiberdrošības līmeni elektroenerģijas sektorā.

(2) Digitalizācijai un kiberdrošībai ir izšķiroša nozīme pamatpakalpojumu nodrošināšanā, tāpēc tās ir stratēģiski svarīgas kritiskajai energoinfrastruktūrai.

(3) Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 ([2]) paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā. Eiropas Parlamenta un Padomes Regula (ES) 2019/941 ([3]) papildina Direktīvu (ES) 2022/2555, nodrošinot, ka kiberdrošības incidentus elektroenerģijas sektorā atbilstoši identificē kā risku un ka to risināšanai izmantotajiem pasākumiem pievērš pienācīgu uzmanību riskgatavības plānos. Regula (ES) 2019/943 papildina Direktīvu (ES) 2022/2555 un Regulu (ES) 2019/941, nosakot konkrētus noteikumus elektroenerģijas sektoram Savienības līmenī. Turklāt šī deleģētā regula papildina Direktīvas (ES) 2022/2555 noteikumus attiecībā uz elektroenerģijas sektoru visos gadījumos, kas ir saistīti ar pārrobežu elektroenerģijas plūsmām.

(4) Savstarpēji savienotu digitalizētu elektroenerģijas sistēmu gadījumā ar kiberuzbrukumiem saistītas elektroenerģijas krīzes novēršanu un pārvaldību nevar uzskatīt par tikai valsts līmenī pildāmu uzdevumu. Šajā nolūkā būtu pilnībā jāizmanto iespējas īstenot efektīvākus pasākumus ar zemākām izmaksām, sadarbojoties reģionālā un Savienības līmenī. Tāpēc ir nepieciešams vienots noteikumu satvars un labāk saskaņotas procedūras, lai nodrošinātu, ka dalībvalstis un citi aktori spēj sekmīgi sadarboties pāri robežām un ka attiecības starp dalībvalstīm un kompetentajām iestādēm, kas ir atbildīgas par elektroenerģiju un kiberdrošību, raksturo labāka pārredzamība un lielāka uzticēšanās un solidaritāte.

(5) Kiberdrošības risku pārvaldībai šīs regulas darbības jomā ir nepieciešams strukturēts process, kas cita starpā paredz apzināt riskus, ko pārrobežu elektroenerģijas plūsmām rada kiberuzbrukumi, saistītos darbības procesus un perimetrus, atbilstošos kiberdrošības kontroles pasākumus un verifikācijas mehānismus. Lai gan viss process ilgs vairākus gadus, katram tā posmam būtu jāveicina vienādi augsts kiberdrošības līmenis nozarē un jāmazina kiberdrošības riski. Visiem procesa dalībniekiem būtu jādara viss iespējamais, lai pēc iespējas ātrāk izstrādātu metodikas un vienotos par tām bez liekas vilcināšanās – katrā ziņā ne vēlāk kā šajā regulā noteiktajos termiņos.

([1]) OV L 158, 14.6.2019., 54. lpp.

([2]) Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris), ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva) (OV L 333, 27.12.2022., 80. lpp.).

([3]) Eiropas Parlamenta un Padomes Regula (ES) 2019/941 (2019. gada 5. jūnijs) par riskgatavību elektroenerģijas sektorā un ar ko atceļ Direktīvu 2005/89/EK (OV L 158, 14.6.2019., 1. lpp.).

(6) Veicot šajā regulā paredzētos kiberdrošības risku novērtējumus Savienības, dalībvalsts, reģiona un vienības līmenī, var aplūkot tikai tos riskus, kurus rada kiberuzbrukumi saskaņā ar definīciju Eiropas Parlamenta un Padomes Regulā (ES) 2022/2554 ([4]), tādējādi izslēdzot no novērtējuma, piemēram, fiziskus uzbrukumus, dabas katastrofas un pārtrauces iekārtu vai cilvēkresursu zuduma dēļ. Savienības mēroga un reģionālos riskus saistībā ar fiziskiem uzbrukumiem vai dabas katastrofām elektroenerģijas jomā jau aptver citi esoši Savienības tiesību akti, tajā skaitā Regulas (ES) 2019/941 5. pants vai Komisijas Regula (ES) 2017/1485 ([5]), ar ko izveido elektroenerģijas pārvades sistēmas darbības vadlīnijas. Arī Eiropas Parlamenta un Padomes Direktīvas (ES) 2022/2557 ([6]) par kritisko vienību noturību mērķis ir mazināt ievainojamības un stiprināt kritisko vienību fizisko noturību, un tā aptver visus attiecīgos dabas un cilvēka radītos riskus, kuri var ietekmēt pamatpakalpojumu sniegšanu, tajā skaitā nelaimes gadījumus, dabas katastrofas, ārkārtas situācijas sabiedrības veselības jomā, piemēram, pandēmijas, un hibrīddraudus vai citus antagonistiskus draudus, tostarp teroristu nodarījumus, noziedzīgo aprindu iefiltrēšanos un sabotāžu.

(7) Šajā regulā izmantotais jēdziens "lielas ietekmes un kritiskas ietekmes vienības" ir fundamentāls, lai būtu iespējams definēt, uz kurām vienībām attieksies regulā aprakstītie pienākumi. Dažādos noteikumos izklāstītās uz risku balstītās pieejas mērķis ir apzināt tādus procesus, atbalsta aktīvus un tos ekspluatējošās vienības, kuri ietekmē pārrobežu elektroenerģijas plūsmas. Atkarībā no tā, kādā mērā iespējamie kiberuzbrukumi var ietekmēt to darbību saistībā ar pārrobežu elektroenerģijas plūsmām, tos var iedalīt "lielas ietekmes" vai "kritiskas ietekmes" kategorijās. Direktīvas (ES) 2022/2555 3. pantā ir noteikti jēdzieni "būtiska vienība" un "svarīga vienība" un kritēriji, pēc kuriem nosaka vienību piederību minētajām kategorijām. Lai gan daudzas vienības vienlaikus uzskatīs par "būtiskām" Direktīvas (ES) 2022/2555 3. panta izpratnē un identificēs kā lielas ietekmes vai kritiskas ietekmes vienības saskaņā ar šīs regulas 24. pantu, šajā regulā noteiktie kritēriji attiecas vienīgi uz šo vienību nozīmi un ietekmi elektroenerģijas procesos, kuri ietekmē pārrobežu plūsmas, un Direktīvas (ES) 2022/2555 3. pantā noteiktos kritērijus neņem vērā.

(8) Šīs regulas darbības jomā ietilpstošās vienības, kuras saskaņā ar šīs regulas 24. pantu uzskata par lielas ietekmes vai kritiskas ietekmes vienībām un uz kurām attiecas minētajā pantā noteiktie pienākumi, ir galvenokārt tādas vienības, kam ir tieša ietekme uz pārrobežu elektroenerģijas plūsmām ES.

(9) Šī regula izmanto ar citiem tiesību aktiem jau ieviestus mehānismus un instrumentus, lai nodrošinātu efektivitāti un izvairītos no dublēšanās mērķu sasniegšanā.

(10) Piemērojot šo regulu, dalībvalstīm, attiecīgajām iestādēm un sistēmu operatoriem būtu jāņem vērā saskaņotie Eiropas standarti un Eiropas standartizācijas organizāciju tehniskās specifikācijas un jārīkojas saskaņā ar Savienības tiesību aktiem, kuri ir saistīti ar to aptverto produktu laišanu tirgū vai nodošanu ekspluatācijā.

([4]) Eiropas Parlamenta un Padomes Regula (ES) 2022/2554 (2022. gada 14. decembris) par finanšu nozares digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 (OV L 333, 27.12.2022., 1. lpp.).

([5]) Komisijas Regula (ES) 2017/1485 (2017. gada 2. augusts), ar ko izveido elektroenerģijas pārvades sistēmas darbības vadlīnijas (OV L 220, 25.8.2017., 1. lpp.).

([6]) Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2557 (2022. gada 14. decembris) par kritisko vienību noturību un Padomes Direktīvas 2008/114/EK atcelšanu (OV L 333, 27.12.2022., 164. lpp.).

(11) Lai mazinātu kiberdrošības riskus, ir jāizstrādā detalizēti noteikumi, kas regulētu to attiecīgo ieinteresēto personu darbības,, kuru nodarbošanās ir saistīta ar pārrobežu elektroenerģijas plūsmu kiberdrošības aspektiem, un sadarbību šādu personu starpā nolūkā nodrošināt sistēmas drošību. Tādiem organizatoriskajiem un tehniskajiem noteikumiem būtu jānodrošina, ka lielāko daļu elektroenerģētisko incidentu, kuru pamatcēlonis ir kiberdrošība, efektīvi risina operatīvajā līmenī. Ir jānosaka, ko attiecīgajām ieinteresētajām personām vajadzētu darīt, lai novērstu šādas krīzes, un kādi pasākumi tām būtu jāveic, ja vairs nepietiek tikai ar sistēmas darbības noteikumiem. Tāpēc ir jāizveido vienots satvars noteikumiem par to, kā novērst vienlaicīgas elektroenerģētiskās krīzes, kuru pamatcēlonis ir kiberdrošība, sagatavoties šādām krīzēm un pārvarēt tās. Tas palielinās pārredzamību gatavošanās posmā un vienlaicīgas elektroenerģētiskās krīzes laikā un nodrošinās, ka pasākumus veic saskaņotā un efektīvā veidā kopīgi ar dalībvalstu kompetentajām iestādēm, kuras ir atbildīgas par kiberdrošību. Dalībvalstīm un attiecīgajām vienībām būtu jānosaka pienākums sadarboties reģionālā līmenī un attiecīgos gadījumos divpusēji, ievērojot solidaritātes principu. Šādas sadarbības un noteikumu mērķis ir sasniegt labāku krīžgatavību kiberdrošības jomā ar mazākām izmaksām, kas saskan arī ar Direktīvas (ES) 2022/2555 mērķiem. Būtu nepieciešams arī stiprināt iekšējo elektroenerģijas tirgu, uzlabojot dalībvalstu savstarpējo uzticēšanos un paļāvību, jo īpaši mazinot pārrobežu elektroenerģijas plūsmu nepamatotas samazināšanas risku un tādējādi novēršot plašāku negatīvu ietekmi uz kaimiņos esošām dalībvalstīm.

(12) Elektroapgādes drošībai ir vajadzīga efektīva sadarbība starp dalībvalstīm, Savienības iestādēm, struktūrām, birojiem un aģentūrām, kā arī attiecīgajām ieinteresētajām personām. Saskaņā ar Eiropas Parlamenta un Padomes Direktīvas (ES) 2019/944 ([7]) 31. un 40. pantu drošas, uzticamas un efektīvas elektroenerģijas sistēmas nodrošināšanā būtiska nozīme ir sadales sistēmu un pārvades sistēmu operatoriem. Dažādām regulatīvajām iestādēm un citām attiecīgajām valsts kompetentajām iestādēm arī ir liela nozīme energoapgādes kiberdrošības nodrošināšanā un uzraudzībā, jo tas ietilpst uzdevumos, kuri tām ir uzticēti ar Direktīvu (ES) 2019/944 un Direktīvu (ES) 2022/2555. Izraugot kādu jau esošu struktūru vai izveidojot jaunu, dalībvalstīm būtu jāieceļ valsts kompetentā iestāde šīs regulas īstenošanai nolūkā nodrošināt visu iesaistīto aktoru pārredzamu un iekļaujošu līdzdalību, efektīvus sagatavošanās pasākumus un pienācīgu regulas īstenošanu, sadarbību starp dažādām attiecīgajām ieinteresētajām personām un kompetentajām iestādēm elektroenerģijas un kiberdrošības jomā, kā arī veicināt tādu elektroenerģētisko krīžu novēršanu un *ex post* izvērtēšanu, kuru pamatcēlonis ir kiberdrošība, kā arī informācijas apmaiņu saistībā ar minēto.

(13) Ja lielas ietekmes vai kritiskas ietekmes vienība sniedz pakalpojumus vairākās dalībvalstīs vai ja tai ir mītne vai cits iedibinājums, vai pārstāvis vienā dalībvalstī, bet tās tīklu un informācijas sistēmas atrodas vienā vai vairākās citās dalībvalstīs, šādām dalībvalstīm būtu jāmudina attiecīgās kompetentās iestādes pielikt visas pūles, lai tās sadarbotos un vajadzības gadījumā palīdzētu cita citai.

(14) Dalībvalstīm būtu jānodrošina, ka attiecībā uz lielas ietekmes un kritiskas ietekmes vienībām kompetentajām iestādēm ir nepieciešamās pilnvaras, lai veicinātu šīs regulas ievērošanu. Tādām pilnvarām būtu jāļauj kompetentajām iestādēm veikt inspekcijas uz vietas un attālinātu uzraudzību. Tas var ietvert izlases veida pārbaudes, regulāras revīzijas, mērķorientētas drošības revīzijas, kuru pamatā ir riska novērtējums vai ar risku saistīta pieejamā informācija, un drošības skenēšanu, pamatojoties uz objektīviem, nediskriminējošiem, taisnīgiem un pārredzamiem riska novērtēšanas kritērijiem, un tajā skaitā tādas informācijas pieprasīšanu, kas ir nepieciešama, lai novērtētu vienības pieņemtos kiberdrošības pasākumus. Tostarp par šādu informāciju būtu jāuzskata dokumentētas kiberdrošības rīcībpolitikas, dati, dokumenti un informācija, kas ir nepieciešama uzraudzības uzdevumu izpildei, pierādījumi par kiberdrošības rīcībpolitikas īstenošanu, piemēram, kvalificēta revidenta veiktu drošības revīziju rezultāti un attiecīgie pamatā esošie pierādījumi.

([7]) Eiropas Parlamenta un Padomes Direktīva (ES) 2019/944 (2019. gada 5. jūnijs) par kopīgiem noteikumiem attiecībā uz elektroenerģijas iekšējo tirgu un ar ko groza Direktīvu 2012/27/ES (OV L 158, 14.6.2019., 125. lpp.).

(15) Lai izvairītos no lielas ietekmes un kritiskas ietekmes vienībām noteikto kiberdrošības risku pārvaldības pienākumu nepilnībām vai dublēšanās, Direktīvā (ES) 2022/2555 paredzētajām valsts iestādēm un šajā regulā paredzētajām kompetentajām iestādēm būtu jāsadarbojas saistībā ar kiberdrošības risku pārvaldības pasākumu īstenošanu un minēto pasākumu izpildes uzraudzību valsts līmenī. Direktīvā (ES) 2022/2555 paredzētās valsts iestādes varētu uzskatīt, ka vienības atbilstība šajā regulā noteiktajām kiberdrošības risku pārvaldības prasībām garantē atbilstību attiecīgajām minētajā direktīvā noteiktajām prasībām, un otrādi.

(16) Lai būtu iespējama vienota pieeja vienlaicīgu elektroenerģētisko krīžu novēršanai un pārvaldībai, dalībvalstīm ir jābūt kopīgai izpratnei par to, kas jāuzskata par vienlaicīgu elektroenerģētisko krīzi un kad kiberuzbrukums ir nozīmīgs faktors šādā krīzē. Būtu jāveicina koordinācija starp dalībvalstīm un attiecīgajām vienībām, jo īpaši nolūkā risināt situāciju, kurā ir esošs vai draudošs potenciālais risks, ka radīsies nozīmīgs elektroenerģijas iztrūkums vai nespēja piegādāt patērētājiem elektroenerģiju, un to ir izraisījis kiberuzbrukums.

(17) Eiropas Parlamenta un Padomes Regulas (ES) 2019/881 ([8]) 1. apsvērums atzīst tīklu un informācijas sistēmu un elektronisko sakaru tīklu un pakalpojumu būtisko nozīmi saimnieciskās darbības uzturēšanā tādās nozīmīgās nozarēs kā enerģētika, savukārt 44. apsvērums paskaidro, ka ES Kiberdrošības aģentūrai (*"ENISA"*) būtu jāsadarbojas ar Eiropas Savienības Energoregulatoru sadarbības aģentūru (*"ACER"*).

(18) Regula (ES) 2019/943 nosaka pārvades sistēmu operatoriem ("PSO") un sadales sistēmu operatoriem ("SSO") konkrētus pienākumus attiecībā uz kiberdrošību. To Eiropas apvienībām, proti, elektroenerģijas pārvades sistēmu operatoru Eiropas tīklam (*"ENTSO-E"*) un Eiropas sadales sistēmu operatoru struktūrai ("ES SSO struktūra"), saskaņā ar minētās regulas attiecīgi 30. un 55. pantu ir jāveicina kiberdrošība sadarbībā ar attiecīgajām iestādēm un regulētajiem subjektiem.

(19) Lai īstenotu vienotu pieeju tādu vienlaicīgu elektroenerģētisko krīžu novēršanai un pārvaldībai, kuru pamatcēlonis ir kiberdrošība, ir jānodrošina arī tas, ka visas attiecīgās ieinteresētās personas izmanto saskaņotas metodes un definīcijas, lai apzinātu riskus, kas ir saistīti ar elektroapgādes kiberdrošību. Ir jābūt arī iespējai faktiski salīdzināt savu un kaimiņu sniegumu attiecīgajā jomā. Tāpēc ir jānosaka procesi, uzdevumi un pienākumi izstrādāt un atjaunināt risku pārvaldības metodikas, incidentu klasifikācijas skalas un kiberdrošības pasākumus, kas ir pielāgoti kiberdrošības riskiem, kuri apdraud pārrobežu elektroenerģijas plūsmas.

(20) Identificēt vienības, kuras atbilst lielas ietekmes un kritiskas ietekmes vienību kritērijiem, ir dalībvalstu pienākums, kura izpildi nodrošina kompetentā iestāde, ko katra dalībvalsts ir izraudzījusies šīs regulas īstenošanai. Lai šajā ziņā mazinātu lielās atšķirības starp dalībvalstīm un nodrošinātu juridisko noteiktību attiecībā uz kiberdrošības risku pārvaldības pasākumiem un ziņošanas pienākumiem visām attiecīgajām vienībām, būtu jāievieš vienots kritēriju kopums tādu vienību noteikšanai, kuras ietilpst šīs direktīvas darbības jomā. Šāds kritēriju kopums būtu jānosaka un regulāri jāatjaunina šajā regulā paredzēto noteikumu un metodiku izstrādes un pieņemšanas procesā.

(21) Šīs regulas noteikumiem nebūtu jāskar Savienības tiesību akti, kuri paredz īpašus noteikumus par informācijas un komunikācijas tehnoloģiju ("IKT") produktu, IKT pakalpojumu un IKT procesu sertifikāciju; jo īpaši tiem nebūtu jāskar Regula (ES) 2019/881 attiecībā uz Eiropas kiberdrošības sertifikācijas shēmu izveides satvaru. Šajā regulā jēdzienam "IKT produkti" būtu jāietver arī tehniskās ierīces un programmatūra, kas ļauj tieši mijiedarboties ar elektrotehnisko tīklu, jo īpaši rūpnieciskajām kontroles sistēmām, ko var izmantot enerģijas pārvadei, enerģijas sadalei un enerģijas ražošanai, kā arī saistītās informācijas vākšanai un pārsūtīšanai. Noteikumiem būtu jānodrošina, ka iepērkamie IKT produkti, IKT pakalpojumi un IKT procesi atbilst Regulas (ES) 2019/881 51. pantā norādītajiem attiecīgajiem drošības mērķiem.

([8]) Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (OV L 151, 7.6.2019., 15. lpp.).

(22) Jaunākie kiberuzbrukumi liecina, ka aizvien biežāk uzbrukumus piegādes ķēdei vērš pret vienībām. Šādi uzbrukumi piegādes ķēdēm ietekmē ne tikai atsevišķās vienības, pret kurām ir vērsts uzbrukums – tiem var būt arī lavīneida ietekme, kas paplašina uzbrukuma mērogu, skarot arī vienības, kas elektrotīklā ir savienotas ar to vienību, kurai uzbruka sākotnēji. Tāpēc ir pievienoti noteikumi un ieteikumi, kas palīdzēs mazināt kiberdrošības riskus attiecībā uz procesiem, kas ir saistīti ar piegādes ķēdi, jo īpaši iepirkumu, un ietekmē pārrobežu elektroenerģijas plūsmas.

(23) Tā kā tīklu un informācijas sistēmu ievainojamību izmantošana var izraisīt būtiskus energoapgādes traucējumus un kaitējumu ekonomikai un patērētājiem, šādas ievainojamības būtu ātri jāatklāj un jānovērš, lai mazinātu riskus. Lai atvieglotu šīs regulas rezultatīvu īstenošanu, attiecīgajām vienībām un kompetentajām iestādēm būtu jāsadarbojas, lai organizētu mācības un testētu darbības, ko uzskata par atbilstošām šim nolūkam, tajā skaitā apmaiņu ar informāciju par kiberdraudiem, kiberuzbrukumiem, ievainojamībām, rīkiem un metodēm, taktiku, paņēmieniem un procedūrām, gatavību kiberdrošības krīžu pārvaldībai un citām mācībām. Tā kā tehnoloģijas pastāvīgi attīstās un elektroenerģijas sektorā notiek strauja digitalizācija, pieņemto noteikumu īstenošanai nevajadzētu kaitēt inovācijai un kļūt par šķērsli, kas kavē ienākt elektroenerģijas tirgū un izmantot inovatīvus risinājumus, kuri veicinātu elektroenerģijas sistēmas efektivitāti un ilgtspēju.

(24) Informācijai, ko vāc nolūkā uzraudzīt šīs regulas īstenošanu, vajadzētu būt saprātīgā mērā ierobežotai, balstoties uz principu "nepieciešamība zināt". Termiņiem, kādus nosaka ieinteresētajām personām šādas informācijas iesniegšanai, vajadzētu būt praktiski izpildāmiem un lietderīgiem. Būtu jāizvairās no dubultās ziņošanas.

(25) Kiberdrošības aizsardzība nebeidzas pie Savienības robežām. Lai sistēma būtu droša, ir nepieciešama kaimiņos esošo trešo valstu iesaiste. Savienībai un tās dalībvalstīm būtu jācenšas atbalstīt kaimiņos esošās trešās valstis, kuru elektroenerģijas infrastruktūra ir savienota ar Eiropas tīklu, tādu kiberdrošības noteikumu piemērošanā, kuri līdzinās šajā regulā paredzētajiem.

(26) Lai jau no paša sākuma uzlabotu drošības koordinēšanu un pārbaudītu noteikumus un metodikas, kas nākotnē būs saistošas, *ENTSO-E*, ES SSO struktūrai un kompetentajām iestādēm būtu jāsāk izstrādāt nesaistošas norādes, tiklīdz šī regula būs stājusies spēkā. Šīs norādes kalpos par bāzlīniju turpmāko noteikumu, nosacījumu un metodiku izstrādei. Vienlaikus kompetentajām iestādēm būtu jāidentificē vienības – kandidātes uz lielas ietekmes un kritiskas ietekmes vienības statusu, lai tās sāktu pildīt pienākumus brīvprātīgā kārtā.

(27) Šī regula ir izstrādāta ciešā sadarbībā ar *ACER*, *ENISA*, *ENTSO-E*, ES SSO struktūru un citām ieinteresētajām personām, lai pieņemtu iedarbīgus, līdzsvarotus un samērīgus noteikumus pārredzamā un līdzdalīgā veidā.

(28) Šī regula papildina un uzlabo krīzes pārvarēšanas pasākumus, kas ieviesti saskaņā ar ES satvaru reaģēšanai kiberdrošības krīzēs, kā to paredz Komisijas ieteikums (ES) 2017/1584 ([9]). Kiberuzbrukums var arī izraisīt elektroenerģētisko krīzi, kas definēta Regulas (ES) 2019/941 2. panta 9. punktā, veicināt šādu krīzi vai noritēt vienlaikus ar to, ietekmējot pārrobežu plūsmas. Tāda elektroenerģētiskā krīze var izraisīt vienlaicīgu elektroenerģētisko krīzi, kas definēta Regulas (ES) 2019/941 2. panta 10. punktā. Šāds incidents var ietekmēt arī citas nozares, kas ir atkarīgas no energoapgādes drošības. Ja šāds incidents pāraug plašapmēra kiberdrošības incidentā Direktīvas (ES) 2022/2555 16. panta nozīmē, būtu jāpiemēro noteikumi minētajā pantā par Eiropas Kiberkrīžu sadarbības organizāciju tīkla ("*EU-CyCLONe*") izveidi. Attiecībā uz krīžu pārvaldību Savienības līmenī attiecīgajām pusēm būtu jāpaļaujas uz ES integrētajiem krīzes situāciju politiskās reaģēšanas mehānismiem ("*IPCR* mehānismi"), ko paredz Padomes Īstenošanas lēmums (ES) 2018/1993 ([10]).

