Europos Sąjungos
oficialusis leidinys

LT
L serija

2024/1366

2024 5 24

KOMISIJOS DELEGUOTASIS REGLAMENTAS (ES) 2024/1366

2024 m. kovo 11 d.

kuriuo Europos Parlamento ir Tarybos reglamentas (ES) 2019/943 papildomas nustatant tinklo kodeksą dėl tarpvalstybinių elektros energijos srautų kibernetinio saugumo aspektų sektorinių taisyklių

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2019 m. birželio 5 d. Europos Parlamento ir Tarybos reglamentą (ES) 2019/943 dėl elektros energijos vidaus rinkos ([1]), ypač į jo 59 straipsnio 2 dalies e punktą,

kadangi:

(1) kibernetinio saugumo rizikos vertinimas yra itin svarbus elektros energijos tiekimo saugumui išlaikyti ir aukštam kibernetinio saugumo lygiui elektros energijos sektoriuje užtikrinti;

(2) skaitmenizacijai ir kibernetiniam saugumui tenka lemiamas vaidmuo teikiant esmines paslaugas ir todėl jie turi strateginę reikšmę ypatingos svarbos energetikos infrastruktūrai;

(3) Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 ([2]) nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti. Europos Parlamento ir Tarybos reglamentu (ES) 2019/941 ([3]) papildoma Direktyva (ES) 2022/2555 užtikrinant, kad kibernetinio saugumo incidentai elektros energijos sektoriuje būtų tinkamai pripažįstami kaip rizikos veiksnys ir kad priemonės jiems neutralizuoti būtų tinkamai integruotos į pasirengimo valdyti riziką planus. Reglamentu (ES) 2019/943 papildoma Direktyva (ES) 2022/2555 ir Reglamentas (ES) 2019/941, Sąjungos lygmeniu nustatant specialias taisykles elektros energijos sektoriui. Be to, šiuo deleguotuoju reglamentu papildomos su tarpvalstybiniais elektros energijos srautais susijusios Direktyvos (ES) 2022/2555 nuostatos dėl elektros energijos sektoriaus;

(4) skaitmenizuotos elektros energijos sistemos yra tarpusavyje susijusios, todėl elektros energijos sistemų krizių, susijusių su kibernetiniais išpuoliais, prevencija ir valdymas negali būti laikomi vien nacionaliniu uždaviniu. Išnaudojant visas regioninio ir Sąjungos bendradarbiavimo galimybes ir remiantis šiuo bendradarbiavimu, turėtų būti parengtos efektyvesnės ir mažiau išlaidų reikalaujančios priemonės. Todėl reikia bendros taisyklių ir geriau koordinuotų procedūrų sistemos, kuria būtų galima užtikrinti, kad valstybės narės ir kiti subjektai galėtų veiksmingai bendradarbiauti tarpvalstybiniu mastu, vadovaudamiesi didesnio skaidrumo, pasitikėjimo ir valstybių narių bei už elektros energijos sistemą ir kibernetinį saugumą atsakingų kompetentingų institucijų solidarumo principais;

(5) siekiant pagal šį reglamentą valdyti kibernetinio saugumo riziką, reikia struktūrinio proceso, kuris apimtų, be kita ko, kibernetinių išpuolių rizikos tarpvalstybiniams elektros energijos srautams nustatymą, atitinkamus veiklos procesus ir perimetrus, atitinkamas kibernetinio saugumo kontrolės priemones ir tikrinimo mechanizmus. Nors viso proceso tvarkaraštis apima kelerius metus, kiekvienas jo etapas turėtų padėti pasiekti aukštą bendrą kibernetinio saugumo lygį šiame sektoriuje ir sumažinti kibernetinio saugumo riziką. Visi proceso dalyviai turėtų kuo labiau stengtis nepagrįstai nedelsdami kuo greičiau ir bet kuriuo atveju ne vėliau kaip iki šiame reglamente nustatytų terminų parengti metodikas ir dėl jų susitarti;

([1]) OL L 158, 2019 6 14, p. 54.

([2]) 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva) (OL L 333, 2022 12 27, p. 80).

([3]) 2019 m. birželio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/941 dėl pasirengimo valdyti riziką elektros energijos sektoriuje, kuriuo panaikinama Direktyva 2005/89/EB (OL L 158, 2019 6 14, p. 1).