(29) Šī regula neskar dalībvalstu kompetenci veikt nepieciešamos pasākumus, lai nodrošinātu savu būtisko drošības interešu aizsardzību, sabiedrisko kārtību un sabiedrisko drošību un lai ļautu izmeklēt un atklāt noziedzīgus nodarījumus un sodīt par tiem atbilstoši Savienības tiesību aktiem. Saskaņā ar LESD 346. pantu dalībvalstīm nav jāsniedz informācija, kuras izpaušanu tās atzīst par būtisku savas drošības interešu apdraudējumu.

([9]) Komisijas Ieteikums (ES) 2017/1584 (2017. gada 13. septembris) par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm (OV L 239, 19.9.2017., 36. lpp.).

([10]) Padomes Īstenošanas lēmums (ES) 2018/1993 (2018. gada 11. decembris) par ES integrētajiem krīzes situāciju politiskās reaģēšanas mehānismiem (OV L 320, 17.12.2018., 28. lpp.).

(30) Lai gan šī regula principā attiecas arī uz vienībām, kas veic darbības elektroenerģijas ražošanā kodolelektrostacijās, dažas no minētajām darbībām var būt saistītas ar valsts drošību.

(31) Jebkādai persondatu apstrādei saskaņā ar šo regulu piemēro Savienības datu aizsardzības tiesību aktus un Savienības privātuma tiesību aktus. Jo īpaši šī regula neskar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 ([11]), Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK ([12]) un Eiropas Parlamenta un Padomes Regulu (ES) 2018/1725 ([13]). Tāpēc šai direktīvai cita starpā nebūtu jāskar tādu iestāžu uzdevumi un pilnvaras, kuras ir kompetentas uzraudzīt atbilstību piemērojamajiem Savienības datu aizsardzības tiesību aktiem un Savienības privātuma tiesību aktiem.

(32) Tā kā starptautiskā sadarbība ir svarīga kiberdrošībai, dalībvalstu izraudzītajām kompetentajām iestādēm, kas ir atbildīgas par to uzdevumu pildīšanu, kuri tām ir uzticēti saskaņā ar šo regulu, būtu jāspēj piedalīties starptautiskās sadarbības tīklos. Tāpēc savu uzdevumu pildīšanas nolūkā kompetentajām iestādēm būtu jāspēj apmainīties ar informāciju, tajā skaitā persondatiem, ar trešo valstu kompetentajām iestādēm, ja ir izpildīti Savienības personas datu aizsardzības tiesību aktos noteiktie nosacījumi persondatu nosūtīšanai uz trešām valstīm, cita starpā nosacījumi, kas ir norādīti Regulas (ES) 2016/679 49. pantā.

(33) Persondatu apstrādi, ciktāl tā ir nepieciešama un samērīga, lai lielas ietekmes un kritiskas ietekmes vienības varētu nodrošināt savu aktīvu drošību, varētu uzskatīt par likumīgu, pamatojoties uz to, ka šāda apstrāde atbilst pārzinim uzliktajam juridiskajam pienākumam saskaņā ar Regulas (ES) 2016/679 6. panta 1. punkta c) apakšpunkta un 6. panta 3. punkta prasībām. Lielas ietekmes un kritiskas ietekmes vienībām, kā arī drošības tehnoloģiju un pakalpojumu sniedzējiem, kuri rīkojas minēto vienību vārdā, var būt nepieciešams apstrādāt persondatus arī leģitīmo interešu ievērošanai saskaņā ar Regulas (ES) 2016/679 6. panta 1. punkta f) apakšpunktu, arī tad, ja šāda apstrāde ir nepieciešama kiberdrošības informācijas kopīgošanas mehānismiem vai brīvprātīgai attiecīgās informācijas paziņošanai saskaņā ar šo regulu. Lai īstenotu pasākumus, kas ir saistīti ar kiberuzbrukumu novēršanu, atklāšanu, apzināšanu, ierobežošanu, analīzi un reaģēšanu uz tiem, pasākumus, kas veicina informētību par konkrētiem kiberdraudiem, informācijas apmaiņu saistībā ar ievainojamības izlabošanu un koordinētu ievainojamības izpaušanu, brīvprātīgu informācijas apmaiņu par minētajiem kiberuzbrukumiem, kā arī kiberdraudiem un ievainojamībām, aizskāruma rādītājiem, taktiku, paņēmieniem un procedūrām, kiberdrošības brīdinājumiem un konfigurācijas rīkiem, var būt jāapstrādā konkrētu kategoriju persondati, piemēram, IP adreses, vienoto resursu vietrāži (URL), domēnu nosaukumi, e-pasta adreses, un – ja tie atklāj persondatus – laika zīmogi. Persondatu apstrāde, ko veic kompetentās iestādes, vienotie kontaktpunkti un *CSIRT*, var būt juridisks pienākums vai var tikt uzskatīta par nepieciešamu, lai veiktu uzdevumu sabiedrības interesēs vai īstenotu oficiālās pilnvaras, kas pārzinim piešķirtas saskaņā ar Regulas (ES) 2016/679 6. panta 1. punkta c) vai e) apakšpunktu un 6. panta 3. punktu, vai lai ievērotu lielas ietekmes vai kritiskas ietekmes vienību leģitīmās intereses, kā to paredz minētās regulas 6. panta 1. punkta f) apakšpunkts. Turklāt valsts tiesību aktos varētu paredzēt noteikumus, kas ļauj kompetentajām iestādēm, vienotajiem kontaktpunktiem un *CSIRT*, ciktāl tas ir nepieciešami un samērīgi, lai nodrošinātu lielas ietekmes un kritiskas ietekmes vienību tīklu un informācijas sistēmu drošību, apstrādāt īpašu kategoriju persondatus saskaņā ar Regulas (ES) 2016/679 9. pantu, jo īpaši paredzot piemērotus un konkrētus pasākumus, kā aizsargāt fizisko personu pamattiesības un intereses, tajā skaitā nosakot tehniskus ierobežojumus šādu datu atkalizmantošanai un izmantojot mūsdienīgus drošības un privātuma aizsardzības pasākumus, piemēram, pseidonimizāciju vai šifrēšanu, ja anonimizācija var būtiski apgrūtināt attiecīgā mērķa sasniegšanu.

([11]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

([12]) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp.).

([13]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp.).

(34) Daudzos gadījumos apdraudējums persondatiem rodas kiberuzbrukuma rezultātā. Šajā sakarā kompetentajām iestādēm būtu jāsadarbojas un jāapmainās ar informāciju par visiem attiecīgajiem jautājumiem ar iestādēm, kas ir minētas Regulā (ES) 2016/679 un Direktīvā 2002/58/EK.

(35) Saskaņā ar Regulas (ES) 2018/1725 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2023. gada 17. novembrī sniedza atzinumu,

IR PIEŅĒMUSI ŠO REGULU.

I NODAĻA

**VISPĀRĪGIE NOTEIKUMI**

*1. pants*

**Priekšmets**

Ar šo regulu izveido tīkla kodeksu, kas nosaka nozarspecifiskus noteikumus attiecībā uz pārrobežu elektroenerģijas plūsmu kiberdrošības aspektiem, tajā skaitā noteikumus par kopīgām minimālajām prasībām, plānošanu, uzraudzību, ziņošanu un krīzes pārvaldību.

*2. pants*

**Darbības joma**

1. Šī regula attiecas uz pārrobežu elektroenerģijas plūsmu kiberdrošības aspektiem tālāk norādīto vienību darbībā, ja tās ir identificētas kā lielas ietekmes vai kritiskas ietekmes vienības saskaņā ar šīs regulas 24. pantu:

a) elektroenerģijas uzņēmumi, kas definēti Direktīvas (ES) 2019/944 2. panta 57. punktā;

b) nominētie elektroenerģijas tirgus operatori ("NETO"), kas definēti Regulas (ES) 2019/943 2. panta 8. punktā;

c) organizētas tirgus vietas vai "organizētie tirgi", kas definēti Komisijas Īstenošanas Regulas (ES) Nr. 1348/2014 ([14]) 2. panta 4. punktā, kas veic darījumus ar produktiem, kuri ir būtiski pārrobežu elektroenerģijas plūsmām;

d) kritisko IKT pakalpojumu sniedzēji, kas minēts šīs regulas 3. panta 9. punktā;

e) *ENTSO-E*, kas izveidota saskaņā ar Regulas (ES) 2019/943 28. pantu;

f) ES SSO struktūra, kas izveidota saskaņā ar Regulas (ES) 2019/943 52. pantu;

g) balansatbildīgās puses, kas definētas Regulas (ES) 2019/943 2. panta 14. punktā;

h) uzlādes punktu operatori, kas definēti Direktīvas (ES) 2022/2555 I pielikumā;

i) reģionālie koordinācijas centri ("RKC"), kas izveidoti saskaņā ar Regulas (ES) 2019/943 35. pantu;

j) pārvaldītu drošības pakalpojumu sniedzēji ("PDPS"), kas definēti Direktīvas (ES) 2022/2555 6. panta 40. punktā;

k) visas citas vienības vai trešās personas, kurām ir deleģēti vai uzdoti pienākumi saskaņā ar šo regulu.

2. Tālāk norādītās iestādes savu esošo pilnvaru ietvaros ir atbildīgas par šajā regulā tām noteikto uzdevumu pildīšanu:

a) Eiropas Savienības Energoregulatoru sadarbības aģentūra ("*ACER*"), kas izveidota saskaņā Eiropas Parlamenta un Padomes Regulu (ES) 2019/942 ([15]);

b) valsts kompetentās iestādes, kuras ir atbildīgas par to uzdevumu izpildi, kuri tām ir uzdoti saskaņā ar šo regulu, un kuras dalībvalstis izraudzījušās saskaņā ar šīs regulas 4. pantu ("kompetentā iestāde");

c) valsts regulatīvās iestādes ("VRI"), ko katra dalībvalsts izraudzījusies saskaņā ar Direktīvas (ES) 2019/944 57. panta 1. punktu;

([14]) Komisijas Īstenošanas regula (ES) Nr. 1348/2014 (2014. gada 17. decembris) par datu ziņošanu, īstenojot 8. panta 2. punktu un 8. panta 6. punktu Eiropas Parlamenta un Padomes Regulā (ES) Nr. 1227/2011 par enerģijas vairumtirgus integritāti un pārredzamību (OV L 363, 18.12.2014., 121. lpp.).

([15]) Eiropas Parlamenta un Padomes Regula (ES) 2019/942 (2019. gada 5. jūnijs), ar ko izveido Eiropas Savienības Energoregulatoru sadarbības aģentūru (OV L 158, 14.6.2019., 22. lpp.).

d) riskgatavības kompetentās iestādes (“RKI”), kas izveidotas saskaņā ar Regulas (ES) 2019/941 3. pantu;

e) datordrošības incidentu reaģēšanas vienības (“*CSIRT*”), kas izraudzītas vai izveidotas saskaņā ar Direktīvas (ES) 2022/2555 10. pantu;

f) kiberdrošības kompetentās iestādes (“KKI”), kas izraudzītas vai izveidotas saskaņā ar Direktīvas (ES) 2022/2555 8. pantu;

g) Eiropas Savienības Kiberdrošības aģentūra, kas izveidotas saskaņā ar Regulu (ES) 2019/881;

h) visas citas iestādes vai trešās personas, kurām ir deleģēti vai uzdoti pienākumi saskaņā ar šīs regulas 4. panta 3. punktu.

3. Šī regula attiecas arī uz visām vienībām, kuras nav iedibinātas Savienībā, bet sniedz pakalpojumus vienībām Savienībā, ja kompetentās iestādes tās ir identificējušas kā lielas ietekmes vai kritiskas ietekmes vienības saskaņā ar šīs regulas 24. panta 2. punktu.

4. Šī regula neskar dalībvalstu pienākumu sargāt valsts drošību un to pilnvaras aizsargāt citas valsts pamatfunkcijas, tostarp valsts teritoriālās integritātes nodrošināšanu un likumības un kārtības uzturēšanu.

5. Šī regula neskar dalībvalstu pienākumu sargāt valsts drošību attiecībā uz darbībām elektroenerģijas ražošanā kodolelektrostacijās, arī darbībām kodolenerģijas vērtības ķēdē, saskaņā ar Līgumiem.

6. Vienības, kompetentās iestādes, vienotie kontaktpunkti un *CSIRT* apstrādā persondatus, ciktāl tas ir nepieciešams šīs regulas mērķiem un saskaņā ar Regulu (ES) 2016/679, un jo īpaši šāda apstrāde balstās uz minētās regulas 6. pantu.

*3. pants*

**Definīcijas**

Piemēro šādas definīcijas:

1) “aktīvi” ir jebkāda materiāla vai nemateriāla veida informācija, programmatūra vai aparatūra tīklu un informācijas sistēmās, kas ir vērtīga fiziskai personai, organizācijai vai valdībai;

2) “riskgatavības kompetentā iestāde” ir kompetentā iestāde, kas izraudzīta saskaņā ar Regulas (ES) 2019/941 3. pantu;

3) “datordrošības incidentu reaģēšanas vienība” ir vienība, kas ir atbildīga par risku un incidentu risināšanu saskaņā ar Direktīvas (ES) 2022/2555 10. pantu;

4) “kritiskas ietekmes aktīvs” ir aktīvs, kas ir nepieciešams kritiskas ietekmes procesa īstenošanai;

5) “kritiskas ietekmes vienība” ir vienība, kas īsteno kritiskas ietekmes procesu un ko kompetentās iestādes ir identificējušas saskaņā ar šīs regulas 24. pantu;

6) “kritiskas ietekmes perimetrs” ir perimetrs, ko ir definējusi šīs regulas 2. panta 1. punktā minēta vienība un kas ietver visus kritiskas ietekmes aktīvus, un kurā var kontrolēt piekļuvi šādiem aktīviem, un pēc kura definē pastiprināto kiberdrošības kontroles pasākumu piemērošanas tvērumu;

7) “kritiskas ietekmes process” ir vienības īstenots darba process, kura elektroenerģijas kiberdrošības ietekmes rādītāji pārsniedz kritiskās ietekmes sliekšņvērtību;

8) “kritiskās ietekmes sliekšņvērtība” ir šīs regulas 19. panta 3. punkta b) apakšpunktā minētās elektroenerģijas kiberdrošības ietekmes rādītāju vērtības, kuru pārsniegšana nozīmē, ka kiberuzbrukums darbības procesam izraisīs kritiskus traucējumus pārrobežu elektroenerģijas plūsmās;

9) “kritisku IKT pakalpojumu sniedzējs” ir vienība, kas nodrošina IKT pakalpojumu vai IKT procesu, kurš ir nepieciešams kritiskas ietekmes vai lielas ietekmes procesam, kas ietekmē pārrobežu elektroenerģijas plūsmu kiberdrošības aspektus un kura apdraudējums var izraisīt kiberuzbrukumu, kura ietekme pārsniegs kritiskas ietekmes vai lielas ietekmes sliekšņvērtību;

10) “pārrobežu elektroenerģijas plūsma” ir pārrobežu plūsma, kas definēta Regulas (ES) 2019/943 2. panta 3. punktā;

11) “kiberuzbrukums” ir kiberuzbrukums, kas definēts Regulas (ES) 2022/2554 3. panta 14. punktā;

12) “kiberdrošība” ir kiberdrošība, kas definēta Regulas (ES) 2019/881 2. panta 1. punktā;

13) “kiberdrošības kontroles pasākums” ir darbības vai procedūras, ko īsteno nolūkā novērst, atklāt vai mazināt kiberdrošības riskus, vai reaģēt uz tiem;

14) “kiberdrošības incidents” ir incidents, kas definēts Direktīvas (ES) 2022/2555 6. panta 6. punktā;

15) “kiberdrošības pārvaldības sistēma” ir politikas, procedūras, vadlīnijas un ar tām saistītie resursi un darbības, ko kopā pārvalda vienība nolūkā aizsargāt savus informācijas aktīvus pret kiberdraudiem, sistemātiski veidojot, ieviešot, īstenojot, uzraugot, pārskatot, uzturot un uzlabojot organizācijas tīklu un informācijas sistēmas drošību;

16) “kiberdrošības operatīvais centrs” ir īpašs centrs, kurā tehniskā komanda viena vai vairāku speciālistu sastāvā un ar kiberdrošības IT sistēmu atbalstu veic ar drošību saistītus uzdevumus (kiberdrošības operatīvā centra (“KOC”) pakalpojumi), piemēram, kiberuzbrukumu un drošības konfigurācijas kļūdu risināšanu, drošības uzraudzību, reģistru analīzi un kiberuzbrukumu atklāšanu;

17) “kiberdraudi” ir kiberdraudi, kas definēti Regulas (ES) 2019/881 2. panta 8. punktā;

18) “kiberdrošības ievainojamību pārvaldība” ir ievainojamību konstatēšana un novēršana;

19) “vienība” ir vienība, kas definēta Direktīvas (ES) 2022/2555 6. panta 38. punktā;

20) “agrīnais brīdinājums” ir informācija, kas ir nepieciešama, lai norādītu, vai pastāv aizdomas, ka būtisku incidentu ir izraisījušas nelikumīgas vai ļaunprātīgas darbības vai ka tam var būt pārrobežu ietekme;

21) “elektroenerģijas kiberdrošības ietekmes indekss” (“*ECII*”) ir indekss vai klasifikācijas skala, ar ko vērtē sekas, ko kiberuzbrukumi var izraisīt darba procesos, kuri ir saistīti ar pārrobežu elektroenerģijas plūsmām;

22) “Eiropas kiberdrošības sertifikācijas shēma” ir shēma, kas definēta Regulas (ES) 2019/881 2. panta 9. punktā;

23) “lielas ietekmes vienība” ir vienība, kas īsteno lielas ietekmes procesu un ko kompetentās iestādes ir identificējušas saskaņā ar šīs regulas 24. pantu;

24) “lielas ietekmes process” ir vienības īstenots darba process, kura elektroenerģijas kiberdrošības ietekmes rādītāji pārsniedz lielas ietekmes sliekšņvērtību;

25) “lielas ietekmes aktīvs” ir aktīvs, kas ir nepieciešams lielas ietekmes procesa īstenošanai;

26) “lielas ietekmes sliekšņvērtība” ir šīs regulas 19. panta 3. punkta b) apakšpunktā minētās elektroenerģijas kiberdrošības ietekmes rādītāju vērtības, kuru pārsniegšana nozīmē, ka kiberuzbrukums darbības procesam izraisīs lielus traucējumus pārrobežu elektroenerģijas plūsmās;

27) “lielas ietekmes perimetrs” ir perimetrs, ko ir noteikusi šīs regulas 2. panta 1. punktā minēta vienība un kas ietver visus lielas ietekmes aktīvus, un kurā var kontrolēt piekļuvi šādiem aktīviem, un kurš nosaka minimālo kiberdrošības kontroles pasākumu piemērošanas tvērumu;

28) “IKT produkts” ir IKT produkts, kas definēts Regulas (ES) 2019/881 2. panta 12. punktā;

29) “IKT pakalpojums” ir IKT pakalpojums, kas definēts Regulas (ES) 2019/881 2. panta 13. punktā;

30) “IKT process” ir IKT process, kas definēts Regulas (ES) 2019/881 2. panta 14. punktā;

31) “mantota sistēma” ir mantota IKT sistēma, kas definēta Regulas (ES) 2022/2554 3. panta 3. punktā;

32) “valsts vienotais kontaktpunkts” ir vienotais kontaktpunkts, ko katra dalībvalsts izrauga vai izveido saskaņā ar Direktīvas (ES) 2022/2555 8. panta 3. punktu;

33) “TID kiberkrīžu pārvaldības iestādes” ir iestādes, ko izrauga vai izveido saskaņā ar Direktīvas (ES) 2022/2555 9. panta 1. punktu;

34) “oriģinators” ir vienība, kura sāka informācijas apmaiņas, informācijas kopīgošanas vai informācijas glabāšanas gadījumu;

35) “iepirkuma specifikācijas” ir specifikācijas, ko vienības nosaka jaunu vai atjauninātu IKT produktu, IKT procesu vai IKT pakalpojumu iepirkumam;

36) “pārstāvis” ir Savienībā pastāvīgi dzīvojoša fiziska persona vai Savienībā iedibināta juridiska persona, kura ir nepārprotami izraudzīta, lai pārstāvētu lielas vai kritiskas ietekmes vienību, kas nav iedibināta Savienībā, bet sniedz pakalpojumus vienībām Savienībā, un pie kuras kompetentā iestāde vai *CSIRT* var vērsties saistībā ar šajā regulā noteiktajiem attiecīgās vienības pienākumiem tā vietā, lai vērstos pie pašas lielas vai kritiskas ietekmes vienības;

37) “risks” ir risks, kas definēts Regulas (ES) 2022/2555 6. panta 9. punktā;

38) “riska ietekmes matrica” ir matrica, ko izmanto riska novērtēšanā, lai katram vērtējamajam riskam noteiktu riska ietekmes līmeni;

39) “vienlaicīga elektroenerģētiskā krīze” ir elektroenerģētiskā krīze, kas definēta Regulas (ES) 2019/941 2. panta 10. punktā;

40) “vienības līmeņa vienotais kontaktpunkts” ir vienotais kontaktpunkts vienības līmenī, ko izrauga saskaņā ar šīs regulas 38. panta 1. punkta c) apakšpunktu;

41) “ieinteresētā persona” ir ikviena persona, kas ir ieinteresēta organizācijas vai procesa sekmīgā un nepārtrauktā darbībā, piemēram, darbinieki, direktori, kapitāldaļu īpašnieki, regulatori, apvienības, piegādātāji un klienti;

42) “standarts” ir standarts, kas definēts Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1025/2012 ([16]) 2. panta 1. punktā;

43) “sistēmas darbības reģions” ir saskaņā ar Regulas (ES) 2019/943 36. pantu izveidotie sistēmas darbības reģioni, kā noteikts I pielikumā *ACER* Lēmumā 05-2022 par sistēmas darbības reģionu noteikšanu;

44) “sistēmas operatori” ir “sadales sistēmas operators” (SSO) un “pārvades sistēmas operators” (PSO), kas definēti Direktīvas (ES) 2019/944 2. panta 29. un 35. punktā;

45) “Savienības mēroga kritiskas ietekmes process” ir elektroenerģijas sektora process (tajā var būt iesaistītas vairākas vienības), pret kuru vērsta kiberuzbrukuma ietekmi var atzīt par kritisku, veicot Savienības mēroga kiberdrošības risku novērtējumu;

46) “Savienības mēroga lielas ietekmes process” ir elektroenerģijas sektora process (tajā var būt iesaistītas vairākas vienības), pret kuru vērsta kiberuzbrukuma ietekmi var uzskatīt par lielu, veicot Savienības mēroga kiberdrošības risku novērtējumu;

47) “aktīvi izmantota neizlabota ievainojamība” ir vēl nepubliskota un neizlabota ievainojamība, par kuru ir ticami pierādījumi, ka kāds sistēmas aktors bez sistēmas īpašnieka atļaujas ir veicis ļaunprātīga koda izpildi;

48) “ievainojamība” ir ievainojamība, kas definēta Direktīvas (ES) 2022/2555 6. panta 15. punktā.

*4. pants*

**Kompetentā iestāde**

1. Iespējami ātrāk, bet katrā ziņā ne vēlāk kā līdz 2024. gada 13. decembrī katra dalībvalsts izrauga valsts pārvaldes vai regulatīvo iestādi, kura ir atbildīga par šajā regulā tai uzdoto uzdevumu izpildi (“kompetentā iestāde”). Kamēr kompetentajai iestādei vēl nav uzdots pildīt uzdevumus saskaņā ar šo regulu, šajā regulā paredzētos kompetentās iestādes uzdevumus pilda regulatīvā iestāde, ko katra dalībvalsts ir norīkojusi saskaņā ar Direktīvas (ES) 2019/944 57. panta 1. punktu.

2. Dalībvalstis bez vilcināšanās informē Komisiju, *ACER*, *ENISA*, saskaņā ar Direktīvas (ES) 2022/2555 14. pantu izveidoto TID sadarbības grupu un saskaņā ar Komisijas 2012. gada 15. novembra Lēmuma ([17]) 1. pantu izveidoto Elektroenerģijas jautājumu koordinācijas grupu un paziņo tām saskaņā ar šā panta 1. punktu izraudzītās kompetentās iestādes nosaukumu un kontaktinformāciju un visas turpmākās izmaiņas šādos datos.

([16]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1025/2012 (2012. gada 25. oktobris) par Eiropas standartizāciju, ar ko groza Padomes Direktīvas 89/686/EEK un 93/15/EEK un Eiropas Parlamenta un Padomes Direktīvas 94/9/EK, 94/25/EK, 95/16/EK, 97/23/EK, 98/34/EK, 2004/22/EK, 2007/23/EK, 2009/23/EK un 2009/105/EK, un ar ko atceļ Padomes Lēmumu 87/95/EEK un Eiropas Parlamenta un Padomes Lēmumu Nr. 1673/2006/EK (OV L 316, 14.11.2012., 12. lpp.).

([17]) Komisijas Lēmums (2012. gada 15. novembris), ar ko izveido Elektroenerģijas jautājumu koordinācijas grupu (2012/C 353/02) (OV C 353, 17.11.2012., 2. lpp.).

3. Dalībvalstis var atļaut savai kompetentajai iestādei deleģēt šajā regulā tām uzdotos uzdevumus citām valsts iestādēm, izņemot šīs regulas 5. pantā uzskaitītos uzdevumus. Kompetentā iestāde uzrauga, kā šo regulu piemēro tās iestādes, kurām tā ir deleģējusi uzdevumus. Kompetentā iestāde, ja tā ir deleģējusi kādu uzdevumu citām iestādēm, paziņo Komisijai, *ACER*, Elektroenerģijas jautājumu koordinācijas grupai, *ENISA* un TID sadarbības grupai šādu iestāžu nosaukumus, kontaktinformāciju, deleģētos uzdevumus un visas turpmākās izmaiņas šādos datos.

*5. pants*

**Sadarbība starp attiecīgajām iestādēm un struktūrām valsts līmenī**

Kompetentās iestādes koordinē un nodrošina pienācīgu sadarbību starp kiberdrošības kompetentajām iestādēm, kiberkrīžu pārvaldības iestādēm, VRI, riskgatavības kompetentajām iestādēm un *CSIRT* nolūkā pildīt šajā regulā noteiktos pienākumus. Kompetentās iestādes arī rūpējas par koordināciju ar citām dalībvalsts noteiktām struktūrām un iestādēm, lai nodrošinātu procedūru efektivitāti un izvairītos no uzdevumu un pienākumu dublēšanās. Kompetentās iestādes var dot rīkojumu attiecīgajām VRI pieprasīt *ACER* atzinumu saskaņā ar šīs regulas 8. panta 3. punktu.

*6. pants*

**Noteikumi vai metodikas vai plāni**

1. PSO sadarbībā ar ES SSO struktūru izstrādā noteikumu vai metodiku priekšlikumus saskaņā ar šā panta 2. punktu vai plānu priekšlikumus saskaņā ar šā panta 3. punktu.

2. Visu kompetento iestāžu apstiprinājums ir nepieciešams šādiem noteikumiem vai metodikām un to grozījumiem:

a) kiberdrošības risku novērtēšanas metodikas saskaņā ar šīs regulas 18. panta 1. punktu;

b) visaptverošais pārrobežu elektroenerģijas plūsmu kiberdrošības risku novērtējuma ziņojums saskaņā ar šīs regulas 23. pantu;

c) minimālie un pastiprinātie kiberdrošības kontroles pasākumi saskaņā ar šīs regulas 29. pantu, elektroenerģijas kiberdrošības kontroles pasākumu kartēšana salīdzinājumā ar standartiem saskaņā ar šīs regulas 34. pantu, tajā skaitā minimālie un pastiprinātie kiberdrošības kontroles pasākumi piegādes ķēdē saskaņā ar šīs regulas 33. pantu;

d) kiberdrošības iepirkuma ieteikums saskaņā ar šīs regulas 35. pantu;

e) kiberuzbrukumu klasifikācijas skalas metodika saskaņā ar šīs regulas 37. panta 8. punktu.

3. Reģionālo kiberdrošības risku mazināšanas plānu priekšlikumiem saskaņā ar šīs regulas 22. pantu ir nepieciešams visu attiecīgā sistēmas darbības reģiona kompetento iestāžu apstiprinājums.

4. Priekšlikumos šā panta 2. punktā uzskaitītajiem noteikumiem un metodikām un šā panta 3. punktā uzskaitītajiem plāniem iekļauj ierosinātos īstenošanas termiņus un aprakstu par to paredzamo ietekmi uz šīs regulas mērķiem.

5. ES SSO struktūra var iesniegt attiecīgajiem PSO pamatotu atzinumu ne vēlāk kā trīs nedēļas pirms termiņa, kurā noteikumu vai metodiku priekšlikums vai plānu priekšlikums ir jāiesniedz kompetentajām iestādēm. Par noteikumu vai metodiku priekšlikumu vai plānu priekšlikumu atbildīgie PSO pirms priekšlikumu iesniegšanas kompetentajām iestādēm apstiprināšanai ņem vērā ES SSO struktūras pamatoto atzinumu. Ja ES SSO struktūras atzinumu neņem vērā, PSO sniedz pamatojumu šādai rīcībai.

6. PSO, kuri kopā izstrādā noteikumus un metodikas vai plānus, cieši sadarbojas savā starpā. PSO ar *ENTSO-E* palīdzību un sadarbībā ar ES SSO struktūru regulāri informē kompetentās iestādes un *ACER* par sasniegto progresu noteikumu vai metodiku vai plānu izstrādē.

*7. pants*

**PSO balsošanas kārtība**

1. Ja PSO, lemjot par noteikumu vai metodiku priekšlikumiem nespēj vienoties, tie lēmumu pieņem kvalificēta vairākuma balsošanā. Balsojot par šādiem priekšlikumiem, kvalificēto vairākumu aprēķina šādi:

a) PSO, kas pārstāv vismaz 55 % no dalībvalstīm, un

b) PSO, kas pārstāv dalībvalstis, kurās dzīvo vismaz 65 % no Savienības iedzīvotājiem.

2. Bloķējošo mazākumu attiecībā uz lēmumiem par šīs regulas 6. panta 2. punktā uzskaitītajiem noteikumu vai metodiku priekšlikumiem veido PSO, kas pārstāv vismaz četras dalībvalstis, pretējā gadījumā uzskata, ka kvalificētais balsu vairākums ir panākts.

3. Ja viena sistēmas darbības reģiona PSO, lemjot par šīs regulas 6. panta 2. punktā uzskaitītajiem plānu priekšlikumiem, nespēj vienoties un ja attiecīgajā reģionā ietilpst vairāk nekā piecas dalībvalstis, PSO pieņem lēmumu kvalificēta vairākuma balsošanā. Kvalificētam balsu vairākumam par šīs regulas 6. panta 2. punktā uzskaitītajiem priekšlikumiem ir nepieciešams šāds balsu vairākums:

a) PSO, kas pārstāv vismaz 72 % no iesaistītajām dalībvalstīm, un

b) PSO, kas pārstāv dalībvalstis, kurās dzīvo vismaz 65 % no attiecīgās teritorijas iedzīvotājiem.

4. Bloķējošo mazākumu attiecībā uz lēmumiem par plānu priekšlikumiem veido vismaz minimālais skaits to PSO, kuri pārstāv vairāk nekā 35 % iesaistīto dalībvalstu iedzīvotāju, un PSO, kas pārstāv vismaz vēl vienu iesaistīto dalībvalsti, pretējā gadījumā uzskata, ka kvalificētais balsu vairākums ir panākts.

5. Kad PSO pieņem lēmumus par noteikumu vai metodiku priekšlikumiem saskaņā ar šīs regulas 6. panta 2. punktu, katrai dalībvalstij ir viena balss. Ja dalībvalsts teritorijā ir vairāki PSO, dalībvalsts sadala balsstiesības starp šiem PSO.

6. Ja PSO sadarbībā ar ES SSO struktūru neiesniedz kompetentajām iestādēm sākotnējo vai grozīto noteikumu vai metodiku priekšlikumu vai plānu priekšlikumu šajā regulā noteiktajos termiņos, tie iesniedz attiecīgajām kompetentajām iestādēm un *ACER* attiecīgo noteikumu vai metodiku vai plānu projektus. Tie paskaidro, kāpēc tiem nav izdevies vienoties. Kompetentās iestādes kopīgi veic atbilstošas darbības nepieciešamo noteikumu vai metodiku vai nepieciešamo plānu pieņemšanai. To var paveikt, piemēram, pieprasot grozījumu izdarīšanu projektos saskaņā ar šo punktu, pārskatot projektus un sagatavojot to galīgās versijas vai, ja projekti nav iesniegti, nosakot un apstiprinot nepieciešamos noteikumus vai metodikas vai plānus.

*8. pants*

**Priekšlikumu iesniegšana kompetentajām iestādēm**

1. PSO iesniedz noteikumu vai metodiku priekšlikumus vai plānu priekšlikumus attiecīgajām kompetentajām iestādēm apstiprināšanai termiņos, kuri ir noteikti attiecīgi šīs regulas 18., 23., 29., 33., 34., 35. un 37. pantā. Kompetentās iestādes var kopīgi pagarināt noteiktos termiņus izņēmuma apstākļos, jo īpaši gadījumos, kad termiņu nav iespējams ievērot no PSO vai ES SSO struktūras neatkarīgu iemeslu dēļ.

2. Noteikumu vai metodiku priekšlikumus vai plānu priekšlikumus, ko iesniedz kompetentajām iestādēm atbilstīgi šā panta 1. punktam, vienlaikus iesniedz *ACER* zināšanai.

3. Pēc VRI kopīga pieprasījuma *ACER* sniedz atzinumu par noteikumu vai metodiku priekšlikumu vai plānu priekšlikumu sešu mēnešu laikā pēc attiecīgo priekšlikumu saņemšanas un paziņo savu atzinumu VRI un kompetentajām iestādēm. VRI, KKI un citas iestādes, kas izraudzītas kā kompetentās iestādes, veic saskaņošanu savā starpā, pirms VRI pieprasa *ACER* atzinumu. *ACER* var iekļaut šādā atzinumā ieteikumus. Pirms atzinuma sniegšanas par šīs regulas 6. panta 2. punktā uzskaitītajiem priekšlikumiem *ACER* apspriežas ar *ENISA*.

4. Kompetentās iestādes apspriežas savā starpā un cieši sadarbojas, lai panāktu vienošanos par ierosinātajiem noteikumiem vai metodikām vai ierosinātajiem plāniem. Pirms noteikumu vai metodiku vai plānu apstiprināšanas tās pārskata un pilnveido priekšlikumus, nepieciešamības gadījumā iepriekš apspriežoties ar *ENTSO-E* un ES SSO struktūru, lai nodrošinātu, ka priekšlikumi atbilst šai regulai un veicina vienādi augstu kiberdrošības līmeni visā Savienībā.

5. Kompetentās iestādes pieņem lēmumu par noteikumiem vai metodikām vai plāniem sešu mēnešu laikā pēc attiecīgo noteikumu vai metodiku vai plānu iesniegšanas attiecīgajā kompetentajā iestādē vai – atbilstošos gadījumos – pēdējā no iesaistītajām attiecīgajām kompetentajām iestādēm.

6. Ja ir saņemts *ACER* atzinums, attiecīgās kompetentās iestādes ņem vērā šādu atzinumu un pieņem lēmumu sešu mēnešu laikā pēc *ACER* atzinuma saņemšanas.

7. Ja kompetentās iestādes kopīgi prasa grozīt ierosinātos noteikumus vai metodikas vai plānus, lai tās varētu tos apstiprināt, PSO sadarbībā ar ES SSO struktūru izstrādā priekšlikumu šādiem grozījumiem noteikumos vai metodikās vai plānos. PSO iesniedz grozīto priekšlikumu apstiprināšanai divu mēnešu laikā pēc attiecīgā pieprasījuma saņemšanas no kompetentajām iestādēm. Kompetentās iestādes lēmumu par grozītajiem noteikumiem vai metodikām vai grozītajiem plāniem pieņem divu mēnešu laikā pēc to iesniegšanas.

8. Ja kompetentās iestādes nespēj vienoties šā panta 5. vai 7. punktā norādītajos termiņos, tās informē par to Komisiju. Komisija var veikt atbilstošus pasākumus, lai noteikumus vai metodikas vai plānus būtu iespējams pieņemt.

9. Kad kompetentās iestādes ir apstiprinājušas noteikumus vai metodikas vai plānus, PSO ar *ENTSO-E* un ES SSO struktūras palīdzību publicē tos savās tīmekļa vietnēs, ja vien šādu informāciju neuzskata par konfidenciālu saskaņā ar šīs regulas 47. pantu.

10. Kompetentās iestādes var kopīgi pieprasīt, lai PSO un ES SSO struktūra iesniegtu priekšlikumus par grozījumiem apstiprinātajos noteikumos vai metodikās vai apstiprinātajos plānos, un noteikt termiņu šādu priekšlikumu iesniegšanai. PSO sadarbībā ar ES SSO struktūru var iesniegt kompetentajām iestādēm priekšlikumus par grozījumiem arī pēc pašu iniciatīvas. Priekšlikumus par grozījumiem noteikumos vai metodikās vai par grozījumiem plānos izstrādā un apstiprina saskaņā ar šajā pantā noteikto procedūru.

11. Ne retāk kā ik pēc trim gadiem pēc attiecīgo noteikumu vai metodiku vai attiecīgo plānu pieņemšanas PSO sadarbībā ar ES SSO struktūru izvērtē pieņemto noteikumu vai metodiku vai pieņemto plānu lietderīgumu un konstatējumus bez liekas vilcināšanās paziņo kompetentajām iestādēm un *ACER*.

*9. pants*

**Apspriešanās**

1. PSO ar *ENTSO-E* palīdzību un sadarbībā ar ES SSO struktūru apspriež šīs regulas 6. panta 2. punktā uzskaitīto noteikumu vai metodiku priekšlikumu projektus vai šīs regulas 6. panta 3. punktā uzskaitīto plānu priekšlikumu projektus ar ieinteresētajām personām, tajā skaitā *ACER*, *ENISA* un katras dalībvalsts kompetento iestādi. Apspriešanās ilgst vismaz mēnesi.

2. Priekšlikumus šīs regulas 6. panta 2. punktā uzskaitītajiem noteikumiem vai metodikām, ko PSO iesnieguši sadarbībā ar ES SSO struktūru, publicē un iesniedz apspriešanai Savienības līmenī. Priekšlikumus šīs regulas 6. panta 3. punktā uzskaitītajiem plāniem, ko PSO iesnieguši sadarbībā ar ES SSO struktūru reģionālā līmenī, publicē un iesniedz apspriešanai vismaz reģionālā līmenī.

3. Ieinteresēto personu viedokļus, ko tās paudušas saskaņā ar šā panta 1. punktu sarīkotās apspriešanās laikā, PSO (ar *ENTSO-E* palīdzību) un ES SSO struktūra, kuri ir atbildīgi par noteikumu vai metodiku priekšlikumu vai plānu priekšlikumu, pienācīgi ņem vērā pirms attiecīgā priekšlikuma iesniegšanas regulatīvajām iestādēm apstiprināšanai. Visos gadījumos kopā ar priekšlikumu iesniedz argumentētu pamatojumu tam, kāpēc apspriešanā paustie viedokļi ir vai nav ņemti vērā, un to savlaicīgi publicē pirms noteikumu vai metodiku priekšlikuma publicēšanas vai vienlaikus ar to.

*10. pants*

**Ieinteresēto personu iesaiste**

*ACER* ciešā sadarbībā ar *ENTSO-E* un ES SSO struktūru organizē ieinteresēto personu iesaisti, tajā skaitā regulāras sanāksmes ar ieinteresētajām personām, lai konstatētu problēmas un piedāvātu uzlabojumus saistībā ar šo regulu.

*11. pants*

**Izmaksu atgūšana**

1. Izmaksas, ko sedz PSO un SSO, uz kuriem attiecas tīkla tarifu regulācija, un kas rodas no šajā regulā noteikto pienākumu izpildes, tajā skaitā izmaksas, ko sedz *ENTSO-E* un ES SSO struktūra, vērtē katras dalībvalsts attiecīgā VRI.

2. Izmaksas, kas novērtētas kā pamatotas, efektīvas un samērīgas, atgūst, izmantojot tīkla tarifus vai citus piemērotus mehānismus, ko nosaka attiecīgā VRI.

3. Pēc attiecīgās VRI pieprasījuma šā panta 1. punktā minētie PSO un SSO saprātīgā termiņā, ko nosaka VRI, iesniedz informāciju, kas ir nepieciešama, lai atvieglotu radušos izmaksu novērtēšanu.

*12. pants*

**Uzraudzība**

1. *ACER* uzrauga šīs regulas īstenošanu saskaņā ar Regulas (ES) 2019/943 32. panta 1. punktu un Regulas (ES) 2019/942 4. panta 2. punktu. Uzraudzības gaitā *ACER* var sadarboties ar *ENISA* un lūgt atbalstu no *ENTSO-E* un ES SSO struktūras. *ACER* regulāri informē Elektroenerģijas jautājumu koordinācijas grupu un TID sadarbības grupu par šīs regulas īstenošanu.

2. Pēc šīs regulas stāšanās spēkā *ACER* ne retāk kā ik pēc trim gadiem publicē ziņojumu, kurā:

a) izskata, kā notiek piemērojamo kiberdrošības risku pārvaldības pasākumu īstenošana attiecībā uz lielas ietekmes un kritiskas ietekmes vienībām;

b) nosaka, vai risku novēršanai elektroenerģijas sektorā var būt nepieciešami papildu noteikumi par kopīgām prasībām, plānošanu, uzraudzību, ziņošanu un krīzes pārvaldību; un

c) nosaka jomas, kurās jāveic uzlabojumi, pārskatot šo regulu, vai regulas neaptvertās jomas un jaunās prioritātes, kas var rasties sakarā ar tehnoloģiju attīstību.

3. Līdz 2025. gada 13. jūnijā *ACER* sadarbībā ar *ENISA* un pēc apspriešanās ar *ENTSO-E* un ES SSO struktūru var izdot norādes par attiecīgo informāciju, kas uzraudzības nolūkā jāpaziņo *ACER*, kā arī par šādas informācijas vākšanas procesu un biežumu, pamatojoties uz darbības rādītājiem, ko nosaka saskaņā ar šā panta 5. punktu.

4. Kompetentās iestādes var piekļūt attiecīgajai informācijai, kas ir *ACER* rīcībā un ko tā ir ieguvusi saskaņā ar šo pantu.

5. *ACER* sadarbībā ar *ENISA* un pēc apspriešanās ar *ENTSO-E* un ES SSO struktūru var noteikt nesaistošus darbības rādītājus darbības uzticamības novērtēšanai saistībā ar pārrobežu elektroenerģijas plūsmu kiberdrošības aspektiem.

6. Šīs regulas 2. panta 1. punktā uzskaitītās vienības iesniedz *ACER* informāciju, kas tai ir nepieciešama, lai pildītu šā panta 2. punktā uzskaitītos uzdevumus.

*13. pants*

**Salīdzinošā vērtēšana**

1. Līdz 2025. gada 13. jūnijā *ACER* sadarbībā ar *ENISA* izstrādā kiberdrošības salīdzinošās vērtēšanas nesaistošo rokasgrāmatu. Rokasgrāmata ir paredzēta VRI un izskaidro tām principus, ko izmanto īstenoto kiberdrošības kontroles pasākumu salīdzinošajai vērtēšanai saskaņā ar šā panta 2. punktu, ņemot vērā kontroles pasākumu īstenošanas izmaksas un to īstenošanai izmantoto procesu, produktu, pakalpojumu, sistēmu un risinājumu darbības lietderīgumu. Izstrādājot kiberdrošības salīdzinošās vērtēšanas nesaistošo rokasgrāmatu, *ACER* ņem vērā esošos salīdzinošās vērtēšanas ziņojumus. Kiberdrošības salīdzinošās vērtēšanas nesaistošo rokasgrāmatu *ACER* iesniedz VRI zināšanai.

2. Divpadsmit mēnešu laikā pēc salīdzinošās vērtēšanas rokasgrāmatas izstrādes saskaņā ar šā panta 1. punktu VRI veic salīdzinošās vērtēšanas analīzi, lai novērtētu, vai pašreizējās investīcijas kiberdrošībā:

a) mazina riskus, kas ietekmē pārrobežu elektroenerģijas plūsmas;

b) sniedz vēlamos rezultātus un rada efektivitātes pieaugumu elektroenerģijas sistēmu attīstībā;

c) ir efektīvas un integrētas aktīvu un pakalpojumu vispārējā iepirkumā.

3. Veicot salīdzinošā vērtējuma analīzi, VRI var ņemt vērā *ACER* izstrādāto kiberdrošības salīdzinošās vērtēšanas nesaistošo rokasgrāmatu un vērtē jo īpaši tālāk minēto:

a) tādu ar kiberdrošību saistīto izdevumu vidējais apmērs, kuri paredzēti, lai mazinātu riskus, kas ietekmē pārrobežu elektroenerģijas plūsmas, jo īpaši attiecībā uz lielas ietekmes un kritiskas ietekmes vienībām;

b) sadarbībā ar *ENTSO-E* un ES SSO struktūru – tādu kiberdrošības pakalpojumu, sistēmu un produktu vidējās cenas, kas lielā mērā veicina kiberdrošības risku pārvaldības pasākumu uzlabošanu un uzturēšanu dažādos sistēmas darbības reģionos;

c) šīs regulas īstenošanai piemērotu kiberdrošības pakalpojumu, sistēmu un risinājumu esība un to izmaksu un funkciju salīdzināmības pakāpe, apzinot iespējamos nepieciešamos pasākumus tēriņu efektivitātes uzlabošanai, jo īpaši situācijās, kad var būt nepieciešamas investīcijas kiberdrošības tehnoloģijās.

4. Ar visu informāciju, kas ir saistīta ar salīdzinošā vērtējuma analīzi, rīkojas un šādu informāciju apstrādā, ievērojot šajā regulā noteiktās datu klasifikācijas prasības, minimālos kiberdrošības kontroles pasākumus un pārrobežu elektroenerģijas plūsmu kiberdrošības risku novērtējuma ziņojumu. Šā panta 2. un 3. punktā minēto salīdzinošā vērtējuma analīzi nepublisko.

5. Neskarot šīs regulas 47. pantā norādītās konfidencialitātes prasības un nepieciešamību aizsargāt to vienību drošību, uz kurām attiecas šīs regulas noteikumi, šā panta 2. un 3. punktā minēto salīdzinošā vērtējuma analīzi nosūta visām VRI, visām kompetentajām iestādēm, *ACER*, *ENISA* un Komisijai.

*14. pants*

**Nolīgumi ar ārpussavienības PSO**

1. Ja sistēmas darbības reģions atrodas līdzās trešai valstij, šāda reģiona PSO 18 mēnešu laikā pēc šīs regulas stāšanās spēkā cenšas noslēgt ar kaimiņos esošās trešās valsts PSO tādus nolīgumus, kuri atbilst attiecīgajiem Savienības tiesību aktiem un nosaka pamatu sadarbībai kiberdrošības aizsardzībā, kā arī mehānismu sadarbībai ar šādiem PSO kiberdrošības jomā.

2. Par nolīgumiem, kas noslēgti saskaņā ar šā panta 1. punktu, PSO informē kompetento iestādi.

*15. pants*

**Juridiskie pārstāvji**

1. Vienības, kurām nav iedibinājuma Savienībā, bet kuras sniedz pakalpojumus vienībām Savienībā un kurām saskaņā ar šīs regulas 24. panta 6. punktu ir paziņots, ka tās ir lielas ietekmes vai kritiskas ietekmes vienības, trīs mēnešu laikā pēc šāda paziņojuma saņemšanas rakstveidā izrauga pārstāvi Savienībā un informē par to kompetento iestādi.

2. Šādam pārstāvim piešķir pilnvaras, lai kompetentās iestādes vai *CSIRT* Savienībā varētu saistībā ar šajā regulā noteiktajiem lielas ietekmes vai kritiskas ietekmes vienības pienākumiem vērsties ne tikai pie konkrētās vienības, bet arī pie tās pārstāvja, vai arī vērsties tikai pie pārstāvja, bet ne pašas vienības. Lielas ietekmes vai kritiskas ietekmes vienība piešķir savam juridiskajam pārstāvim nepieciešamās pilnvaras un pietiekamus resursus, lai garantētu to efektīvu un savlaicīgu sadarbību ar attiecīgajām kompetentajām iestādēm vai *CSIRT*.