(6) kibernetinio saugumo rizikos vertinimai Sąjungos, valstybių narių, regionų ir subjektų lygmeniu šiame reglamente gali apimti tik kibernetinių išpuolių, apibrėžtų Europos Parlamento ir Tarybos reglamente (ES) 2022/2554 ([4]), rizikos veiksnius, todėl gali neapimti, pavyzdžiui, fizinių išpuolių, gaivalinių nelaimių ir atjungimų dėl infrastruktūros objektų ar žmogiškųjų išteklių praradimo. Sąjungos masto ir regioninė rizika, susijusi su fiziniais išpuoliais ar gaivalinėmis nelaimėmis elektros energijos srityje, jau reglamentuojama kitais galiojančiais Sąjungos teisės aktais, įskaitant Reglamento (ES) 2019/941 5 straipsnį arba Komisijos reglamentą (ES) 2017/1485 ([5]), kuriuo nustatomos elektros energijos perdavimo sistemos eksploatavimo gairės. Panašiai, Europos Parlamento ir Tarybos direktyva (ES) 2022/2557 ([6]) dėl ypatingos svarbos subjektų atsparumo siekiama sumažinti pažeidžiamumą ir sustiprinti fizinį ypatingos svarbos subjektų atsparumą ir reglamentuojami visi atitinkami dėl gamtos ir žmogaus kylančios rizikos veiksniai, galintys paveikti esmines paslaugas, įskaitant avarijas, gaivalines nelaimes, ekstremaliąsias visuomenės sveikatos situacijas, pvz., pandemijas, ir hibridines grėsmes ar kitas priešiškas grėsmes, įskaitant teroristinius išpuolius, nusikalstamą infiltraciją ir sabotažą;

(7) sąvoka „didelio poveikio ir ypatingos svarbos poveikio subjektai“ šiame reglamente būtina siekiant apibrėžti subjektų, kuriems bus taikomos šiame reglamente apibūdintos pareigos, grupę. Įvairiose nuostatose išdėstytu rizika grindžiamu požiūriu siekiama nustatyti procesus, pagalbinį turtą ir jį eksploatuojančius subjektus, turinčius poveikį tarpvalstybiniams elektros energijos srautams. Priklausomai nuo galimų kibernetinių išpuolių poveikio jų administruojamiems tarpvalstybiniams elektros energijos srautams laipsnio, jie gali būti laikomi didelio poveikio arba ypatingos svarbos poveikio subjektais. Direktyvos (ES) 2022/2555 3 straipsnyje nustatytos esminių ir svarbių subjektų sąvokos ir subjektų priskyrimo prie tų kategorijų kriterijai. Nors daugelis minėtų subjektų bus tuo pačiu metu laikomi esminiais subjektais pagal Direktyvos (ES) 2022/2555 3 straipsnį ir didelio poveikio arba ypatingos svarbos poveikio subjektais pagal šio reglamento 24 straipsnį ir bus atitinkamai identifikuoti, šiame reglamente nustatyti kriterijai taikomi tik jų vaidmeniui ir poveikiui elektros energijos sistemos procesuose, veikiančiuose tarpvalstybinius srautus, visai neatsižvelgiant į Direktyvos (ES) 2022/2555 3 straipsnyje nustatytus kriterijus;

(8) į šio reglamento taikymo sritį patenkantys subjektai, pagal šio reglamento 24 straipsnį laikomi didelio poveikio arba ypatingos svarbos poveikio subjektais, kuriems taikomos reglamente nustatytos pareigos, visų pirma yra tie, kurie turi tiesioginį poveikį tarpvalstybiniams elektros energijos srautams Europos Sąjungoje;

(9) siekiant užtikrinti efektyvumą ir išvengti dubliavimosi įgyvendinant tikslus, šiame reglamente naudojamasi galiojančiais mechanizmais ir priemonėmis, jau nustatytais kituose teisės aktuose;

(10) taikydamos šį reglamentą valstybės narės, atitinkamos valdžios institucijos ir sistemos operatoriai turėtų atsižvelgti į sutartus Europos standartus ir Europos standartizacijos organizacijos technines specifikacijas bei laikytis Sąjungos teisės aktų, susijusių su gaminių, kuriems taikomi tie Sąjungos teisės aktai, teikimu rinkai ar eksploatacijos pradžia;

([4]) 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011 (OL L 333, 2022 12 27, p. 1).

([5]) 2017 m. rugpjūčio 2 d. Komisijos reglamentas (ES) 2017/1485, kuriuo nustatomos elektros energijos perdavimo sistemos eksploatavimo gairės (OL L 220, 2017 8 25, p. 1).

([6]) Europos Parlamento ir Tarybos direktyva (ES) 2022/2557 2022 m. gruodžio 14 d. dėl ypatingos svarbos subjektų atsparumo, kuria panaikinama Tarybos direktyva 2008/114/EB (OL L 333, 2022 12 27, p. 164).