3. Minētais pārstāvis ir iedibināts vienā no dalībvalstīm, kurā attiecīgā vienība piedāvā savus pakalpojumus. Uzskata, ka šāda vienība ir tās dalībvalsts jurisdikcijā, kurā pārstāvis ir iedibināts. Lielas ietekmes vai kritiskas ietekmes vienības paziņo sava juridiskā pārstāvja vārdu un uzvārdu vai nosaukumu, pasta adresi, e-pasta adresi un tālruņa numuru kompetentajai iestādei tajā dalībvalstī, kurā juridiskajam pārstāvim ir dzīvesvieta vai kurā tas iedibināts.

4. Iecelto juridisko pārstāvi ir iespējams saukt pie atbildības par šajā regulā noteikto pienākumu nepildīšanu, neskarot saukšanu pie atbildības un prasības tiesā, kuras var ierosināt pret pašu lielas ietekmes vai kritiskas ietekmes vienību.

5. Ja nav izraudzīta pārstāvja Savienībā atbilstoši šim pantam, jebkura dalībvalsts, kurā vienība sniedz pakalpojumus, var iesniegt tiesā prasību pret vienību par šajā regulā noteikto pienākumu nepildīšanu.

6. Juridiskā pārstāvja norīkošanu Savienībā saskaņā ar šā panta 1. punktu neuzskata par iedibināšanos Savienībā.

*16. pants*

**Sadarbība starp *ENTSO-E* un ES SSO struktūru**

1. *ENTSO-E* un ES SSO struktūra sadarbojas, veicot kiberdrošības risku novērtējumus saskaņā ar šīs regulas 19. un 21. pantu, un jo īpaši pildot šādus uzdevumus:

a) kiberdrošības risku novērtēšanas metodiku izstrāde saskaņā ar šīs regulas 18. panta 1. punktu;

b) visaptverošā pārrobežu elektroenerģijas plūsmu kiberdrošības risku novērtējuma ziņojuma izstrāde saskaņā ar šīs regulas 23. pantu;

c) vienotā elektroenerģijas kiberdrošības satvara izstrāde saskaņā ar III nodaļu;

d) kiberdrošības iepirkuma ieteikuma izstrāde saskaņā ar šīs regulas 35. pantu;

e) kiberuzbrukumu klasifikācijas skalas metodikas izstrāde saskaņā ar šīs regulas 37. panta 8. punktu;

f) elektroenerģijas kiberdrošības ietekmes indeksa (“*ECII*”) pagaidu versijas izstrāde saskaņā ar šīs regulas 48. panta 1. punkta a) apakšpunktu;

g) lielas ietekmes un kritiskas ietekmes vienību apvienotā pagaidu saraksta izveide saskaņā ar šīs regulas 48. panta 3. punktu;

h) Savienības mēroga lielas ietekmes un kritiskas ietekmes procesu pagaidu saraksta izveide saskaņā ar šīs regulas 48. panta 4. punktu;

i) Eiropas un starptautisko standartu un kontroles pasākumu pagaidu saraksta sagatavošana saskaņā ar šīs regulas 48. panta 6. punktu;

j) Savienības mēroga kiberdrošības risku novērtējuma sagatavošana saskaņā ar šīs regulas 19. pantu;

k) reģionālo kiberdrošības risku novērtējumu sagatavošana saskaņā ar šīs regulas 21. pantu;

l) reģionālo kiberdrošības risku mazināšanas plānu sagatavošana saskaņā ar šīs regulas 22. pantu;

m) norāžu izstrāde par IKT produktiem, IKT pakalpojumiem un IKT procesiem paredzētām Eiropas kiberdrošības sertifikācijas shēmām saskaņā ar šīs regulas 36. pantu;

n) šīs regulas īstenošanas vadlīniju izstrāde sadarbībā ar *ACER* un *ENISA*.

2. Sadarbība starp *ENTSO-E* un ES SSO struktūru var notikt, izveidojot kiberdrošības risku darba grupu.

3. *ENTSO-E* un ES SSO struktūra regulāri informē *ACER*, *ENISA*, TID sadarbības grupu un Elektroenerģijas jautājumu koordinācijas grupu par panākto progresu, īstenojot Savienības mēroga un reģionālos kiberdrošības risku novērtējumus saskaņā ar šīs regulas 19. un 21. pantu.

*17. pants*

**Sadarbība starp *ACER* un kompetentajām iestādēm**

*ACER* sadarbībā ar kompetentajām iestādēm:

1) uzrauga to, kā īsteno kiberdrošības risku pārvaldības pasākumus saskaņā ar šīs regulas 12. panta 2. punkta a) apakšpunktu un ziņošanas pienākumus saskaņā ar šīs regulas 27. un 39. pantu; un

2) uzrauga šīs regulas 6. panta 2. un 3. punktā minēto noteikumu, metodiku vai plānu pieņemšanas procesu un to īstenošanu. Sadarbība starp *ACER-E*, *ENISA* un katru no kompetentajām iestādēm var notikt, izveidojot kiberdrošības risku uzraudzības struktūru.

II NODAĻA

**RISKU NOVĒRTĒŠANA UN ATTIECĪGO KIBERDROŠĪBAS RISKU IDENTIFICĒŠANA**

*18. pants*

**Kiberdrošības risku novērtēšanas metodikas**

1. Līdz 2025. gada 13. martā PSO ar ENTSO-E palīdzību, sadarbībā ar ES SSO struktūru un pēc apspriešanās ar TID sadarbības grupu iesniedz priekšlikumu par metodikām kiberdrošības risku novērtēšanai Savienības, reģionālā un dalībvalsts līmenī.

2. Metodikas kiberdrošības risku novērtēšanai Savienības, reģionālā un dalībvalsts līmenī ietver tālāk minēto:

a) saraksts, kurā uzskaitīti aplūkojamie kiberdraudi, tajā skaitā vismaz šādi piegādes ķēdes apdraudējumi:

   i) būtiski un pēkšņi bojājumi piegādes ķēdē;

   ii) IKT produktu, IKT pakalpojumu vai IKT procesu nepieejamība piegādes ķēdē;

iii) kiberuzbrukumi, kuru sākšanai izmantoti piegādes ķēdes aktori;

iv) sensitīvas informācijas nopludināšana, izmantojot piegādes ķēdi, tajā skaitā piegādes ķēdes izsekošana;

v) vājo vietu vai lūku ieviešana IKT produktos, IKT pakalpojumos vai IKT procesos, izmantojot piegādes ķēdes aktorus;

b) kritēriji, pēc kādiem nosaka, vai kiberdrošības risku ietekme ir liela vai kritiska, šim nolūkam izmantojot sekām un iespējamībai noteiktās sliekšņvērtības;

c) pieeja, ko izmanto, lai analizētu kiberdrošības riskus, ko rada mantotās sistēmas, kiberuzbrukumu izraisītā lavīnveida ietekme un tīkla ekspluatēšanā izmantoto sistēma darbība reāllaikā;

d) pieeja, ko izmanto, lai analizētu kiberdrošības riskus, ko rada atkarība no viena IKT produktu, IKT pakalpojumu vai IKT procesu piegādātāja.

3. Ar metodikām, kas domātas kiberdrošības risku novērtēšanai Savienības, reģionālā un dalībvalsts līmenī, kiberdrošības riskus novērtē, izmantojot to pašu riska ietekmes matricu. Riska ietekmes matrica:

a) mēra kiberuzbrukumu sekas, pamatojoties uz šādiem kritērijiem:

i) zaudētā slodze;

ii) elektroenerģijas ražošanas apjoma samazinājums;

iii) zaudētā jauda primārajā frekvences stabilizēšanas rezervē;

iv) zaudētā jauda elektrotīkla darbības atjaunošanai pēc pilnīgas vai daļējas izslēgšanās, neizmantojot ārēju pārvades tīklu (t.s. darbības atjaunošana pēc izslēgšanās jeb "black start");

v) klientus ietekmējošas elektroapgādes pārtrauces paredzamais ilgums kopā ar pārtrauces mērogu klientu skaita izteiksmē;

vi) citi kvantitatīvi vai kvalitatīvi kritēriji, kas varētu pamatoti kalpot par rādītājiem tādas ietekmes novērtēšanai, kuru rada kiberuzbrukums pārrobežu elektroenerģijas plūsmām;

b) mēra incidenta iespējamību, ko izsaka kā kiberuzbrukumu biežumu gadā.

4. Metodikas kiberdrošības risku novērtēšanai Savienības līmenī apraksta, kā noteikt *ECII* vērtības, kas atbilst lielas ietekmes un kritiskas ietekmes sliekšņvērtībām. *ECII* dod iespēju vienībām, veicot darbības ietekmes novērtējumus saskaņā ar šīs regulas 26. panta 4. punkta c) apakšpunkta i) punktu, ar šā panta 2. punkta b) apakšpunktā minēto kritēriju palīdzību aplēst risku ietekmi uz to darbības procesiem.

5. *ENTSO-E*, rīkojoties saskaņoti ar ES SSO struktūru, informē Elektroenerģijas jautājumu koordinācijas grupu par kiberdrošības risku novērtēšanas metodiku priekšlikumiem, kas izstrādāti saskaņā ar šā panta 1. punktu.

*19. pants*

**Savienības mēroga kiberdrošības risku novērtējums**

1. Neskarot Direktīvas (ES) 2022/2555 22. pantu, *ENTSO-E*, sadarbojoties ar ES SSO struktūru un apspriežoties ar TID sadarbības grupu, deviņu mēnešu laikā pēc metodiku apstiprināšanas saskaņā ar šīs regulas 8. pantu un turpmāk ik pēc trim gadiem veic Savienības mēroga kiberdrošības risku novērtējumu un sagatavo Savienības mēroga kiberdrošības risku novērtējuma ziņojuma projektu. Šim nolūkam tie izmanto metodikas, kas izstrādātas saskaņā ar šīs regulas 18. pantu un apstiprinātas saskaņā ar šīs regulas 8. pantu, lai identificētu, analizētu un izvērtētu iespējamās sekas, ko radīs kiberuzbrukumi, kas ietekmē elektroenerģijas sistēmas darbības drošību un rada traucējumus pārrobežu elektroenerģijas plūsmās. Savienības mēroga kiberdrošības risku novērtējumā neaplūko kiberuzbrukumu radīto juridisko vai finansiālo kaitējumu vai kaitējumu reputācijai.

2. Savienības mēroga kiberdrošības risku novērtējums ietver šādus elementus:

a) Savienības mēroga lielas ietekmes procesi un Savienības mēroga kritiskas ietekmes procesi;

b) riska ietekmes matrica, ko vienības un kompetentās iestādes izmanto, lai novērtētu kiberdrošības risku, kas konstatēts dalībvalsts līmeņa kiberdrošības risku novērtējumā, kurš veikts saskaņā ar šīs regulas 20. pantu, un vienības līmeņa kiberdrošības risku novērtējumā, kurš veikts saskaņā ar šīs regulas 26. panta 2. punkta b) apakšpunktu.

3. Attiecībā uz Savienības mēroga lielas ietekmes procesiem un Savienības mēroga kritiskas ietekmes procesiem Savienības mēroga kiberdrošības risku novērtējums ietver:

a) kiberuzbrukuma iespējamo seku novērtējumu, izmantojot rādītājus, kas ir noteikti kiberdrošības risku novērtēšanas metodikā, kas izstrādāta saskaņā ar šīs regulas 18. panta 2., 3. un 4. punktu un apstiprināta saskaņā ar šīs regulas 8. pantu;

b) *ECII* un lielas ietekmes un kritiskas ietekmes sliekšņvērtības, ko kompetentās iestādes izmanto saskaņā ar šīs regulas 24. panta 1. un 2. punktu, lai identificētu lielas ietekmes un kritiskas ietekmes vienības, kas ir iesaistītas Savienības mēroga lielas ietekmes procesos un Savienības mēroga kritiskas ietekmes procesos.

4. Savienības mēroga kiberdrošības risku novērtējuma ziņojuma projektu, kurā ir izklāstīti Savienības mēroga kiberdrošības risku novērtējuma rezultāti, *ENTSO-E* sadarbībā ar ES SSO struktūru iesniedz *ACER* atzinuma sniegšanai. *ACER* izdod atzinumu par ziņojuma projektu trīs mēnešu laikā pēc tā saņemšanas. Gatavojot ziņojuma galīgo versiju, *ENTSO-E* un ES SSO struktūra maksimāli ņem vērā *ACER* atzinumu.

5. Trīs mēnešu laikā pēc *ACER* atzinuma saņemšanas *ENTSO-E* sadarbībā ar ES SSO struktūru paziņo Savienības mēroga kiberdrošības risku novērtējuma galīgo ziņojumu *ACER*, Komisijai, *ENISA* un kompetentajām iestādēm.

*20. pants*

**Dalībvalsts kiberdrošības risku novērtējums**

1. Katra kompetentā iestāde veic dalībvalsts kiberdrošības risku novērtējumu visām lielas ietekmes un kritiskas ietekmes vienībām attiecīgajā dalībvalstī, izmantojot metodikas, kas izstrādātas saskaņā ar šīs regulas 18. pantu un apstiprinātas saskaņā ar šīs regulas 8. pantu. Dalībvalsts kiberdrošības risku novērtējumā nosaka un analizē riskus, kādi piemīt kiberuzbrukumiem, kuri ietekmē elektroenerģijas sistēmas darbības drošību, radot traucējumus pārrobežu elektroenerģijas plūsmās. Dalībvalsts kiberdrošības risku novērtējumā neaplūko kiberuzbrukumu radīto juridisko vai finansiālo kaitējumu vai kaitējumu reputācijai.

2. Divdesmit viena mēneša laikā pēc paziņojuma nosūtīšanas lielas ietekmes un kritiskas ietekmes vienībām saskaņā ar šīs regulas 24. panta 6. punktu un turpmāk ik pēc trim gadiem, skaitot no minētās dienas, katra kompetentā iestāde pēc apspriešanās ar KKI, kas ir atbildīga par elektroenerģijas jomu, un ar *CSIRT* atbalstu iesniedz *ENTSO-E* un ES SSO struktūrai dalībvalsts kiberdrošības risku novērtējuma ziņojumu, kurā iekļauj šādu informāciju par lielas ietekmes un kritiskas ietekmes darbības procesiem:

a) šīs regulas 29. pantā minēto minimālo un pastiprināto kiberdrošības kontroles pasākumu īstenošanas statuss;

b) saraksts, kurā uzskaitīti kiberuzbrukumi, par kuriem iepriekšējos trīs gados ir ziņots saskaņā ar šīs regulas 38. panta 3. punktu;

c) pārskats, kurā apkopota informācija par kiberdraudiem, par kuriem iepriekšējos trīs gados ir ziņots saskaņā ar šīs regulas 38. panta 6. punktu;

d) par katru Savienības mēroga lielas ietekmes vai kritiskas ietekmes procesu – aplēse par informācijas un attiecīgo aktīvu konfidencialitātes, integritātes un pieejamības apdraudējuma riskiem;

e) nepieciešamības gadījumā – saraksts, kurā uzskaitītas papildu vienības, kas ir identificētas kā lielas ietekmes vai kritiskas ietekmes vienības saskaņā ar šīs regulas 24. panta 1., 2., 3. un 5. punktu.

3. Dalībvalsts kiberdrošības risku novērtējuma ziņojumā ņem vērā dalībvalsts riskgatavības plānu, kas izstrādāts saskaņā ar Regulas (ES) 2019/941 10. pantu.

4. Iekļaujot dalībvalsts kiberdrošības risku novērtējuma ziņojumā šā panta 2. punkta a)–d) apakšpunktā minēto informāciju, to nesasaista ar konkrētām vienībām vai aktīviem. Dalībvalsts kiberdrošības risku novērtējuma ziņojumā iekļauj arī risku novērtējumu attiecībā uz pagaidu atkāpēm, ko dalībvalstu kompetentās iestādes ir atļāvušas saskaņā ar šīs regulas 30. pantu.

5. *ENTSO-E* un ES SSO struktūra var pieprasīt no kompetentajām iestādēm papildu informāciju saistībā ar uzdevumiem, kas ir norādīti šā panta 2. punkta a) un c) apakšpunktā.

6. Kompetentās iestādes nodrošina, ka to sniegtā informācija ir precīza un pareiza.

*21. pants*

**Reģionālo kiberdrošības risku novērtējumi**

1. *ENTSO-E*, sadarbojoties ar ES SSO struktūru un apspriežoties ar attiecīgo reģionālo koordinācijas centru, veic reģionālo kiberdrošības risku novērtējumu katram sistēmas darbības reģionam, izmantojot metodikas, kas izstrādātas saskaņā ar šīs regulas 19. pantu un apstiprinātas saskaņā ar šīs regulas 8. pantu, lai identificētu, analizētu un izvērtētu tādu kiberuzbrukumu riskus, kuri ietekmē elektroenerģijas sistēmas darbības drošību un rada traucējumus pārrobežu elektroenerģijas plūsmās. Reģionālo kiberdrošības risku novērtējumos neaplūko kiberuzbrukumu radīto juridisko vai finansiālo kaitējumu vai kaitējumu reputācijai.

2. *ENTSO-E*, sadarbojoties ar ES SSO struktūru un apspriežoties ar TID sadarbības grupu, 30 mēnešu laikā pēc paziņojuma nosūtīšanas lielas ietekmes un kritiskas ietekmes vienībām saskaņā ar šīs regulas 24. panta 6. punktu un turpmāk ik pēc trim gadiem sagatavo reģionālo kiberdrošības risku novērtējuma ziņojumu katram sistēmas darbības reģionam.

3. Reģionālo kiberdrošības risku novērtējuma ziņojumā ņem vērā attiecīgo informāciju, kas ir iekļauta Savienības mēroga kiberdrošības risku novērtējuma ziņojumos un dalībvalsts kiberdrošības risku novērtējuma ziņojumos.

4. Reģionālo kiberdrošības risku novērtējumā aplūko ar kiberdrošību saistītas reģionālas elektroenerģētiskās krīzes scenārijus, kas apzināti saskaņā ar Regulas (EU) 2019/941 6. pantu.

*22. pants*

**Reģionālo kiberdrošības risku mazināšanas plāni**

1. Trīsdesmit sešu mēnešu laikā pēc paziņojuma nosūtīšanas lielas ietekmes un kritiskas ietekmes vienībām saskaņā ar šīs regulas 24. panta 6. punktu, bet ne vēlāk kā līdz 2031. gada 13. jūnijā, un turpmāk ik pēc trim gadiem PSO ar *ENTSO-E* palīdzību, sadarbojoties ar ES SSO struktūru un apspriežoties ar reģionālajiem koordinācijas centriem un TID sadarbības grupu, izstrādā reģionālo kiberdrošības risku mazināšanas plānu katram sistēmas darbības reģionam.

2. Reģionālo kiberdrošības risku mazināšanas plānā iekļauj:

a) minimālos un pastiprinātos kiberdrošības kontroles pasākumus, ko lielas ietekmes un kritiskas ietekmes vienības piemēro sistēmas darbības reģionā;

b) kiberdrošības riskus, kas ir atlikuši sistēmas darbības reģionos pēc šā punkta a) apakšpunktā minēto kontroles pasākumu piemērošanas.

3. *ENTSO-E* iesniedz reģionālo kiberdrošības risku mazināšanas plānus attiecīgajiem pārvades sistēmu operatoriem, kompetentajām iestādēm un Elektroenerģijas jautājumu koordinācijas grupai. Elektroenerģijas jautājumu koordinācijas grupa var ieteikt grozījumus.

4. PSO ar *ENTSO-E* palīdzību, sadarbojoties ar ES SSO struktūru un apspriežoties ar TID sadarbības grupu, atjaunina reģionālo kiberdrošības risku mazināšanas plānus ik pēc trim gadiem, ja vien apstākļi neprasa atjaunināt tos biežāk.

*23. pants*

**Visaptverošais pārrobežu elektroenerģijas plūsmu kiberdrošības risku novērtējuma ziņojums**

1. Četrdesmit mēnešu laikā pēc paziņojuma nosūtīšanas lielas ietekmes un kritiskas ietekmes vienībām saskaņā ar šīs regulas 24. panta 6. punktu un turpmāk ik pēc trim gadiem PSO ar *ENTSO-E* palīdzību, sadarbojoties ar ES SSO struktūru un apspriežoties ar TID sadarbības grupu, iesniedz Elektroenerģijas jautājumu koordinācijas grupai ziņojumu par kiberdrošības risku novērtējuma rezultātiem attiecībā uz pārrobežu elektroenerģijas plūsmām ("visaptverošais pārrobežu elektroenerģijas plūsmu kiberdrošības risku novērtējuma ziņojums").

2. Visaptverošā pārrobežu elektroenerģijas plūsmu kiberdrošības risku novērtējuma ziņojuma pamatā ir Savienības mēroga kiberdrošības risku novērtējuma ziņojums, dalībvalstu kiberdrošības risku novērtējuma ziņojumi un reģionālo kiberdrošības risku novērtējuma ziņojumi, un tajā iekļauj šādu informāciju:

a) saraksts, kurā uzskaitīti Savienības mēroga lielas ietekmes un kritiskas ietekmes procesi, kas identificēti Savienības mēroga kiberdrošības risku novērtējuma ziņojumā saskaņā ar šīs regulas 19. panta 2. punkta a) apakšpunktu, tajā skaitā aplēses par to kiberdrošības risku iespējamību un ietekmi, kuri izvērtēti reģionālo kiberdrošības risku novērtējuma ziņojumos saskaņā ar šīs regulas 21. panta 2. punktu un 19. panta 3. punkta a) apakšpunktu;

b) aktuālie kiberdraudi, pievēršot īpašu uzmanību jaunradušamies draudiem un riskiem, kas apdraud elektroenerģijas sistēmu;

c) kiberuzbrukumi iepriekšējā periodā Savienības līmenī, sniedzot kritisku pārskatu par to, kā šādi kiberuzbrukumi varēja ietekmēt pārrobežu elektroenerģijas plūsmas;

d) kiberdrošības pasākumu īstenošanas vispārējais statuss;

e) 37. un 38. punktā minēto informācijas plūsmu īstenošanas statuss;

f) saraksts, kurā uzskaitīta informācija vai konkrēti kritēriji informācijas klasificēšanai saskaņā ar šīs regulas 46. pantu;

g) konstatētie un uzsvērtie riski, ko var radīt piegādes ķēdes nedroša pārvaldība;

h) saskaņā ar šīs regulas 44. pantu organizēto reģionālo un starpreģionālo kiberdrošības mācību rezultāti un šādās mācībās gūtā pieredze;

i) analīze par vispārējo pārrobežu kiberdrošības risku attīstību elektroenerģijas sektorā kopš iepriekšējiem reģionālo kiberdrošības risku novērtējumiem;

j) cita informācija, kas var būt noderīga, lai apzinātu šīs regulas iespējamos uzlabojumus vai nepieciešamību pārskatīt šo regulu vai kādus no tās instrumentiem;

k) apkopota un anonimizēta informācija par atkāpēm, kas atļautas saskaņā ar šīs regulas 30. panta 3. punktu.

3. Šīs regulas 2. panta 1. punktā uzskaitītās vienības var piedalīties visaptverošā pārrobežu elektroenerģijas plūsmu kiberdrošības risku novērtējuma ziņojuma sagatavošanā, ievērojot informācijas konfidencialitāti saskaņā ar šīs regulas 47. pantu. PSO ar *ENTSO-E* palīdzību un sadarbībā ar ES SSO struktūru sāk apspriešanos ar minētajām vienībām jau ziņojuma izstrādes sākumposmā.

4. Uz visaptverošo pārrobežu elektroenerģijas plūsmu kiberdrošības risku novērtējuma ziņojumu attiecas šīs regulas 46. pantā minētie noteikumi par informācijas apmaiņas aizsardzību. Neskarot šīs regulas 10. panta 4. punktu un 47. panta 4. punktu, *ENTSO-E* un ES SSO struktūra publicē minētā ziņojuma publisko versiju, kurā nav informācijas, kas varētu kaitēt šīs regulas 2. panta 1. punktā uzskaitītajām vienībām. Minētā ziņojuma publisko versiju publicē vienīgi ar TID sadarbības grupas un Elektroenerģijas jautājumu koordinācijas grupas piekrišanu. *ENTSO-E*, rīkojoties saskaņoti ar ES SSO struktūru, ir atbildīga par ziņojuma publiskās versijas sagatavošanu un publicēšanu.

*24. pants*

**Lielas ietekmes un kritiskas ietekmes vienību identificēšana**

1. Katra kompetentā iestāde, izmantojot *ECII* un lielas ietekmes un kritiskas ietekmes sliekšņvērtības, kas ir iekļautas Savienības mēroga kiberdrošības risku novērtējuma ziņojumā saskaņā ar šīs regulas 19. panta 3. punkta b) apakšpunktu, savā dalībvalstī identificē lielas ietekmes un kritiskas ietekmes vienības, kas ir iesaistītas Savienības mēroga lielas ietekmes un kritiskas ietekmes procesos. Kompetentās iestādes var pieprasīt no vienības savā dalībvalstī informāciju, lai noteiktu konkrētās vienības *ECII* vērtības. Ja vienībai noteiktais *ECII* pārsniedz lielas ietekmes vai kritiskas ietekmes sliekšņvērtību, identificēto vienību iekļauj sarakstā, kurš ietilpst šīs regulas 20. panta 2. punktā minētajā dalībvalsts kiberdrošības risku novērtējuma ziņojumā.

2. Katra kompetentā iestāde, izmantojot *ECII* un lielas ietekmes un kritiskas ietekmes sliekšņvērtības, kas ir iekļautas Savienības mēroga kiberdrošības risku novērtējuma ziņojumā saskaņā ar šīs regulas 19. panta 3. punkta b) apakšpunktu, identificē lielas ietekmes un kritiskas ietekmes vienības, kas nav iedibinātas Savienībā, taču aktīvi darbojas tajā. Kompetentās iestādes var pieprasīt no vienības, kas nav iedibināta Savienībā, informāciju, lai aprēķinātu šādas vienības *ECII* vērtības.

3. Katra kompetentā iestāde savā dalībvalstī kā lielas ietekmes vai kritiskas ietekmes vienības var identificēt vēl citas papildu vienības, ja ir izpildīti tālāk norādītie kritēriji:

a) vienība ietilpst grupā, kas sastāv no vairākām vienībām, un pastāv nozīmīgs risks, ka kiberuzbrukums tās ietekmēs vienlaikus;

b) vienību grupas kopējais *ECII* pārsniedz lielas ietekmes vai kritiskas ietekmes sliekšņvērtību.

4. Ja kompetentā iestāde identificē papildu vienības saskaņā ar šā panta 3. punktu, visus procesus tajās vienībās, kuru grupas kopējais *ECII* pārsniedz lielas ietekmes sliekšņvērtību, uzskata par lielas ietekmes procesiem, un visus procesus tajās vienībās, kuru grupas kopējais *ECII* pārsniedz kritiskas ietekmes robežvērtību, uzskata par kritiskas ietekmes procesiem.

5. Ja kompetentā iestāde identificē šā panta 3. punkta a) apakšpunktā minētās vienības vairākās dalībvalstīs, tā informē par to citas kompetentās iestādes, *ENTSO-E* un ES SSO struktūru. *ENTSO-E* sadarbībā ar ES SSO struktūru, pamatojoties uz visu kompetento iestāžu iesniegto informāciju, sniedz kompetentajām iestādēm analīzi par tādu vairākās dalībvalstīs izvietotu vienību kopumu, kas var radīt izkliedētus traucējumus pārrobežu elektroenerģijas plūsmās un var izraisīt kiberuzbrukumu. Ja vairākās dalībvalstīs izvietotu vienību grupu atzīst par kopumu, kura *ECII* pārsniedz lielas ietekmes vai kritiskas ietekmes sliekšņvērtību, visas iesaistītās kompetentās iestādes identificē šādā grupā ietilpstošās vienības kā lielas ietekmes vai kritiskas ietekmes vienības attiecīgajā dalībvalstī, pamatojoties uz vienību grupas kopējo *ECII*, un iekļauj tās sarakstā, kurš ietilpst Savienības mēroga kiberdrošības risku novērtējuma ziņojumā.

6. Katra kompetentā iestāde deviņu mēnešu laikā pēc paziņojuma saņemšanas no *ENTSO-E* un ES SSO struktūras par Savienības mēroga kiberdrošības risku novērtējuma ziņojumu saskaņā ar 19. panta 5. punktu, bet katrā ziņā ne vēlāk kā līdz 2028. gada 13. jūnijā paziņo sarakstā iekļautajām vienībām, ka tās ir identificētas kā lielas ietekmes vai kritiskas ietekmes vienības attiecīgajā dalībvalstī.

7. Kad kompetentajai iestādei saskaņā ar 27. panta c) apakšpunktu paziņo, ka pakalpojumu sniedzējs ir kritiska IKT pakalpojuma sniedzējs, kompetentā iestāde par to informē kompetentās iestādes tajās dalībvalstīs, kuru teritorijā atrodas pakalpojumu sniedzēja mītne vai pārstāvis. Pēc šādas informācijas saņemšanas attiecīgā kompetentā iestāde paziņo pakalpojumu sniedzējam, ka tas ir identificēts kā kritisku pakalpojumu sniedzējs.

*25. pants*

**Valsts verifikācijas shēmas**

1. Kompetentās iestādes var izveidot valsts verifikācijas shēmu, lai pārliecinātos, ka saskaņā ar šīs regulas 24. panta 1. punktu identificētās kritiskas ietekmes vienības ir īstenojušas valsts tiesisko regulējumu, kas ir iekļauts šīs regulas 34. pantā minētajā kartēšanas matricā. Valsts verifikācijas shēmas pamatā var būt kompetentās iestādes veikta inspekcija, neatkarīga drošības revīzija vai savstarpēja profesionālizvērtēšana, ko kritiskas ietekmes vienības tajā pašā dalībvalstī veic kompetentās iestādes uzraudzībā.

2. Ja kompetentā iestāde nolemj izveidot valsts verifikācijas shēmu, tā nodrošina, ka verifikāciju veic, ievērojot tālāk norādītās prasības:

a) profesionālizvērtēšanas, revīzijas vai inspekcijas veicējs ir neatkarīgs no verificējamās kritiskas ietekmes vienības un neatrodas interešu konfliktā;

b) darbiniekiem, kuri veic profesionālizvērtēšanu, revīziju vai pārbaudi, ir pierādāmas zināšanas šādās jomās:

   i) kiberdrošība elektroenerģijas sektorā;

   ii) kiberdrošības pārvaldības sistēmas;

   iii) revīzijas principi;

   iv) kiberdrošības risku novērtēšana;

   v) vienotais elektroenerģijas kiberdrošības satvars;

   vi) valsts tiesiskais un regulatīvais satvars un Eiropas un starptautiskie standarti, kas attiecas uz verifikācijas tvērumu;

   vii) verifikācijas tvērumā ietilpstošie kritiskas ietekmes procesi;

c) profesionālizvērtēšanas, revīzijas vai pārbaudes veicējam ir pietiekami daudz laika savu uzdevumu izpildei;

d) profesionālizvērtēšanas, revīzijas vai pārbaudes veicējs veic pienācīgus pasākumus, lai verifikācijas laikā iegūto informāciju aizsargātu atbilstoši tās konfidencialitātes līmenim; un

e) profesionālizvērtēšanu, revīziju vai inspekcijas veic vismaz reizi gadā un ne retāk kā ik pēc trim gadiem – par visu verifikācijas tvērumu.

3. Ja kompetentā iestāde nolemj izveidot valsts verifikācijas shēmu, tā katru gadu ziņo *ACER* par to, cik bieži tā ir veikusi inspekcijas saskaņā ar attiecīgo shēmu.

*26. pants*

**Kiberdrošības risku pārvaldība vienības līmenī**

1. Katra lielas ietekmes un kritiskas ietekmes vienība, ko kompetentās iestādes identificējušas saskaņā ar šīs regulas 24. panta 1. punktu, īsteno kiberdrošības risku pārvaldību attiecībā uz visiem saviem aktīviem, kuri ietilpst lielas ietekmes un kritiskas ietekmes perimetrā. Katra lielas ietekmes un kritiskas ietekmes vienība ne retāk kā ik pēc trim gadiem veic risku pārvaldību, kas ietver šā panta 2. punktā minētos posmus.

2. Katra lielas ietekmes un kritiskas ietekmes vienība īsteno kiberdrošības risku pārvaldību, pamatojoties uz pieeju, kuras mērķis ir aizsargāt savas tīklu un informācijas sistēmas un kura ietver tālāk minētos posmus:

a) konteksta noskaidrošana;

b) kiberdrošības risku novērtēšana vienības līmenī;

c) kiberdrošības risku mazināšana;

d) kiberdrošības risku pieņemšana.

3. Konteksta noskaidrošanas posmā katra lielas ietekmes un kritiskas ietekmes vienība:

a) nosaka kiberdrošības risku novērtēšanas tvērumu, kurā iekļauj *ENTSO-E* un ES SSO struktūras identificētos lielas ietekmes un kritiskas ietekmes procesus un citus procesus, pret kuriem var vērst kiberuzbrukumus, kam ir liela vai kritiska ietekme uz pārrobežu elektroenerģijas plūsmām; un

b) nosaka riska izvērtēšanas un riska pieņemšanas kritērijus saskaņā ar riska ietekmes matricu, kuru vienības un kompetentās iestādes izmanto kiberdrošības risku novērtēšanai un kura ir iekļauta Savienības līmeņa, reģionālā līmeņa un dalībvalsts risku novērtēšanas metodikās, ko *ENTSO-E* un ES SSO struktūra izstrādājuši saskaņā ar šīs regulas 19. panta 2. punktu.

4. Kiberdrošības risku novērtēšanas posmā katra lielas ietekmes un kritiskas ietekmes vienība:

a) identificē kiberdrošības riskus, ņemot vērā tālāk minēto:

i) visi aktīvi, kuri atbalsta Savienības mēroga lielas ietekmes un kritiskas ietekmes procesus, kopā ar novērtējumu par iespējamo ietekmi uz pārrobežu elektroenerģijas plūsmām aktīva apdraudējuma gadījumā;

ii) iespējamie kiberdraudi, ņemot vērā kiberdraudus, kas ir identificēti jaunākajā visaptverošajā pārrobežu elektroenerģijas plūsmu kiberdrošības risku novērtējuma ziņojumā, kas ir minēts šīs regulas 23. pantā, un piegādes ķēdes apdraudējumi;

iii) ievainojamības, tajā skaitā ievainojamības mantotās sistēmās;

iv) iespējamu kiberuzbrukumu scenāriji, tajā skaitā tādu kiberuzbrukumu, kuri ietekmē elektroenerģijas sistēmu darbības drošību un rada traucējumus pārrobežu elektroenerģijas plūsmās;

v) Savienības līmenī veiktās attiecīgās risku izvērtēšanas un novērtējumi, tajā skaitā koordinētie kritisko piegādes ķēžu riska novērtējumi saskaņā ar Direktīvas (ES) 2022/2555 22. pantu; un

vi) jau īstenotie kontroles pasākumi;

b) analizē saskaņā ar šā punkta a) apakšpunktu noteikto kiberdrošības risku iespējamību un sekas un nosaka kiberdrošības riska līmeni, izmantojot riska ietekmes matricu, kuru izmanto kiberdrošības risku novērtēšanai un kura ir iekļauta Savienības līmeņa, reģionālā līmeņa un dalībvalsts risku novērtēšanas metodikās, ko PSO ar *ENTSO-E* palīdzību un sadarbībā ar ES SSO struktūru izstrādāja saskaņā ar šīs regulas 19. panta 2. punktu;

c) klasificē aktīvus atkarībā no iespējamām sekām kiberdrošības apdraudējuma gadījumā un nosaka lielas ietekmes un kritiskas ietekmes perimetru, veicot šādas darbības:

i) visiem procesiem, ko aptver kiberdrošības risku novērtējums, veic darbības ietekmes novērtējumu, izmantojot *ECII*;

ii) klasificē procesu kā lielas ietekmes vai kritiskas ietekmes procesu, ja tā *ECII* pārsniedz attiecīgi lielas ietekmes vai kritiskas ietekmes sliekšņvērtību;

iii) nosaka, ka visi lielas ietekmes un kritiskas ietekmes aktīvi ir nepieciešami attiecīgi lielas ietekmes vai kritiskas ietekmes procesiem;

iv) nosaka lielas ietekmes un kritiskas ietekmes perimetrus, kuri ietver attiecīgi visus lielas ietekmes un kritiskas ietekmes aktīvus, lai piekļuvi šiem perimetriem varētu kontrolēt;

d) izvērtē kiberdrošības riskus un sakārto tos prioritārā secībā, izmantojot šā panta 3. punkta b) apakšpunktā minētos risku izvērtēšanas un risku pieņemšanas kritērijus.

5. Kiberdrošības risku mazināšanas posmā katra lielas ietekmes un kritiskas ietekmes vienība izstrādā vienības līmeņa risku mazināšanas plānu, atlasot risku pārvaldībai un atlikušo risku noteikšanai piemērotus riska mazināšanas risinājumus.

6. Kiberdrošības risku pieņemšanas posmā katra lielas ietekmes un kritiskas ietekmes vienība izlemj, vai pieņemt atlikušo risku, pamatojoties uz riska pieņemšanas kritērijiem, ko noteica saskaņā ar šā panta 3. punkta b) apakšpunktu.

7. Katra lielas ietekmes un kritiskas ietekmes vienība reģistrē šā panta 1. punktā norādītos aktīvus aktīvu reģistrā. Aktīvu reģistrs nav risku novērtējuma ziņojuma sastāvdaļa.

8. Kompetentā iestāde pārbaudes laikā var pārbaudīt reģistrā iekļautos aktīvus.

*27. pants*

**Ziņošana par risku novērtējumu vienības līmenī**

Katra lielas ietekmes un kritiskas ietekmes vienība 12 mēnešu laikā pēc paziņojuma saņemšanas, ka tā ir identificēta kā lielas ietekmes vai kritiskas ietekmes vienība saskaņā ar šīs regulas 24. panta 6. punktu, un turpmāk ik pēc trim gadiem iesniedz kompetentajai iestādei ziņojumu ar šādu informāciju:

1) saraksts, kurā ir uzskaitīti kontroles pasākumi, kas atlasīti iekļaušanai vienības līmeņa risku mazināšanas plānā saskaņā ar šīs regulas 26. panta 5. punktu, un norādīts katra kontroles pasākuma pašreizējais īstenošanas statuss;

2) par katru Savienības mēroga lielas ietekmes vai kritiskas ietekmes procesu – aplēse par informācijas un attiecīgo aktīvu konfidencialitātes, integritātes un pieejamības apdraudējuma risku. Šādu riska aplēsi sagatavo saskaņā ar šīs regulas 19. panta 2. punktā minēto riska ietekmes matricu;

3) saraksts, kurā uzskaitīti kritisko IKT pakalpojumu sniedzēji, kuri vienībā nodrošina kritiskas ietekmes procesus.

III NODAĻA

**VIENOTAIS ELEKTROENERĢIJAS KIBERDROŠĪBAS SATVARS**

*28. pants*

**Vienotā elektroenerģijas kiberdrošības satvara sastāvs, darbība un pārskatīšana**

1. Vienotais elektroenerģijas kiberdrošības satvars sastāv no tālāk minētajiem kontroles pasākumiem un kiberdrošības pārvaldības sistēmas:

a) minimālie kiberdrošības kontroles pasākumi, kas izstrādāti saskaņā ar šīs regulas 29. pantu;

b) pastiprinātie kiberdrošības kontroles pasākumi, kas izstrādāti saskaņā ar šīs regulas 29. pantu;

c) saskaņā ar šīs regulas 34. pantu izstrādātā kartēšanas matrica, kurā šā punkta a) un b) apakšpunktā minētie kontroles pasākumi ir kartēti salīdzinājumā ar atsevišķiem Eiropas un starptautiskiem standartiem un valsts tiesiskajiem vai regulatīvajiem satvariem;

d) saskaņā ar šīs regulas 32. pantu izveidota kiberdrošības pārvaldības sistēma.

2. Visas lielas ietekmes vienības piemēro šā panta 1. punkta a) apakšpunktā minētos minimālos kiberdrošības kontroles pasākumus savā lielas ietekmes perimetrā.

3. Visas kritiskas ietekmes vienības piemēro šā panta 1. punkta b) apakšpunktā minētos pastiprinātos kiberdrošības kontroles pasākumus savā kritiskas ietekmes perimetrā.

4. Septiņu mēnešu laikā pēc pirmā Savienības mēroga kiberdrošības risku novērtējuma ziņojuma projekta iesniegšanas saskaņā ar šīs regulas 19. panta 4. punktu šā panta 1. punktā minēto vienoto elektroenerģijas kiberdrošības satvaru papildina ar minimālajiem un pastiprinātajiem kiberdrošības kontroles pasākumiem piegādes ķēdē, kas izstrādāti saskaņā ar šīs regulas 33. pantu.

*29. pants*

**Minimālie un pastiprinātie kiberdrošības kontroles pasākumi**

1. Septiņu mēnešu laikā pēc pirmā Savienības mēroga kiberdrošības risku novērtējuma ziņojuma projekta iesniegšanas saskaņā ar šīs regulas 19. panta 4. punktu PSO ar *ENTSO-E* palīdzību un sadarbībā ar ES SSO struktūru izstrādā priekšlikumu par minimālajiem un pastiprinātajiem kiberdrošības kontroles pasākumiem.

2. Sešu mēnešu laikā pēc katra reģionālo kiberdrošības risku novērtējuma ziņojuma sagatavošanas saskaņā ar šīs regulas 21. panta 2. punktu PSO ar *ENTSO-E* palīdzību un sadarbībā ar ES SSO struktūru iesniedz kompetentajai iestādei priekšlikumu par grozījumiem minimālajos un pastiprinātajos kiberdrošības kontroles pasākumos. Priekšlikumu sagatavo saskaņā ar šīs regulas 8. panta 10. punktu, un tajā ņem vērā reģionālo risku novērtējumā norādītos riskus.

3. Minimālos un pastiprinātos kiberdrošības kontroles pasākumus verificē, iesaistoties valsts verifikācijas shēmā šīs regulas 31. pantā noteiktajā kārtībā vai organizējot neatkarīgas trešās personas veiktas drošības revīzijas saskaņā ar šīs regulas 25. panta 2. punktā uzskaitītajām prasībām.

4. Izstrādājot sākotnējos minimālos un pastiprinātos kiberdrošības kontroles pasākumus saskaņā ar šā panta 1. punktu, pamatojas uz riskiem, kas ir norādīti šīs regulas 19. panta 5. punktā minētajā Savienības mēroga kiberdrošības risku novērtējuma ziņojumā. Izstrādājot grozītos minimālos un pastiprinātos kiberdrošības kontroles pasākumus saskaņā ar šā panta 2. punktu, pamatojas uz šīs regulas 21. panta 2. punktā minēto reģionālo kiberdrošības risku novērtējuma ziņojumu.

5. Minimālie kiberdrošības kontroles pasākumi ietver kontroles pasākumus nodotās informācijas aizsardzībai saskaņā ar šīs regulas 46. pantu.

6. Divpadsmit mēnešu laikā pēc minimālo un pastiprināto kiberdrošības kontroles pasākumu apstiprināšanas saskaņā ar šīs regulas 8. panta 5. punktu vai pēc katras to atjaunināšanas saskaņā ar šīs regulas 8. panta 10. punktu vienības, kas ir uzskaitītas šīs regulas 2. panta 1. punktā un identificētas kā kritiskas ietekmes un lielas ietekmes vienības saskaņā ar šīs regulas 24. pantu, izstrādājot vienības līmeņa risku mazināšanas plānu saskaņā ar šīs regulas 26. panta 5. punktu, piemēro minimālos kiberdrošības kontroles pasākumus lielas ietekmes perimetrā un pastiprinātos kiberdrošības kontroles pasākumus kritiskas ietekmes perimetrā.

*30. pants*

**Atkāpes no minimālajiem un pastiprinātajiem kiberdrošības kontroles pasākumiem**

1. Šīs regulas 2. panta 1. punktā uzskaitītās vienības var lūgt attiecīgajai kompetentajai iestādei, lai tā atļauj vienībai atkāpties no pienākuma piemērot šīs regulas 29. panta 6. punktā minētos minimālos un pastiprinātos kiberdrošības kontroles pasākumus. Kompetentā iestāde var atļaut šādu atkāpi ar vienu no tālāk minētajiem pamatojumiem:

a) izņēmuma apstākļos, ja vienība var pierādīt, ka atbilstošo kiberdrošības kontroles pasākumu īstenošanas izmaksas ievērojami pārsniegs ieguvumus. Lai palīdzētu vienībām, *ACER* un *ENTSO-E* sadarbībā ar SSO struktūru var kopīgi izstrādāt norādes par kiberdrošības kontroles pasākumu izmaksu aplēšanu;

b) ja vienība iesniedz vienības līmeņa risku mazināšanas plānu, kas paredz izmantot alternatīvus kontroles pasākumus, kuri mazinās kiberdrošības riskus līdz līmenim, kas ir pieņemams saskaņā ar šīs regulas 26. panta 3. punkta b) apakšpunktā minētajiem risku pieņemšanas kritērijiem.

2. Trīs mēnešu laikā pēc šā panta 1. punktā minētā lūguma saņemšanas kompetentā iestāde pieņem lēmumu par to, vai atļaut atkāpi no minimālajiem un pastiprinātajiem kiberdrošības kontroles pasākumiem. Atkāpes no minimālajiem un pastiprinātajiem kiberdrošības kontroles pasākumiem atļauj uz laikposmu, kas nav ilgāks par trim gadiem, paredzot iespēju pēc tam saņemt atļauju atkārtoti.

3. Apkopotu un anonimizētu informāciju par atļautajām atkāpēm kā pielikumu iekļauj šīs regulas 23. pantā minētajā visaptverošajā pārrobežu elektroenerģijas plūsmu kiberdrošības risku novērtējuma ziņojumā. Ja nepieciešams, *ENTSO-E* un ES SSO struktūra kopīgi atjaunina šādu sarakstu.

*31. pants*

**Vienotā elektroenerģijas kiberdrošības satvara verifikācija**

1. Ne vēlāk kā 24 mēnešus pēc šīs regulas 28. panta 1. punkta a), b) un c) apakšpunktā minēto kontroles pasākumu pieņemšanas un tā paša punkta d) apakšpunktā minētās kiberdrošības pārvaldības sistēmas izveides katra saskaņā ar šīs regulas 24. panta 1. punktu identificēta kritiskas ietekmes vienība spēj pēc kompetentās iestādes pieprasījuma pierādīt, ka ir izpildītas prasības par kiberdrošības pārvaldības sistēmu un minimālajiem vai pastiprinātajiem kiberdrošības kontroles pasākumiem.

2. Katra kritiskas ietekmes vienība izpilda šā panta 1. punktā minēto pienākumu, organizējot neatkarīgas trešās personas veiktas drošības revīzijas saskaņā ar šīs regulas 25. panta 2. punktā uzskaitītajām prasībām vai iesaistoties valsts verifikācijas shēmā saskaņā ar šīs regulas 25. panta 1. punktu.

3. Verifikācija par kritiskas ietekmes vienības atbilstību prasībām par kiberdrošības pārvaldības sistēmu un minimālajiem vai pastiprinātajiem kiberdrošības kontroles pasākumiem aptver visus kritiskas ietekmes vienības aktīvus kritiskas ietekmes perimetrā.

4. Kritiskas ietekmes vienības atbilstību prasībām par kiberdrošības pārvaldības sistēmu un minimālajiem vai pastiprinātajiem kiberdrošības kontroles pasākumiem regulāri verificē atkārtoti ne vēlāk kā 36 mēnešus pēc iepriekšējās verifikācijas pabeigšanas un turpmāk ik pēc trim gadiem.

5. Katra saskaņā ar šīs regulas 24. pantu identificētā kritiskas ietekmes vienība pierāda atbilstību prasībām par šīs regulas 28. panta 1. punkta a), b) un c) apakšpunktā minētajiem kontroles pasākumiem un tā paša punkta d) apakšpunkta minētās kiberdrošības pārvaldības sistēmas izveidi, paziņojot kompetentajai iestādei atbilstības verifikācijas rezultātus.

*32. pants*

**Kiberdrošības pārvaldības sistēma**

1. Katra lielas ietekmes un kritiskas ietekmes vienība 24 mēnešu laikā pēc paziņojuma saņemšanas no kompetentās iestādes par to, ka tā ir identificēta kā lielas ietekmes vai kritiskas ietekmes vienība saskaņā ar šīs regulas 24. panta 6. punktu, izveido kiberdrošības pārvaldības sistēmu un turpmāk ik pēc trim gadiem pārskata to, lai:

a) noteiktu kiberdrošības pārvaldības sistēmas tvērumu, ņemot vērā mijiedarbi ar un atkarību no citām vienībām;

b) nodrošinātu, ka visa augstākā vadība ir informēta par attiecīgajiem juridiskajiem pienākumiem un ar savlaicīgu lēmumu pieņemšanu un ātru reaģēšanu aktīvi veicina kiberdrošības pārvaldības sistēmas īstenošanu;

c) nodrošinātu, ka ir pieejami drošības pārvaldības sistēmai nepieciešamie resursi;

d) izstrādātu kiberdrošības politiku, ko dokumentē un izplata gan vienībā, gan pusēm, kuras ietekmē drošības riski;

e) sadalītu un izziņotu pienākumus saistībā ar kiberdrošībai būtiskiem uzdevumiem;

f) īstenotu kiberdrošības risku pārvaldību vienības līmenī, kā tā ir definēta šīs regulas 26. pantā;

g) noteiktu un nodrošinātu resursus, kas ir nepieciešami kiberdrošības pārvaldības sistēmas īstenošanai, uzturēšanai un pastāvīgai uzlabošanai, ņemot vērā nepieciešamo kompetenci un informētību par kiberdrošības resursiem;

h) noteiktu kiberdrošībai būtisku iekšējo un ārējo saziņu;

i) izstrādātu, atjauninātu un kontrolētu dokumentētu informāciju saistībā ar kiberdrošības pārvaldības sistēmu;

j) izvērtētu kiberdrošības pārvaldības sistēmas sniegumu un lietderību;

k) ar plānotiem intervāliem rīkotu iekšējās revīzijas nolūkā nodrošināt kiberdrošības pārvaldības sistēmas sekmīgu īstenošanu un uzturēšanu;

l) ar plānotiem intervāliem izskatītu kiberdrošības pārvaldības sistēmas īstenošanu; un kontrolētu kiberdrošības pārvaldības sistēmas resursu un darbību atbilstību politikai, procedūrām un vadlīnijām un novērstu neatbilstības.

2. Kiberdrošības pārvaldības sistēmas tvērums ietver visus lielas ietekmes un kritiskas ietekmes vienības aktīvus, kuri ietilpst lielas ietekmes un kritiskas ietekmes perimetrā.

3. Kompetentās iestādes mudina izmantot Eiropas vai starptautiskos standartus un specifikācijas, kas ir saistītas ar pārvaldības sistēmām un būtiskas tīklu un informācijas drošībai, taču nepieprasa izmantot konkrēta veida tehnoloģiju un nepieļauj diskrimināciju citu tehnoloģiju izmantošanas gadījumā.

*33. pants*

**Minimālie un pastiprinātie kiberdrošības kontroles pasākumi piegādes ķēdē**

1. Septiņu mēnešu laikā pēc pirmā Savienības mēroga kiberdrošības risku novērtējuma ziņojuma projekta iesniegšanas saskaņā ar šīs regulas 19. panta 4. punktu PSO ar *ENTSO-E* palīdzību un sadarbībā ar ES SSO struktūru izstrādā priekšlikumu par minimālajiem un pastiprinātajiem kiberdrošības kontroles pasākumiem piegādes ķēdē, kas mazinātu Savienības mēroga kiberdrošības risku novērtējumos norādītos piegādes ķēdes riskus, papildinot minimālos un pastiprinātos kiberdrošības kontroles pasākumus, kas izstrādāti saskaņā ar šīs regulas 29. pantu. Minimālos un pastiprinātos kiberdrošības kontroles pasākumus piegādes ķēdē izstrādā kopā ar šīs regulas 29. pantā paredzētajiem minimālajiem un pastiprinātajiem kiberdrošības kontroles pasākumiem. Minimālie un pastiprinātie kiberdrošības kontroles pasākumi piegādes ķēdē aptver visus lielas ietekmes vai kritiskas ietekmes vienības lielas ietekmes vai kritiskas ietekmes perimetrā ietilpstošos IKT produktus, IKT pakalpojumus un IKT procesus visā to aprites ciklā. Izstrādājot priekšlikumu par minimālajiem un pastiprinātajiem kiberdrošības kontroles pasākumiem piegādes ķēdē, apspriežas ar TID sadarbības grupu.

2. Minimālos kiberdrošības kontroles pasākumus piegādes ķēdē veido tādi lielas ietekmes vai kritiskas ietekmes vienības veikti kontroles pasākumi, kuri:

a) ietver ieteikumus IKT produktu, IKT pakalpojumu un IKT procesu iepirkumam attiecībā uz kiberdrošības specifikācijām, kuri paredz vismaz tālāk minēto:

   i) to piegādātāja darbinieku iepriekšējās darbības pārbaude, kuri ir iesaistīti piegādes ķēdē un rīkojas ar sensitīvu informāciju vai kuriem ir piekļuve vienības lielas ietekmes vai kritiskas ietekmes aktīviem. Iepriekšējās darbības pārbaude var ietvert vienības darbinieku vai darbuzņēmēju identitātes un iepriekšējās darbības pārbaudi saskaņā ar valsts tiesību aktiem un procedūrām un attiecīgajiem un piemērojamajiem Savienības tiesību aktiem, tajā skaitā Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 un Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/680 ([18]). Iepriekšējās darbības pārbaudes ir samērīgas un stingri aprobežojas ar to, kas ir nepieciešams. Tās veic vienīgi nolūkā izvērtēt iespējamu drošības risku attiecīgajai vienībai. Tām ir jābūt samērīgām ar veicamā darba prasībām, piekļūstamās informācijas klasifikāciju un subjektīvajiem riskiem, un tās var veikt pati vienība, ārējs uzņēmums, kas veic drošības pārbaudi, vai arī var izmantot valdības noteiktu pārbaudes procedūru;

   ii) procesi IKT produktu, IKT pakalpojumu un IKT procesu drošai un kontrolētai projektēšanai, izstrādei un ražošanai, kas veicina tādu IKT produktu, IKT pakalpojumu un IKT procesu projektēšanu un izstrādi, kuros ir iekļauti pienācīgi tehniskie pasākumi kiberdrošības nodrošināšanai;

   iii) tādu tīklu un informācijas sistēmu izstrāde, kurās ierīces neuzskata par uzticamām pat tad, ja tās ietilpst drošā perimetrā, visi saņemtie pieprasījumi ir jāverificē un tiek piemērots mazāko tiesību princips;

   iv) piegādātāja piekļuve vienības aktīviem;

([18]) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (OV L 119, 4.5.2016., 89. lpp.).

v) piegādātāja līgumiskas saistības aizsargāt vienības sensitīvo informāciju un ierobežot piekļuvi tai;

vi) attiecīgas kiberdrošības iepirkuma specifikācijas, ko izvirza piegādātāja apakšuzņēmējiem;

vii) IKT produktiem, IKT pakalpojumiem vai IKT procesiem noteikto kiberdrošības specifikāciju izsekojamība no izstrādes posma līdz ražošanai un tālāk līdz piegādei;

viii) atbalsts drošības atjauninājumiem visā IKT produktu, IKT pakalpojumu vai IKT procesu dzīves ciklā;

ix) tiesības veikt piegādātāja projektēšanas, izstrādes un ražošanas procesu kiberdrošības revīziju; un

x) piegādātāja riska profila novērtējums;

b) nosaka, ka šādām vienībām jāņem vērā šā punkta a) apakšpunktā minētie ieteikumi iepirkuma organizēšanai, slēdzot līgumus ar piegādātājiem, sadarbības partneriem un citiem piegādes ķēdes dalībniekiem, kuri aptver gan IKT produktu, IKT pakalpojumu vai IKT procesu piegādes parastajā kārtībā, gan nevēlamus notikumus un apstākļus, piemēram, līgumu izbeigšanu vai nodošanu citam līguma partnera nolaidības dēļ;

c) nosaka, ka šādām vienībām jāņem vērā rezultāti, kas iegūti, veicot attiecīgos koordinētos kritisko piegādes ķēžu drošības riska novērtējumus saskaņā ar Direktīvas (ES) 2022/2555 22. panta 1. punktu;

d) ietver kritērijus tādu piegādātāju atlasei un nolīgšanai, kuri spēj izpildīt šā punkta a) apakšpunktā norādītās kiberdrošības specifikācijas un kuru kiberdrošības līmenis ir atbilstošs piegādātāja piegādāto IKT produktu, IKT pakalpojumu vai IKT procesu kiberdrošības riskiem;

e) ietver kritērijus, kas ir paredzēti, lai dažādotu IKT produktu, IKT pakalpojumu un IKT procesu piegādes avotus un mazinātu risku kļūt atkarīgam no viena tirgotāja;

f) ietver kritērijus piegādātāja iekšējo darbības procesu kiberdrošības specifikāciju regulārai uzraudzībai, pārskatīšanai vai revīzijai katra IKT produkta, IKT pakalpojuma un IKT procesa visā aprites ciklā.

3. Izstrādājot kiberdrošības specifikācijas šā panta 2. punkta a) apakšpunktā minētajam kiberdrošības iepirkuma ieteikumam, lielas ietekmes vai kritiskas ietekmes vienības izmanto iepirkuma principus, kuri atbilst Eiropas Parlamenta un Padomes Direktīvai 2014/24/ES ([19]) saskaņā ar šīs regulas 35. panta 4. punktu vai nosaka savas specifikācijas, pamatojoties uz vienības līmeņa kiberdrošības risku novērtējuma rezultātiem.

4. Pastiprinātie kiberdrošības kontroles pasākumi piegādes ķēdē ietver kritiskas ietekmes vienības veiktus kontroles pasākumus, lai iepirkuma gaitā pārliecinātos, ka IKT produkti, IKT pakalpojumi un IKT procesi, ko izmantos kā kritiskas ietekmes aktīvus, atbilst kiberdrošības specifikācijām. IKT produktu, IKT pakalpojumu vai IKT procesu verificē, izmantojot vai nu šīs regulas 31. pantā minēto Eiropas kiberdrošības sertifikācijas shēmu, vai arī vienības atlasītas un organizētas verifikācijas darbības. Verifikācijas darbību dziļums un tvērums ir pietiekams, lai sniegtu pārliecību, ka IKT produktu, IKT pakalpojumu vai IKT procesu var izmantot vienības līmeņa risku novērtējumā norādīto risku mazināšanai. Kritiskas ietekmes vienība dokumentē darbības, ko veic norādīto risku mazināšanai.

5. Minimālos un pastiprinātos kiberdrošības kontroles pasākumus piegādes ķēdē piemēro attiecīgo IKT produktu, IKT pakalpojumu un IKT procesu iepirkumam. Minimālie un pastiprinātie kiberdrošības kontroles pasākumi piegādes ķēdē attieksies uz iepirkuma procesiem, kurus vienībās, kas ir identificētas kā kritiskas ietekmes un lielas ietekmes vienības saskaņā ar šīs regulas 24. pantu, sāk sešus mēnešus pēc šīs regulas 29. pantā minēto minimālo un pastiprināto kiberdrošības kontroles pasākumu pieņemšanas vai atjaunināšanas.

([19]) Eiropas Parlamenta un Padomes Direktīva 2014/24/ES (2014. gada 26. februāris) par publisko iepirkumu un ar ko atceļ Direktīvu 2004/18/EK (OV L 94, 28.3.2014., 65. lpp.).

6. Sešu mēnešu laikā pēc katra reģionālo kiberdrošības risku novērtējuma ziņojuma sagatavošanas saskaņā ar šīs regulas 21. panta 2. punktu PSO ar *ENTSO-E* palīdzību un sadarbībā ar ES SSO struktūru iesniedz kompetentajai iestādei priekšlikumu par grozījumiem minimālajos un pastiprinātajos kiberdrošības kontroles pasākumos piegādes ķēdē. Priekšlikumu sagatavo saskaņā ar šīs regulas 8. panta 10. punktu, un tajā ņem vērā reģionālo risku novērtējumā norādītos riskus.

*34. pants*

**Kartēšanas matrica elektroenerģijas kiberdrošības kontroles pasākumu salīdzināšanai ar standartiem**

1. Septiņu mēnešu laikā pēc Savienības mēroga kiberdrošības risku novērtējuma ziņojuma pirmā projekta iesniegšanas saskaņā ar šīs regulas 19. panta 4. punktu PSO ar *ENTSO-E* palīdzību, sadarbojoties ar ES SSO struktūru un apspriežoties ar *ENISA*, izstrādā priekšlikumu matricai, ar ko kartē šīs regulas 28. panta 1. punkta a) un b) apakšpunktā noteiktos kontroles pasākumus salīdzinājumā ar atsevišķiem Eiropas un starptautiskajiem standartiem, kā arī ar attiecīgajām tehniskajām specifikācijām ("kartēšanas matrica"). *ENTSO-E* un ES SSO struktūra dokumentē dažādu kontroles pasākumu līdzvērtīgumu šīs regulas 28. panta 1. punkta a) un b) apakšpunktā noteiktajiem kontroles pasākumiem.

2. Kompetentās iestādes var iesniegt *ENTSO-E* un ES SSO struktūrai šīs regulas 28. panta 1. punkta a) un b) apakšpunktā noteikto kontroles pasākumu kartējumu ar atsauci uz saistītajiem valsts tiesiskajiem vai regulatīvajiem satvariem, tajā dalībvalstu valsts standartiem saskaņā ar Direktīvas (ES) 2022/2555 25. pantu. Ja dalībvalsts kompetentā iestāde iesniedz šādu kartējumu, *ENTSO-E* un ES SSO struktūra iekļauj attiecīgo valsts kartējumu kartēšanas matricā.

3. Sešu mēnešu laikā pēc katra reģionālo kiberdrošības risku novērtējuma ziņojuma sagatavošanas saskaņā ar šīs regulas 21. panta 2. punktu PSO ar *ENTSO-E* palīdzību, sadarbojoties ar ES SSO struktūru un apspriežoties ar *ENISA*, iesniedz kompetentajai iestādei priekšlikumu par grozījumiem kartēšanas matricā. Priekšlikumu sagatavo saskaņā ar šīs regulas 8. panta 10. punktu, un tajā ņem vērā reģionālo risku novērtējumā norādītos riskus.

IV NODAĻA

**KIBERDROŠĪBAS IEPIRKUMA IETEIKUMI**

*35. pants*

**Kiberdrošības iepirkuma ieteikumi**

1. Darba programmā, ko izveido un atjaunina katrreiz, kad pieņem reģionālo kiberdrošības risku novērtējuma ziņojumu, PSO ar *ENTSO-E* palīdzību un sadarbībā ar ES SSO struktūru izstrādā nesaistošu kiberdrošības iepirkuma ieteikumu kopumus, ko lielas ietekmes un kritiskas ietekmes vienības var izmantot par pamatu lielas ietekmes un kritiskas ietekmes perimetros ietilpstošu IKT produktu, IKT pakalpojumu un IKT procesu iepirkumam. Darba programmā iekļauj tālāk minēto:

a) to IKT produktu, IKT pakalpojumu un IKT procesu apraksts un veidu klasifikācija, kurus lielas ietekmes un kritiskas ietekmes vienības izmanto lielas ietekmes un kritiskas ietekmes perimetrā;

b) saraksts, kurā ir uzskaitīti to IKT produktu, IKT pakalpojumu un IKT procesu veidi, kuriem izstrādā nesaistošu kiberdrošības iepirkuma ieteikumu kopumu, pamatojoties uz attiecīgajiem reģionālo kiberdrošības risku novērtējuma ziņojumiem un lielas ietekmes un kritiskas ietekmes vienību prioritātēm.

2. *ENTSO-E* sadarbībā ar ES SSO struktūru 6 mēnešu laikā pēc reģionālo kiberdrošības risku novērtējuma ziņojuma pieņemšanas vai atjaunināšanas iesniedz *ACER* darba programmas kopsavilkumu.

3. PSO ar *ENTSO-E* palīdzību un sadarbībā ar ES SSO struktūru cenšas nodrošināt, ka nesaistošie kiberdrošības iepirkuma ieteikumi, ko izstrādā, pamatojoties uz attiecīgo kiberdrošības risku novērtējumu, sistēmas darbības reģionos ir līdzīgi vai salīdzināmi. Kiberdrošības iepirkuma ieteikumu kopumi aptver vismaz šīs regulas 33. panta 2. punkta a) apakšpunktā minētās specifikācijas. Ja tas ir iespējams, specifikācijas atlasa no Eiropas un starptautiskajiem standartiem.

4. PSO ar *ENTSO-E* palīdzību un sadarbībā ar ES SSO struktūru nodrošina, ka kiberdrošības iepirkuma ieteikumu kopumi:

a) atbilst Direktīvā 2014/24/ES noteiktajiem iepirkuma principiem; un

b) un ir saderīgi ar jaunākajām pieejamajām Eiropas kiberdrošības sertifikācijas shēmām, kuras attiecas uz IKT produktu, IKT pakalpojumu vai IKT procesu, un ņem vērā šādas shēmas.

*36. pants*

**Norādes par Eiropas kiberdrošības sertifikācijas shēmu izmantošanu IKT produktu, IKT pakalpojumu un IKT procesu iepirkumam**

1. Saskaņā ar šīs regulas 35. pantu izstrādātajos nesaistošajos kiberdrošības iepirkuma ieteikumos var iekļaut nozarspecifiskas norādes par Eiropas kiberdrošības sertifikācijas shēmu izmantošanu, ja ir pieejama kritiskas ietekmes vienību izmantotā IKT produkta, IKT pakalpojuma vai IKT procesa veidam piemērota shēma, bet neskarot satvaru Eiropas kiberdrošības sertifikācijas shēmu izveidei saskaņā ar Regulas (ES) 2019/881 46. pantu.

2. PSO ar *ENTSO-E* palīdzību un sadarbībā ar ES SSO struktūru cieši sadarbojas ar *ENISA*, sniedzot nozarspecifiskas norādes, ko iekļauj nesaistošajos kiberdrošības iepirkuma ieteikumos saskaņā ar šā panta 1. punktu.

V NODAĻA

**INFORMĀCIJAS PLŪSMAS, KIBERUZBRUKUMI UN KRĪZES PĀRVALDĪBA**

*37. pants*

**Informācijas kopīgošanas noteikumi**

1. Ja kompetentā iestāde saņem informāciju saistībā ar ziņojamu kiberuzbrukumu, tā:

a) novērtē šādas informācijas konfidencialitātes līmeni un paziņo novērtējuma iznākumu vienībai bez liekas kavēšanās, bet ne vēlāk kā 24 stundu laikā pēc informācijas saņemšanas;

b) mēģina atrast Savienībā līdzīgu kiberuzbrukumu, par kuru būtu ziņots citām kompetentajām iestādēm, lai noteiktu sakarības starp informāciju, kas saņemta sakarā ar ziņojamo kiberuzbrukumu, un informāciju, kas iesniegta sakarā ar citiem kiberuzbrukumiem, un papildinātu esošo informāciju, stiprinātu un koordinētu reaģēšanu kiberdrošības jomā;

c) ir atbildīga par komercnoslēpumu izņemšanu un informācijas anonimizēšanu saskaņā ar attiecīgajiem valsts un Savienības tiesību aktiem;

d) kopīgo informāciju ar valsts vienotajiem kontaktpunktiem, *CSIRT* un visām saskaņā ar šīs regulas 4. punktu izraudzītajām kompetentajām iestādēm pārējās dalībvalstīs bez liekas kavēšanās, bet ne vēlāk kā 24 stundu laikā pēc informācijas saņemšanas par ziņojamo kiberuzbrukumu, un regulāri sniedz minētajām iestādēm vai struktūrām atjauninātu informāciju;

e) pēc šā panta 1. punkta c) apakšpunktā paredzētās anonimizācijas un komercnoslēpumu izņemšanas izplata informāciju par kiberuzbrukumu kritiskas ietekmes un lielas ietekmes vienībām savā dalībvalstī bez liekas kavēšanās, bet ne vēlāk kā 24 stundu laikā pēc informācijas saņemšanas saskaņā ar šā panta 1. punkta a) apakšpunktu, un regulāri sniedz atjauninātu informāciju, kas ļauj vienībām organizēt iedarbīgu aizsardzību;

f) var pieprasīt, lai ziņojošā lielas ietekmes vai kritiskas ietekmes vienība drošā veidā izplatītu ziņojamo informāciju par kiberuzbrukumu tālāk citām vienībām, kuras tas var ietekmēt, lai panāktu situācijas apzināšanos elektroenerģijas sektorā un nepieļautu, ka īstenojas risks, kas var izraisīt pārrobežu elektroenerģijas plūsmu kiberdrošības incidentu;

g) iesniedz *ENISA* kopsavilkuma ziņojumu ar informāciju par kiberuzbrukumu, kas ir anonimizēta un no kuras ir izņemti komercnoslēpumi.

2. Ja *CSIRT* uzzina par aktīvi izmantotu neizlabotu ievainojamību, tā:

a) nevilcinoties informē par to *ENISA*, izmantojot piemērotu, drošu informācijas apmaiņas kanālu, ja vien citos Savienības tiesību aktos nav noteikts citādi;

b) sniedz atbalstu attiecīgajai vienībai, lai tā saņemtu no ražotāja vai pakalpojuma sniedzēja risinājumu, kā iedarbīgi, koordinēti un ātri pārvaldīt aktīvi izmantoto neizlaboto ievainojamību vai kādus iedarbīgus un efektīvus pasākumus veikt riska mazināšanai;

c) nodod pieejamo informāciju tirgotājam un, ja tas ir iespējams, lūdz ražotāju vai pakalpojuma sniedzēju sagatavot sarakstu, kurā ir uzskaitītas dalībvalstu *CSIRT*, uz kurām attiecas aktīvi izmantotā neizlabotā ievainojamība un kuras ir jāinformē;

d) kopīgo pieejamo informāciju ar *CSIRT*, kuras noskaidrotas saskaņā ar iepriekšējo apakšpunktu, pamatojoties uz principu "nepieciešamība zināt";

e) kopīgo riska mazināšanas stratēģijas un pasākumus, ja tādi ir, attiecībā uz ziņoto aktīvi izmantoto neizlaboto ievainojamību.

3. Ja kompetentā iestāde uzzina par aktīvi izmantotu neizlabotu ievainojamību, tā:

a) rīkojoties saskaņoti ar *CSIRT* savā dalībvalstī, kopīgo riska mazināšanas stratēģijas un pasākumus, ja tādi ir, attiecībā uz ziņoto aktīvi izmantoto neizlaboto ievainojamību;

b) kopīgo informāciju ar *CSIRT* tajā dalībvalstī, kurā tika ziņots par aktīvi izmantoto neizlaboto ievainojamību.

4. Ja kompetentā iestāde uzzina par neizlabotu ievainojamību, bet vēl nav pierādījumu par tās aktīvu izmantošanu, kompetentā iestāde bez liekas kavēšanās saskaņo rīcību ar *CSIRT* koordinētai ievainojamības izpaušanai, kā to paredz Direktīvas (ES) 2022/2555 12. panta 1. punkts.

5. Ja *CSIRT* saņem ar kiberdraudiem saistītu informāciju no vienas vai vairākām lielas ietekmes vai kritiskas ietekmes vienībām saskaņā ar šīs regulas 38. panta 6. punktu, tā bez liekas kavēšanās, bet ne vēlāk kā četru stundu laikā pēc informācijas saņemšanas izplata šo informāciju vai citu informāciju, kas ir svarīga saistīto risku novēršanai, atklāšanai, reaģēšanai uz tiem vai to mazināšanai, savas dalībvalsts kritiskas ietekmes un lielas ietekmes vienībām un attiecīgos gadījumos arī visām attiecīgajām *CSIRT* un savas valsts vienotajam kontaktpunktam.

6. Ja kompetentā iestāde no vienas vai vairākām lielas ietekmes vai kritiskas ietekmes vienībām uzzina informāciju, kas ir saistīta ar kiberdraudiem, tā pārsūta šo informāciju *CSIRT* šā panta 5. punktā norādītajiem nolūkiem.

7. Kompetentās iestādes var pilnībā vai daļēji deleģēt šā panta 3. un 4. punktā noteiktos pienākumus attiecībā uz vienu vai vairākām lielas ietekmes vai kritiskas ietekmes vienībām, kuras darbojas vairākās dalībvalstīs, citai kompetentajai iestādei vienā no šādām dalībvalstīm, ja iesaistītās kompetentās iestādes ir par to vienojušās savā starpā.

8. PSO ar *ENTSO-E* palīdzību un sadarbībā ar ES SSO struktūru līdz 2025. gada 13. jūnijā izstrādā kiberuzbrukumu klasifikācijas skalas metodiku. PSO ar *ENTSO-E* un ES SSO struktūras palīdzību var lūgt kompetentās iestādes apspriesties ar *ENISA* un attiecīgajām kiberdrošības kompetentajām iestādēm, lai saņemtu palīdzību šādas klasifikācijas skalas izstrādē. Metodika nodrošina kiberuzbrukumu klasifikāciju pēc to smaguma, iedalot tos piecos līmeņos, un divi augstākie līmeņi ir "liels" un "kritisks". Klasifikācijas pamatā ir tālāk minēto parametru novērtējums:

a) potenciālā ietekme, ņemot vērā apdraudētos aktīvus un perimetrus, kas noteikti saskaņā ar šīs regulas 26. panta 4. punkta (c) apakšpunktu; un

b) kiberuzbrukuma nopietnība.

9. Līdz 2026. gada 13. jūnijā *ENTSO-E* sadarbībā ar ES SSO struktūru veic priekšizpēti, lai novērtētu iespēju izstrādāt vienotu rīku, kas ļautu visām vienībām kopīgot informāciju ar attiecīgajām valsts iestādēm, un tam nepieciešamās finansiālās izmaksas.

10. Priekšizpētē par šādu vienotu rīku noskaidro, vai ir iespējams, ka:

a) tas atbalsta lielas ietekmes un kritiskas ietekmes vienības, sniedzot attiecīgu ar drošību saistītu informāciju par pārrobežu elektroenerģijas plūsmu darbību, piemēram, ziņojot par kiberuzbrukumiem tuvu reāllaikam un izplatot agrīnos brīdinājumus saistībā ar kiberdrošības jautājumiem un neizpaustām ievainojamībām aprīkojumā, ko izmanto elektroenerģijas sistēmā;

b) to var uzturēt piemērotā un ļoti uzticamā vidē;

c) tas ļauj vākt datus no kritiskas ietekmes un lielas ietekmes vienībām un atvieglo konfidenciālas informācijas izņemšanu un datu anonimizāciju, kā arī datu ātru izplatīšanu kritiskas ietekmes un lielas ietekmes vienībām.

11. *ENTSO-E* sadarbībā ar ES SSO struktūru:

a) apspriežas ar *ENISA* un TID sadarbības grupu, valstu vienotajiem kontaktpunktiem un galveno ieinteresēto personu pārstāvjiem, vērtējot minētās iespējas;

b) iesniedz priekšizpētes rezultātus *ACER* un TID sadarbības grupai.

12. *ENTSO-E* sadarbībā ar ES SSO struktūru var analizēt un veicināt kritiskas ietekmes un lielas ietekmes vienību ierosinātās iniciatīvas šādu informācijas kopīgošanas rīku izvērtēšanai un testēšanai.

*38. pants*

**Lielas ietekmes un kritiskas ietekmes vienību uzdevumi attiecībā uz informācijas kopīgošanu**

1. Katra lielas ietekmes un kritiskas ietekmes vienība:

a) attiecībā uz visiem aktīviem savā kiberdrošības perimetrā, ko nosaka saskaņā ar šīs regulas 26. panta 4. punkta c) apakšpunktu, izveido vismaz KOC spējas:

   i) nodrošināt, ka attiecīgajām tīklu un informācijas sistēmām un lietojumprogrammām ir drošības žurnāli drošības uzraudzībai, lai būtu iespējams atklāt anomālijas un iegūt informāciju par kiberuzbrukumiem;

   ii) īstenot drošības uzraudzību, tajā skaitā atklāt ielaušanās gadījumus un novērtēt tīklu un informācijas sistēmu ievainojamības;

   iii) analizēt un vajadzības gadījumā veikt visus nepieciešamos pasākumus, lai savu iespēju robežās pildītu savu pienākumu aizsargāt vienību;

   iv) piedalīties šajā pantā aprakstītajā informācijas vākšanā un kopīgošanā;

b) ir tiesīga iepirkt visas vai kādu daļu no a) apakšpunktā minētajām spējām no PDPS. Kritiskas ietekmes un lielas ietekmes vienības saglabā atbildību par PDPS un uzrauga to darbu;

c) informācijas kopīgošanas vajadzībām izraudzīt vienības līmeņa vienoto kontaktpunktu.

2. *ENISA* var izdot nesaistošas norādes par šādu spēju veidošanu vai pakalpojuma nodošanu PDPS kā apakšuzņēmējiem, kas ietilpst uzdevumos, kuri tai ir uzdoti saskaņā ar Regulas (ES) 2019/881 6. panta 2. punktu.

3. Katra kritiskas ietekmes un lielas ietekmes vienība nodod attiecīgo informāciju, kas ir saistīta ar ziņojamu kiberuzbrukumu, attiecīgajām *CSIRT* un kompetentajai iestādei bez liekas kavēšanās, bet ne vēlāk kā četru stundu laikā pēc tam, kad kļuva skaidrs, ka par konkrēto incidentu ir jāziņo.

4. Ar kiberuzbrukumu saistītu informāciju uzskata par ziņojamu, ja kiberuzbrukuma skartā vienība ir novērtējusi tā smagumu diapazonā no "liela" līdz "kritiskam", ievērojot kiberuzbrukumu klasifikācijas skalas metodiku, ko paredz šīs regulas 37. panta 8. punkts. Par incidenta klasifikāciju ziņo vienības līmeņa vienotais kontaktpunkts, ko izraudzīja saskaņā ar šā panta 1. punkta c) apakšpunktu.

5. Ja *CSIRT* saņem no kritiskas ietekmes un lielas ietekmes vienībām attiecīgu informāciju, kas ir saistīta ar aktīvi izmantotām neizlabotām ievainojamībām, *CSIRT* var pārsūtīt šādu informāciju attiecīgajai kompetentajai iestādei. Ņemot vērā paziņotās informācijas sensitivitātes līmeni, *CSIRT* var nepārsūtīt informāciju vai novilcināt tās pārsūtīšanu, pamatojoties uz attaisnojošiem iemesliem, kas ir saistīti ar kiberdrošību.

6. Katra kritiskas ietekmes un lielas ietekmes vienība bez liekas kavēšanās iesniedz attiecīgajām *CSIRT* visu informāciju, kas ir saistīta ar ziņojamiem kiberdraudiem, kuriem var būt pārrobežu ietekme. Ar kiberdraudiem saistītu informāciju uzskata par ziņojamu, ja ir izpildīts vismaz viens no tālāk minētajiem nosacījumiem:

a) informācija ir būtiska citām kritiskas ietekmes un lielas ietekmes vienībām, lai tās varētu novērst vai atklāt risku, reaģēt uz to vai mazināt tā ietekmi;

b) konstatētie paņēmieni, taktika un procedūras, ko izmantoja saistībā ar uzbrukumu, ļauj iegūt tādu informāciju kā, piemēram, apdraudētie URL vai IP adreses, jaucējkodi vai citi atribūti, kas noder uzbrukuma kontekstualizēšanai un sakarību noteikšanai;

c) kiberdraudu labākai novērtēšanai un kontekstualizācijai var noderēt papildu informācija, ko sniedz pakalpojumu sniedzēji vai trešās personas, uz kurām šī regula neattiecas.

7. Kopīgojot informāciju saskaņā ar šo pantu, katra kritiskas ietekmes un lielas ietekmes vienība norāda tālāk minēto:

a) ka informāciju iesniedz saskaņā ar šo regulu;

b) vai informācija attiecas uz:

i) ziņojamu kiberuzbrukumu, kā minēts šā panta 3. punktā;

ii) nepubliskotām aktīvi izmantotām neizlabotām ievainojamībām, kā minēts šā panta 4. punktā;

iii) ziņojamu kiberuzbrukumu, kā minēts šā panta 5. punktā;

c) ja tas ir ziņojams kiberuzbrukums – kiberuzbrukuma līmeni saskaņā ar šīs regulas 37. panta 8. punktā minēto kiberuzbrukumu klasifikācijas skalas metodiku un informāciju, ko izmantoja klasifikācijai, tajā skaitā vismaz kiberuzbrukuma smaguma pakāpi.

8. Ja kritiskas ietekmes vai lielas ietekmes vienība ziņo par būtisku incidentu saskaņā ar Direktīvas (ES) 2022/2555 23. pantu un, ziņojot par incidentu saskaņā ar minēto pantu, iesniedz attiecīgu informāciju, kas ir jāiesniedz saskaņā ar šā panta 3. punktu, vienības ziņošanu saskaņā ar minētās direktīvas 23. panta 1. punktu uzskata par informācijas ziņošanu saskaņā ar šā panta 3. punktu.

9. Situācijās, kad informācijas kopīgošana var izraisīt kiberuzbrukumu, katra kritiskas ietekmes un lielas ietekmes vienība ziņo savai kompetentajai iestādei vai *CSIRT*, skaidri norādot konkrētu informāciju, ko drīkst nodot tikai kompetentajai iestādei vai *CSIRT*. Katrai kritiskas ietekmes un lielas ietekmes vienībai ir tiesības iesniegt kompetentajai *CSIRT* informācijas nekonfidenciālo versiju.

*39. pants*

**Kiberuzbrukumu atklāšana un rīkošanās ar saistīto informāciju**

1. Kritiskas ietekmes un lielas ietekmes vienības attīsta nepieciešamās spējas risināt atklātos kiberuzbrukumus, saņemot nepieciešamo atbalstu no attiecīgās kompetentās iestādes, *ENTSO-E* un ES SSO struktūras. Attiecīgajā dalībvalstī izraudzītā CSIRT var sniegt atbalstu kritiskas ietekmes un lielas ietekmes vienībām, pildot uzdevumus, kuri ir uzdoti CSIRT saskaņā ar Direktīvas (ES) 2022/2555 11. panta 5. punkta a) apakšpunktu. Kritiskas ietekmes un lielas ietekmes vienības īsteno iedarbīgus procesus, lai identificētu un klasificētu kiberuzbrukumus, kuri ietekmēs vai var ietekmēt pārrobežu elektroenerģijas plūsmas, un reaģētu uz šādiem uzbrukumiem nolūkā mazināt to ietekmi.

2. Ja kiberuzbrukums ietekmē pārrobežu elektroenerģijas plūsmas, skarto kritiskas ietekmes un lielas ietekmes vienību vienības līmeņa vienotie kontaktpunkti sadarbojas, lai apmainītos ar informāciju, un šo procesu koordinē kompetentā iestāde tajā dalībvalstī, kurā par kiberuzbrukumu ziņoja vispirms.

3. Kritiskas ietekmes un lielas ietekmes vienības:

a) nodrošina, ka to vienības līmeņa vienotajam kontaktpunktam, pamatojoties uz principu "nepieciešamība zināt", ir piekļuve informācijai, ko tās ar kompetentās iestādes starpniecību saņēma no valsts vienotā kontaktpunkta;

b) ja tas jau nav izdarīts saskaņā ar Direktīvas (ES) 2022/2555 3. panta 4. punktu, paziņo savas iedibinājuma dalībvalsts kompetentajai iestādei un valsts vienotajam kontaktpunktam sarakstu, kurā norāda savus vienības līmeņa vienotos kontaktpunktus kiberdrošības jautājumos:

   i) no kuriem kompetentā iestāde un valsts vienotais kontaktpunkts varētu saņemt informāciju par ziņojamiem kiberuzbrukumiem;

   ii) uz kuriem kompetentajām iestādēm un valstu vienotajiem kontaktpunktiem varētu būt jānosūta informācija;

c) kiberuzbrukumu gadījumiem izstrādā kiberuzbrukuma pārvaldības procedūras, tajā skaitā nosaka funkcijas un pienākumus, uzdevumus un reaģēšanas darbības, pamatojoties uz kritiskas ietekmes un lielas ietekmes perimetrā novērojamajām izmaiņām kiberuzbrukuma gaitā;

d) vismaz reizi gadā testē vispārējās kiberuzbrukuma pārvaldības procedūras, testējot vismaz vienu scenāriju par tiešu vai netiešu ietekmi uz pārrobežu elektroenerģijas plūsmām. Kritiskas ietekmes un lielas ietekmes vienības var veikt šādu ikgadējo testu šīs regulas 43. pantā minēto regulāro mācību laikā. Par plāna reaģēšanai uz kiberuzbrukumu ikgadējo testu var izmantot jebkuru reālu darbību reaģēšanai uz kiberuzbrukumu, kura sekas atbilst vismaz 2. līmenim saskaņā ar šīs regulas 37. panta 8. punktā minēto kiberuzbrukumu klasifikācijas skalas metodiku un kura pamatcēlonis ir kiberdrošība.

4. Dalībvalstis var deleģēt šā panta 1. punktā minētos uzdevumus arī reģionālajiem koordinācijas centriem saskaņā ar Regulas (ES) 2019/943 37. panta 2. punktu.

*40. pants*

**Krīzes pārvaldība**

1. Ja kompetentā iestāde konstatē, ka elektroenerģētiskā krīze ir saistīta ar kiberuzbrukumu, kurš ietekmē vairākas dalībvalstis, skarto dalībvalstu kompetentās iestādes, KKI, RKI un TID kiberkrīžu pārvaldības iestādes kopīgi izveido *ad hoc* pārrobežu krīzes koordinācijas grupu.

2. *Ad hoc* pārrobežu krīzes koordinācijas grupa:

a) koordinē visas attiecīgās kiberdrošības informācijas efektīvu izguvi un tās tālāku izplatīšanu krīzes pārvaldības procesā iesaistītajām vienībām;

b) organizē saziņu starp visām krīzes skartajām vienībām un kompetentajām iestādēm, lai mazinātu pārklāšanos un lai analīze un tehniskie reaģēšanas pasākumi, kuru mērķis ir atrisināt vienlaicīgas elektroenerģētiskās krīzes, kuru pamatcēlonis ir kiberdrošība, būtu efektīvāki;

c) sadarbībā ar kompetentajām *CSIRT* nodrošina nepieciešamās specializētās zināšanas, tajā skaitā sniedz incidenta skartajām vienībām praktiskus padomus par iespējamo ietekmes mazināšanas pasākumu īstenošanu;

d) ievērojot šīs regulas 46. pantā noteiktos aizsardzības principus, informē Komisiju un Elektroenerģijas jautājumu koordinācijas grupu un turpmāk regulāri sniedz tām jaunāko informāciju par incidenta statusu;

e) lūdz padomu attiecīgajām iestādēm, aģentūrām vai vienībām, kuras var palīdzēt mazināt elektroenerģētisko krīzi.

3. Ja kiberuzbrukums ir atzīts vai varētu tikt atzīts par plašapmēra kiberdrošības incidentu, *ad hoc* pārrobežu krīzes koordinācijas grupa nekavējoties informē saskaņā ar Direktīvas (ES) 2022/2555 9. panta 1. punktu izveidotās valsts kiberkrīžu pārvaldības iestādes incidenta skartajās dalībvalstīs, kā arī Komisiju un *EU-CyCLONe*. Tādā gadījumā *ad hoc* pārrobežu krīzes koordinācijas grupa sniedz atbalstu *EU-CyCLONe* attiecībā uz nozares specifiku.

4. Kritiskas ietekmes un lielas ietekmes vienības izveido spējas, sagatavo iekšējās vadlīnijas, gatavības plānus un personālu un nodrošina, ka viss minētais ir to rīcībā, lai tās varētu piedalīties pārrobežu krīzes atklāšanā un mazināšanā. Vienlaicīgas elektroenerģētiskās krīzes skarta kritiskas ietekmes vai lielas ietekmes vienība sadarbībā ar kompetento iestādi noskaidro krīzes pamatcēloni, lai noteiktu, kādā apmērā krīze ir saistīta ar kiberuzbrukumu.

5. Dalībvalstis var deleģēt šā panta 4. punktā minētos uzdevumus arī reģionālajiem koordinācijas centriem saskaņā ar Regulas (ES) 2019/943 37. panta 2. punktu.

*41. pants*

**Kiberdrošības krīžu pārvaldības un reaģēšanas plāni**

1. Divdesmit četru mēnešu laikā pēc Savienības mēroga risku novērtējuma ziņojuma paziņošanas *ACER*, tā ciešā sadarbībā ar *ENISA*, *ENTSO-E*, ES SSO struktūru, KKI, kompetentajām iestādēm, RKI, VRI un valstu TID kiberkrīžu pārvaldības iestādēm izstrādā Savienības līmeņa kiberdrošības krīžu pārvaldības un reaģēšanas plānu elektroenerģijas sektoram.

2. Divpadsmit mēnešu laikā pēc tam, kad *ACER* ir izstrādājusi Savienības līmeņa kiberdrošības krīžu pārvaldības un reaģēšanas plānu elektroenerģijas sektoram saskaņā ar šā panta 1. punktu, katra kompetentā iestāde izstrādā valsts kiberdrošības krīžu pārvaldības un reaģēšanas plānu pārrobežu elektroenerģijas plūsmām, ņemot vērā Savienības līmeņa kiberdrošības krīžu pārvaldības plānu un saskaņā ar Regulas (ES) 2019/941 10. pantu izveidoto valsts riskgatavības plānu. Šāds plāns saskan ar Direktīvas (ES) 2022/2555 9. panta 4. punktā paredzēto plānu reaģēšanai uz plašapmēra kiberdrošības incidentiem un krīzēm. Kompetentā iestāde rīkojas saskaņoti ar kritiskas ietekmes un lielas ietekmes vienībām un RKI savā dalībvalstī.

3. Valsts plānu reaģēšanai uz plašapmēra kiberdrošības incidentiem un krīzēm, ko jāizstrādā saskaņā ar Direktīvas (ES) 2022/2555 9. panta 4. punktu, uzskata par šajā pantā paredzēto valsts kiberdrošības krīžu pārvaldības plānu, ja tajā ir iekļauti noteikumi par krīzes pārvaldību un reaģēšanu uz to gadījumos, kad tā ietekmē pārrobežu elektroenerģijas plūsmas.

4. Dalībvalstis var deleģēt šā panta 1. un 2. punktā uzskaitītos uzdevumus arī reģionālajiem koordinācijas centriem saskaņā ar Regulas (ES) 2019/943 37. panta 2. punktu.

5. Kritiskas ietekmes un lielas ietekmes vienības nodrošina, ka to procesi ar kiberdrošību saistītu krīžu pārvaldībai:

a) paredz saderīgas pārrobežu kiberdrošības incidenta risināšanas procedūras, kā definēts Direktīvas (ES) 2022/2555 6. panta 8. punktā, un tās ir oficiāli iekļautas vienību krīzes pārvaldības plānos;

b) ir iekļauti vispārējos krīzes pārvaldības pasākumos.

6. Divpadsmit mēnešu laikā pēc paziņojuma nosūtīšanas kritiskas ietekmes un lielas ietekmes vienībām saskaņā ar šīs regulas 24. panta 6. punktu un turpmāk ik pēc trim gadiem kritiskas ietekmes un lielas ietekmes vienības izstrādā vienības līmeņa krīzes pārvaldības plānu, kas ir paredzēts ar kiberdrošību saistītai krīzei, un iekļauj to savos vispārējos krīzes pārvaldības plānos. Šāds plāns ietver vismaz tālāk minēto:

a) krīzes izziņošanas noteikumus, kas ir izklāstīti Regulas (ES) 2019/941 14. panta 2. un 3. punktā;

b) skaidrus uzdevumus un pienākumus krīzes pārvaldībai, tajā skaitā citu attiecīgu kritiskas ietekmes un lielas ietekmes vienību uzdevumus;

c) atjauninātu kontaktinformāciju, kā arī noteikumus saziņai un informācijas kopīgošanai krīzes situācijā, tajā skaitā savienojumu ar *CSIRT*.

7. Krīzes pārvaldības pasākumus saskaņā ar Direktīvas (ES) 2022/2555 21. panta 2. punkta c) apakšpunktu uzskata par šajā pantā paredzēto vienības līmeņa krīzes pārvaldības plānu elektroenerģijas sektoram, ja tajā ir iekļautas visas šā panta 6. punktā uzskaitītās prasības.

8. Krīzes pārvaldības plānus testē šīs regulas 43., 44. un 45. pantā minētajās kiberdrošības mācībās.

9. Kritiskas ietekmes un lielas ietekmes vienības iekļauj vienības līmeņa krīzes pārvaldības plānus savos darbības nepārtrauktības plānos attiecībā uz kritiskas ietekmes un lielas ietekmes procesiem. Vienības līmeņa krīzes pārvaldības plāni ietver:

a) procesus, kuri ir atkarīgi no IT pakalpojumu pieejamības, integritātes un uzticamības;

b) visu darbības nepārtrauktības objektu izvietojumu, tajā skaitā aparatūras un programmatūras atrašanās vietas;

c) visus ar darbības nepārtrauktības procesus saistītos uzdevumus un pienākumus.

10. Kritiskas ietekmes un lielas ietekmes vienības atjaunina vienības līmeņa krīzes pārvaldības plānus ne retāk kā ik pēc trim gadiem un pēc nepieciešamības.

11. *ACER* atjaunina saskaņā ar šā panta 1. punktu izstrādāto Savienības līmeņa kiberdrošības krīžu pārvaldības un reaģēšanas plānu elektroenerģijas sektoram ne retāk kā ik pēc trim gadiem un pēc nepieciešamības.

12. Katra kompetentā iestāde atjaunina saskaņā ar šā panta 2. punktu izstrādāto valsts kiberdrošības krīžu pārvaldības un reaģēšanas plānu pārrobežu elektroenerģijas plūsmām ne retāk kā ik pēc trim gadiem un pēc nepieciešamības.

13. Kritiskas ietekmes un lielas ietekmes vienības savus darbības nepārtrauktības plānus testē ne retāk kā ik pēc trim gadiem vai pēc būtisku izmaiņu ieviešanas kritiskas ietekmes procesā. Darbības nepārtrauktības plāna testu rezultātus dokumentē. Kritiskas ietekmes un lielas ietekmes vienības var iekļaut darbības nepārtrauktības plānu kiberdrošības mācībās.

14. Kritiskas ietekmes un lielas ietekmes vienības atjaunina darbības nepārtrauktības plānu pēc nepieciešamības, bet ne retāk kā ik pēc trim gadiem, ņemot vērā testa rezultātus.

15. Ja testā konstatē nepilnības darbības nepārtrauktības plānā, kritiskas ietekmes un lielas ietekmes vienība novērš nepilnības 180 kalendāra dienu laikā pēc testa un veic jaunu testu, lai iegūtu pierādījumus, ka korektīvie pasākumi ir bijuši rezultatīvi.

16. Ja kritiskas ietekmes vai lielas ietekmes vienība nespēj novērst nepilnības 180 kalendāra dienu laikā, tā norāda iemeslus ziņojumā, ko jāiesniedz kompetentajai iestādei saskaņā ar šīs regulas 27. pantu.

*42. pants*

**Kiberdrošības agrīnā brīdinājuma spējas elektroenerģijas sektoram**

1. Kompetentās iestādes sadarbojas ar *ENISA*, lai veidotu Elektroenerģijas kiberdrošības agrīnās brīdināšanas spējas (*ECEAC*), kas ietilpst palīdzībā dalībvalstīm, ko sniedz saskaņā ar Regulas (ES) 2019/881 6. panta 2. un 7. punktu.

2. *ECEAC* ļauj *ENISA*, īstenojot Regulas (ES) 2019/881 7. panta 7. punktā uzskaitītos uzdevumus, veikt tālāk minēto:

a) vākt informāciju, ko brīvprātīgi iesniedz:

   i) *CSIRT*, kompetentās iestādes;

   ii) šīs regulas 2. pantā uzskaitītās vienības;

   iii) citas vienības, kuras vēlas brīvprātīgi iesniegt attiecīgu informāciju;

b) novērtēt un klasificēt saņemto informāciju;

c) novērtēt informāciju, kurai var piekļūt *ENISA*, lai noskaidrotu kiberrisku nosacījumus un attiecīgos rādītājus attiecībā uz pārrobežu elektroenerģijas plūsmu aspektiem;

d) noteikt apstākļus un rādītājus, kas bieži ir saistīti ar kiberuzbrukumiem elektroenerģijas sektoram;

e) īstenojot novērtējumu un konstatējot riska faktorus, noteikt, vai ir jāveic tālāka analīze un preventīvi pasākumi;

f) informēt kompetentās iestādes par konstatētajiem riskiem un attiecīgajām vienībām ieteiktajiem preventīvajiem pasākumiem;

g) informēt visas attiecīgās vienības, kas ir uzskaitītas šīs regulas 2. pantā, par rezultātiem, ko ieguva, vērtējot informāciju saskaņā ar šā panta b), c) un d) apakšpunktu;

h) periodiski iekļaut attiecīgo informāciju situācijas apzināšanās ziņojumā, ko sagatavo saskaņā ar Regulas (ES) 2019/881 7. panta 6. punktu;

i) ja iespējams, pamatojoties uz saņemto informāciju, izdarīt secinājumus par piemērojamajiem datiem, kuri liecina par iespējamu drošības pārkāpumu vai kiberuzbrukumu ("aizskāruma rādītāji").

3. Pildot Direktīvas (ES) 2022/2555 11. panta 3. punkta b) apakšpunktā noteiktos uzdevumus, *CSIRT* no *ENISA* saņemto informāciju nekavējoties izplata attiecīgajām vienībām.

4. *ACER* pārrauga *ECEAC* lietderību. *ENISA* palīdz *ACER*, sniedzot visu nepieciešamo informāciju saskaņā ar Regulas (ES) 2019/881 6. panta 2. punktu un 7. panta 1. punktu. Šādas uzraudzības darbības analīze ietilpst pārraudzībā saskaņā ar šīs regulas 12. pantu.

VI NODAĻA

**ELEKTROENERĢIJAS KIBERDROŠĪBAS MĀCĪBU SATVARS**

*43. pants*

**Kiberdrošības mācības vienību un dalībvalstu līmenī**

1. Līdz 31. decembrim nākamajā gadā pēc tā gada, kurā nosūtīja paziņojumu kritiskas ietekmes vienībām, un turpmāk ik pēc trim gadiem katra kritiskas ietekmes vienība rīko kiberdrošības mācības, kurās viens vai vairāki scenāriji paredz kiberuzbrukumus, kas tieši vai netieši ietekmē pārrobežu elektroenerģijas plūsmas un ir saistīti ar riskiem, ko konstatēja dalībvalsts un vienības līmeņa kiberdrošības risku novērtējumos saskaņā ar šīs regulas attiecīgi 20. un 27. pantu.

2. Atkāpjoties no šā panta 1. punkta, RKI pēc apspriešanās ar kompetento iestādi un attiecīgo kiberkrīžu pārvaldības iestādi, ko izraudzīja vai izveidoja saskaņā ar Direktīvas (ES) 2022/2555 9. pantu, var nolemt organizēt šā panta 1. punktā aprakstītās mācības dalībvalsts līmenī, nevis rīkot kiberdrošības mācības vienības līmenī. Šajā sakarā kompetentā iestāde informē:

a) visas kritiskas ietekmes vienības dalībvalstī, VRI, *CSIRT* un KKI ne vēlāk kā līdz 30. jūnijam iepriekšējā gadā pirms vienības līmeņa kiberdrošības mācībām;

b) katru vienību, kura piedalīsies dalībvalsts līmeņa kiberdrošības mācībās, ne vēlāk kā sešus mēnešus pirms mācību plānotā sākuma.

3. RKI ar *CSIRT* sniegto tehnisko atbalstu organizē šā panta 2. punktā aprakstītās kiberdrošības mācības dalībvalsts līmenī atsevišķi vai kopā ar citām kiberdrošības mācībām attiecīgajā dalībvalstī. Lai minētās mācības varētu sarīkot kopā, RKI var atlikt šā panta 1. punktā minētās kiberdrošības mācības dalībvalsts līmenī uz vienu gadu.

4. Vienības līmeņa un dalībvalsts līmeņa kiberdrošības mācībām jāsaskan ar valsts kiberdrošības krīžu pārvaldības satvariem, ko nosaka Direktīvas (ES) 2022/2555 9. panta 4. punkta d) apakšpunkts.

5. Līdz 2026. gada 31. decembrī un turpmāk ik pēc trim gadiem *ENTSO-E* sadarbībā ar ES SSO struktūru dara pieejamu mācību scenārija veidni šā panta 1. punktā minēto kiberdrošības mācību rīkošanai vienības un dalībvalsts līmenī. Veidni sagatavo, ņemot vērā jaunāko kiberdrošības risku novērtējumu vienības un dalībvalsts līmenī, un tajā iekļauj galvenos sekmīguma kritērijus. *ENTSO-E* un ES SSO struktūra iesaista veidnes izstrādāšanā *ACER* un *ENISA*.

*44. pants*

**Reģionālās vai starpreģionālās kiberdrošības mācības**

1. Līdz 2029. gada 31. decembrī un turpmāk ik pēc trim gadiem *ENTSO-E* sadarbībā ar ES SSO struktūru katrā sistēmas darbības reģionā organizē reģionālās kiberdrošības mācības. Reģionālajās kiberdrošības mācībās piedalās kritiskas ietekmes vienības no attiecīgā sistēmas darbības reģiona. *ENTSO-E* sadarbībā ar ES SSO struktūru var reģionālo kiberdrošības mācību vietā organizēt starpreģionālas kiberdrošības mācības, kas tajā pašā laikposmā notiek vairākos sistēmas darbības reģionos. Mācībās ņem vērā citus esošos kiberdrošības risku novērtējumus un Savienības līmenī izstrādātos scenārijus.

2. *ENISA* sniedz atbalstu *ENTSO-E* un ES SSO struktūrai reģionālo vai starpreģionālo kiberdrošības mācību sagatavošanā un organizēšanā.

3. *ENTSO-E* sadarbībā ar ES SSO struktūru informē kritiskas ietekmes vienības, kas piedalīsies reģionālās vai starpreģionālās kiberdrošības mācībās, sešus mēnešus pirms mācību plānotā sākuma.

4. Organizators, kurš rīko regulārās kiberdrošības mācības Savienības līmenī saskaņā ar Regulas (ES) 2019/881 7. panta 5. punktu vai citas obligātas kiberdrošības mācības, kas ir saistītas ar elektroenerģijas sektoru tajā pašā ģeogrāfiskajā perimetrā, var uzaicināt piedalīties *ENTSO-E* un ES SSO struktūru. Tādos gadījumos šā panta 1. punktā noteiktais pienākums nav spēkā, ja vien visas konkrētā sistēmas darbības reģiona kritiskas ietekmes vienības piedalās tajā pašās mācībās.

5. Ja *ENTSO-E* un ES SSO struktūra piedalās šā panta 4. punktā minētajās kiberdrošības mācībās, tie var par vienu gadu atlikt šā panta 1. punktā minētās reģionālās vai starpreģionālās kiberdrošības mācības.

6. Līdz 2027. gada 31. decembrī un turpmāk ik pēc trim gadiem *ENTSO-E*, rīkojoties saskaņoti ar ES SSO struktūru, dara pieejamu mācību scenārija veidni reģionālo un starpreģionālo kiberdrošības mācību rīkošanai. Veidni sagatavo, ņemot vērā jaunākā kiberdrošības risku novērtējuma rezultātus reģionālā līmenī, un tajā iekļauj galvenos sekmīguma kritērijus. *ENTSO-E* apspriežas ar Komisiju un var lūgt *ACER*, *ENISA* un Kopīgajam pētniecības centram padomu par reģionālo un starpreģionālo kiberdrošības mācību organizēšanu un īstenošanu.

*45. pants*

**Vienības un dalībvalsts līmeņa un reģionālo un starpreģionālo kiberdrošības mācību rezultāti**

1. Šīs regulas 43. panta 1. un 2. punktā un 44. panta 1. punktā minētajās kiberdrošības mācībās pēc kritiskas ietekmes vienības pieprasījuma piedalās kritisko pakalpojumu sniedzēji, kas sniedz kritiskas ietekmes vienībai pakalpojumus jomā, kura atbilst attiecīgo kiberdrošības mācību tvērumam.

2. Šīs regulas 43. panta 1. un 2. punktā un 44. panta 1. punktā minēto kiberdrošības mācību organizatori, kuriem pēc pieprasījuma sniedz padomus *ENISA*, saskaņā ar Regulas (ES) 2019/881 7. panta 5. punktu analizē un apkopo attiecīgo kiberdrošības mācību rezultātus, sagatavojot visiem dalībniekiem adresētu kopsavilkuma ziņojumu, kurā norāda gūtās atziņas. Ziņojumā iekļauj šādu informāciju:

a) mācību scenāriji, sanāksmju protokoli, pamatnostājas, panākumi un atziņas, ko guva elektroenerģijas vērtības ķēdes jebkurā līmenī;

b) vai tika izpildīti galvenie sekmīguma kritēriji;

c) saraksts, kurā uzskaitīti ieteikumi vienībām, kuras piedalījās attiecīgajās kiberdrošības mācībās, par to, kā labot, pielāgot vai mainīt kiberdrošības krīzes procesus, procedūras, saistītos pārvaldības modeļus un esošās līgumattiecības ar kritisko pakalpojumu sniedzējiem.

3. Pēc *CSIRT* tīkla, TID sadarbības grupas vai *EU-CyCLONe* pieprasījuma šīs regulas 43. panta 1. un 2. punktā un 44. panta 1. punktā minēto kiberdrošības mācību organizatori informē tos par attiecīgo kiberdrošības mācību rezultātiem. Organizatori sniedz katrai no vienībām, kuras piedalījās mācībās, šā panta 2. punkta a) un b) apakšpunktā minēto informāciju. Šā minētā punkta c) apakšpunktā minēto ieteikumu sarakstu organizatori nodod vienīgi tām vienībām, kurām šie ieteikumi ir adresēti.

4. Šīs regulas 43. panta 1. un 2. punktā un 44. panta 1. punktā minēto kiberdrošības mācību organizatori regulāri seko līdzi tam, kā vienības, kuras piedalījās mācībās, īsteno ieteikumus saskaņā ar šā panta 2. punkta c) apakšpunktu.

VII NODAĻA

**INFORMĀCIJAS AIZSARDZĪBA**

*46. pants*

**Nodotās informācijas aizsardzības principi**

1. Šīs regulas 2. panta 1. punktā uzskaitītās vienības nodrošina, ka saskaņā ar šo regulu sniegtajai, saņemtajai, nodotajai vai pārsūtītajai informācijai var piekļūt, vienīgi pamatojoties uz principu "nepieciešamība zināt" un saskaņā ar attiecīgajiem Savienības un valsts tiesību aktiem par informācijas drošību.

2. Šīs regulas 2. panta 1. punktā uzskaitītās vienības nodrošina, ka ar informāciju, ko sniedz, saņem, nodod vai pārsūta saskaņā ar šo regulu, rīkojas un izseko tai visā šādas informācijas aprites ciklā, un aprites cikla beigās to drīkst darīt publiski pieejamu vienīgi anonimizētā veidā.

3. Šīs regulas 2. panta 1. punktā uzskaitītās vienības nodrošina visu nepieciešamo organizatorisko un tehnisko aizsardzības pasākumu ieviešanu, lai garantētu un aizsargātu saskaņā ar šo regulu sniegtās, saņemtās, nodotās vai pārsūtītās informācijas konfidencialitāti, integritāti, pieejamību un nenoliedzamību neatkarīgi no līdzekļiem, kādus izmantoja minētajos procesos. Aizsardzības pasākumi:

a) ir samērīgi;

b) ņem vērā kiberdrošības riskus, kuri ir saistīti ar jau zināmiem un jauniem apdraudējumiem, kam šāda informācija var tikt pakļauta šīs regulas kontekstā;

c) iespēju robežās pamatojas uz valsts, Eiropas vai starptautiskiem standartiem un paraugpraksi;

d) tiek dokumentēti.

4. Šīs regulas 2. panta 1. punktā uzskaitītās vienības nodrošina, ka ikvienu fizisku personu, kurai ir piešķirta piekļuve saskaņā ar šo regulu sniegtajai, saņemtajai, nodotajai vai pārsūtītajai informācijai, instruē par vienības līmenī piemērojamajiem drošības noteikumiem un par pasākumiem un procedūrām, kuras attiecas uz informācijas aizsardzību. Minētās vienības nodrošina, ka attiecīgā fiziskā persona apstiprina, ka tās pienākums ir aizsargāt informāciju saskaņā ar norādījumiem, ko tā saņēma instruktāžas laikā.

5. Šīs regulas 2. panta 1. punktā uzskaitītās vienības nodrošina, ka piekļuvi informācijai, ko sniedz, saņem, nodod vai pārsūta saskaņā ar šo regulu, piešķir vienīgi tādām fiziskām personām:

a) kuras ir pilnvarotas piekļūt šādai informācijai, pamatojoties uz to darba pienākumiem un tikai tādā apmērā, kāds ir nepieciešams tām uzdoto uzdevumu izpildei;

b) kuru ētikas un godprātības principus vienība varēja novērtēt un par kuru iepriekšējās darbības pārbaudē fiziskās personas uzticamības izvērtēšanai saskaņā ar paraugpraksi un vienības standarta drošības prasībām, un, ja nepieciešams, arī saskaņā ar valsts tiesību aktiem neguva pierādījumus, kuru dēļ pārbaudes iznākums būtu nelabvēlīgs.

6. Šīs regulas 2. panta 1. punktā uzskaitītās vienības saņem rakstveida piekrišanu no fiziskās vai juridiskās personas, kura sākotnēji radīja vai iesniedza konkrēto informāciju, pirms nodot šādu informāciju trešai personai, kura neietilpst šīs regulas darbības jomā.

7. Šīs regulas 2. panta 1. punktā uzskaitīta vienība var uzskatīt, kā šādu informāciju drīkst nodot citiem, neievērojot šā panta 1. un 4. punktā minētās prasības, ja to dara, lai novērstu vienlaicīgu elektroenerģētisko krīzi, kuras pamatcēlonis ir kiberdrošība, vai pārrobežu krīzi Savienībā citā sektorā. Tādā gadījumā vienība:

a) apspriežas ar kompetento iestādi un saņem no tās atļauju nodot šādu informāciju;

b) anonimizē šādu informāciju, saglabājot elementus, kas ir nepieciešami, lai informētu sabiedrību par nenovēršamu un nopietnu risku, kas apdraud pārrobežu elektroenerģijas plūsmas, un par iespējamiem ietekmes mazināšanas pasākumiem;

c) aizsargā informācijas oriģinatora, kā arī to vienību identitāti, kuras apstrādā šādu informāciju saskaņā ar šo regulu.

8. Atkāpjoties no šā panta 6. punkta, kompetentās iestādes var nodot saskaņā ar šo regulu sniegto, saņemto, nodoto vai pārsūtīto informāciju trešai personai, kas nav uzskaitīta šīs regulas 2. panta 1. punktā, nesaņemot iepriekšēju rakstveida piekrišanu no informācijas oriģinatora, taču tām ir pēc iespējas ātrāk jāinformē par to oriģinators. Pirms izpaust trešai personai, kas nav uzskaitīta šīs regulas 2. panta 1. punktā, saskaņā ar šo regulu sniegto, saņemto, nodoto vai pārsūtīto informāciju, attiecīgā kompetentā iestāde saprātīgā mērā nodrošina, ka attiecīgā trešā persona ir informēta par spēkā esošajiem drošības noteikumiem, un gūst pietiekamu pārliecību par to, ka attiecīgā trešā persona spēj aizsargāt saņemto informāciju, ievērojot šā panta 1.–5. punktu. Lai aizsargātu informācijas oriģinatora identitāti, kompetentā iestāde anonimizē šādu informāciju, saglabājot elementus, kas ir nepieciešami, lai informētu sabiedrību par nenovēršamu un nopietnu risku, kas apdraud pārrobežu elektroenerģijas plūsmas, un par iespējamiem ietekmes mazināšanas pasākumiem. Tādā gadījumā trešā persona, kas nav uzskaitīta šīs regulas 2. panta 1. punktā, aizsargā saņemto informāciju saskaņā ar jau spēkā esošajiem vienības līmeņa noteikumiem vai, ja tas nav iespējams, saskaņā ar attiecīgās kompetentās iestādes noteiktajiem noteikumiem un norādījumiem.

9. Šis pants neattiecas uz vienībām, kuras nav uzskaitītas šīs regulas 2. panta 1. punktā un kurām nodod informāciju saskaņā ar šā panta 6. punktu. Tādā gadījumā piemēro šā panta 7. punktu, vai arī kompetentā iestāde var izsniegt šādai vienībai rakstveida noteikumus, kuri jāpiemēro, ja tā saņem informāciju saskaņā ar šo regulu.

*47. pants*

**Informācijas konfidencialitāte**

1. Uz informāciju, ko sniedz, saņem, nodod vai pārsūta saskaņā ar šo regulu, attiecas šā panta 2.–5. punktā noteiktie nosacījumi par dienesta noslēpuma glabāšanu un Regulas (ES) 2019/943 65. pantā noteiktās prasības. Informāciju, ko šīs regulas 2. pantā uzskaitītās vienības sniedz, saņem, nodod vai pārsūta savā starpā šīs regulas īstenošanas nolūkā, aizsargā, ņemot vērā konfidencialitātes līmeni, kādu attiecīgajai informācijai ir piemērojis oriģinators.

2. Uz šīs regulas 2. pantā uzskaitītajām vienībām attiecas pienākums glabāt dienesta noslēpumu.

3. KKI, VRI, RKI un *CSIRT* apmainās ar visu informāciju, kas tām ir nepieciešama savu uzdevumu pildīšanai.

4. Informāciju, ko šīs regulas 2. panta 1. punktā uzskaitītās vienības saņem, nodod vai pārsūta savā starpā nolūkā īstenot šīs regulas 23. pantu, anonimizē un apkopo.

5. Informāciju, ko vienība vai iestāde, uz ko attiecas šī regula, ir saņēmusi savu pienākumu pildīšanas gaitā, nedrīkst izpaust nevienai citai vienībai vai iestādei, neskarot gadījumus, uz kuriem attiecas valstu tiesību akti, pārējie šīs regulas noteikumi vai citi attiecīgi Savienības tiesību akti.

6. Neskarot valsts vai Savienības tiesību aktus, iestāde, vienība vai fiziska persona, kas saņēma informāciju saskaņā ar šo regulu, drīkst izmantot šādu informāciju vienīgi šajā regulā tai noteikto pienākumu pildīšanai, nevis kādiem citiem nolūkiem.

7. *ACER* pēc apspriešanās ar *ENISA*, visām kompetentajām iestādēm, *ENTSO-E* un ES SSO struktūru līdz 2025. gada 13. jūnijā izdod vadlīnijas visām šīs regulas 2. panta 1. punktā uzskaitītajām vienībām par informācijas apmaiņas mehānismiem un jo īpaši par paredzētajām saziņas plūsmām un metodēm informācijas anonimizācijai un apkopošanai šā panta īstenošanas nolūkā.

8. Ja informācija ir konfidenciāla saskaņā ar Savienības un valsts noteikumiem, to nodod Komisijai un citām attiecīgajām iestādēm vienīgi tad, ja šāda informācijas apmaiņa ir nepieciešama šīs regulas piemērošanai. Apmainās tikai ar to informāciju, kas ir nepieciešama un samērīga šādas apmaiņas nolūkam. Informācijas apmaiņā ievēro minētās informācijas konfidencialitāti un aizsargā kritiskas ietekmes vai lielas ietekmes vienību drošību un komerciālās intereses.

VIII NODAĻA

**NOBEIGUMA NOTEIKUMI**

*48. pants*

**Pārejas perioda noteikumi**

1. Kamēr šīs regulas 6. panta 2. punktā minētie noteikumi vai metodikas vai šīs regulas 6. panta 3. punktā minētie plāni vēl nav apstiprināti, *ENTSO-E* sadarbībā ar ES SSO struktūru izstrādā nesaistošas norādes par šādiem jautājumiem:

a) elektroenerģijas kiberdrošības ietekmes indeksa ("*ECII*") pagaidu versija saskaņā ar šā panta 2. punktu;

b) Savienības mēroga lielas ietekmes un kritiskas ietekmes procesu pagaidu saraksts saskaņā ar šā panta 4. punktu; un

c) pagaidu saraksts, kurā uzskaita Eiropas un starptautiskos standartus un kontroles pasākumus, ko jāievēro saskaņā ar valsts tiesību aktiem, kuri attiecas uz pārrobežu elektroenerģijas plūsmu kiberdrošības aspektiem, saskaņā ar šā panta 6. punktu.

2. Līdz 2024. gada 13. oktobrī *ENTSO-E* sadarbībā ar ES SSO struktūru izstrādā ieteikumu par pagaidu *ECII*. *ENTSO-E* sadarbībā ar ES SSO struktūru paziņo ieteikto pagaidu *ECII* kompetentajām iestādēm.

3. Četru mēnešu laikā pēc ieteiktā pagaidu *ECII* saņemšanas, bet ne vēlāk kā līdz 2025. gada 13. februārī kompetentās iestādes, pamatojoties uz ieteikto *ECII*, identificē savā dalībvalstī kandidātes uz lielas ietekmes un kritiskas ietekmes vienības statusu un sagatavo lielas ietekmes un kritiskas ietekmes vienību pagaidu sarakstu. Pagaidu sarakstā norādītās lielas ietekmes un kritiskas ietekmes vienības var brīvprātīgā kārtā pildīt pienākumus, kuri tām ir noteikti šajā regulā, pamatojoties uz piesardzības principu. Līdz 2025. gada 13. martā kompetentās iestādes paziņo pagaidu sarakstā norādītajām vienībām, ka tās ir tikušas identificētas kā lielas ietekmes vai kritiskas ietekmes vienības.

4. Līdz 2024. gada 13. decembrī *ENTSO-E* sadarbībā ar ES SSO struktūru izstrādā Savienības mēroga lielas ietekmes un kritiskas ietekmes procesu pagaidu sarakstu. Vienības, kuras saņēmušas paziņojumu saskaņā ar šā panta 3. punktu un brīvprātīgi nolēma pildīt pienākumus, kuri tām ir noteikti šajā regulā, pamatojoties uz piesardzības principu, izmanto lielas ietekmes un kritiskas ietekmes procesu pagaidu sarakstu, lai noteiktu lielas ietekmes un kritiskas ietekmes pagaidu perimetru un aktīvus, kuri jāiekļauj pirmajā vienības līmeņa kiberdrošības risku novērtējumā.

5. Līdz 2024. gada 13. septembrī katra kompetentā iestāde saskaņā ar šīs regulas 4. panta 1. punktu iesniedz *ENTSO-E* un ES SSO struktūrai sarakstu, kurā uzskaita valsts tiesību aktus, kuri attiecas uz pārrobežu elektroenerģijas plūsmu kiberdrošības aspektiem.

6. Ņemot vērā kompetento iestāžu iesniegto informāciju, *ENTSO-E* sadarbībā ar ES SSO struktūru līdz 2025. gada 13. jūnijā sagatavo pagaidu sarakstu, kurā uzskaita Eiropas un starptautiskos standartus un kontroles pasākumus, ko jāievēro saskaņā ar valsts tiesību aktiem, kuri attiecas uz pārrobežu elektroenerģijas plūsmu kiberdrošības aspektiem.

7. Eiropas un starptautisko standartu un kontroles pasākumu pagaidu sarakstā iekļauj:

a) Eiropas un starptautiskos standartus un valsts tiesību aktus, kuri sniedz norādes par vienības līmeņa kiberdrošības risku pārvaldības metodikām; un

b) kiberdrošības kontroles pasākumus, kas ir līdzvērtīgi tiem kontroles pasākumiem, kurus ir paredzēts iekļaut minimālajos un pastiprinātajos kiberdrošības kontroles pasākumos.

8. Gatavojot standartu pagaidu saraksta galīgo versiju, *ENTSO-E* un ES SSO struktūra ņem vērā *ENISA* un *ACER* iesniegtos viedokļus. *ENTSO-E* un ES SSO struktūra publicē Eiropas un starptautisko standartu un kontroles pasākumu pagaidu sarakstu savās tīmekļa vietnēs.

9. Saskaņā ar šā panta 1. punktu izstrādāto nesaistošo norāžu priekšlikumus *ENTSO-E* un ES SSO struktūra apspriež ar *ENISA* un *ACER*.

10. Kamēr minimālie un pastiprinātie kiberdrošības kontroles pasākumi vēl nav izstrādāti saskaņā ar šīs regulas 29. pantu un pieņemti saskaņā ar šīs regulas 8. pantu, šīs regulas 2. panta 1. punktā uzskaitītās vienības cenšas aizvien plašāk piemērot saskaņā ar šā panta 1. punktu izstrādātās nesaistošās norādes.

*49. pants*

**Stāšanās spēkā**

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī.*

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2024. gada 11. martā

*Komisijas vārdā –*
*priekšsēdētāja*
Ursula VON DER LEYEN