(11) siekiant sušvelninti kibernetinio saugumo riziką, reikia parengti išsamų taisyklių sąvadą, kuriame būtų reglamentuojami atitinkamų suinteresuotųjų subjektų, kurių veikla susijusi su tarpvalstybinių elektros energijos srautų kibernetinio saugumo aspektais, veiksmai ir jų tarpusavio bendradarbiavimas, kad būtų užtikrintas sistemos saugumas. Tomis organizacinėmis ir techninėmis taisyklėmis turėtų būti užtikrinama, kad dauguma elektros energijos sistemos incidentų, kurių pagrindinės priežastys susijusios su kibernetiniu saugumu, būtų veiksmingai neutralizuojami eksploatavimo lygmeniu. Reikia išdėstyti, ką tie atitinkami suinteresuotieji subjektai turėtų daryti, kad užkirstų kelią tokioms krizėms, ir kokių priemonių jie gali imtis, jeigu vien sistemos eksploatacijos taisyklių nebeužtenka. Todėl reikia sukurti bendrą taisyklių sistemą, kaip užkirsti kelią vienalaikėms elektros energijos sektoriaus krizėms, kurių pagrindinė priežastis susijusi su kibernetiniu saugumu, kaip joms pasirengti ir kaip jas valdyti. Taip užtikrinamas didesnis skaidrumas pasirengimo etapu ir vienalaikės elektros energijos sektoriaus krizės metu ir užtikrinama, kad priemonių būtų imamasi koordinuotai ir veiksmingai kartu su už kibernetinį saugumą atsakingomis valstybių narių kompetentingomis institucijomis. Valstybės narės ir atitinkami subjektai turėtų būti įpareigojami solidariai bendradarbiauti regioniniu lygmeniu ir, kai taikytina, dvišaliu pagrindu. Šiuo bendradarbiavimu ir taisyklėmis ketinama pasiekti geresnį pasirengimą mažesnėmis sąnaudomis valdyti kibernetinio saugumo riziką, kaip numatyta ir pagal Direktyvos (ES) 2022/2555 tikslus. Be to, reikia sustiprinti vidaus elektros energijos rinką didinant pasitikėjimą ir užtikrintumą visose valstybėse narėse, visų pirma sumažinant riziką, kad bus nepagrįstai apriboti tarpvalstybiniai elektros energijos srautai, ir taip sumažinant neigiamo šalutinio poveikio kaimyninėms valstybėms narėms riziką;

(12) elektros energijos tiekimo saugumui užtikrinti reikia veiksmingo valstybių narių, Sąjungos institucijų, įstaigų, tarnybų ir agentūrų bei atitinkamų suinteresuotųjų subjektų bendradarbiavimo. Skirstymo sistemos operatoriams ir perdavimo sistemos operatoriams tenka itin svarbus vaidmuo užtikrinant saugią, patikimą ir efektyvią elektros energijos sistemą pagal Europos Parlamento ir Tarybos direktyvos (ES) 2019/944 ([7]) 31 ir 40 straipsnius. Įvairioms reguliavimo institucijoms ir kitoms atitinkamoms kompetentingoms nacionalinėms institucijoms taip pat tenka svarbus vaidmuo užtikrinant ir stebint elektros energijos tiekimo kibernetinį saugumą – jos tai daro atlikdamos savo funkcijas, joms priskirtas direktyvomis (ES) 2019/944 ir (ES) 2022/2555. Valstybės narės turėtų paskirti esamą arba naują subjektą savo kompetentinga nacionaline institucija, atsakinga už šio reglamento įgyvendinimą, kad būtų užtikrintas skaidrus ir įtraukus visų susijusių subjektų dalyvavimas, efektyvus pasirengimas ir tinkamas reglamento įgyvendinimas, įvairių atitinkamų suinteresuotųjų subjektų ir elektros energijos bei kibernetinio saugumo srities kompetentingų institucijų tarpusavio bendradarbiavimas ir palankesnių sąlygų sudarymas, kad būtų užkertamas kelias elektros energijos sektoriaus krizėms, kurių pagrindinės priežastys susijusios su kibernetiniu saugumu, būtų atliekamas šių krizių *ex post* vertinimas ir keičiamasi su tuo susijusia informacija;

(13) kai didelio poveikio arba ypatingos svarbos poveikio subjektas teikia paslaugas daugiau negu vienoje valstybėje narėje arba turi būstinę arba kitą buveinę arba atstovą valstybėje narėje, tačiau jo tinklas ir informacinės sistemos yra vienoje arba keliose kitose valstybėse narėse, tos valstybės narės turėtų skatinti savo atitinkamas kompetentingas institucijas kuo labiau stengtis bendradarbiauti tarpusavyje ir prireikus viena kitai padėti;

(14) valstybės narės turėtų užtikrinti, kad kompetentingos institucijos turėtų reikiamus įgaliojimus didelio poveikio ir ypatingos svarbos poveikio subjektų atžvilgiu ir taip būtų skatinama laikytis šio reglamento. Tais įgaliojimais kompetentingoms institucijoms turėtų būti sudarytos sąlygos atlikti patikrinimus vietoje ir vykdyti nuotolinę priežiūrą. Tai gali būti atsitiktiniai patikrinimai, reguliarūs auditai, tiksliniai saugumo auditai, grindžiami rizikos vertinimais arba su rizika susijusia informacija, ir saugumo patikrinimai pagal objektyvius, nediskriminacinius, sąžiningus ir skaidrius rizikos vertinimo kriterijus, pagal kuriuos taip pat būtų galima prašyti informacijos, reikalingos subjekto taikomoms kibernetinio saugumo priemonėms įvertinti. Ta informacija turėtų apimti dokumentais įformintas kibernetinio saugumo politikos priemones, priežiūros užduotims atlikti reikalingus prieigos duomenis, dokumentus ar kitą informaciją ir kibernetinio saugumo politikos priemonių įgyvendinimo įrodymus, pavyzdžiui, kvalifikuoto auditoriaus atliktų saugumo auditų rezultatus ir atitinkamus pagrindžiamuosius įrodymus;

([7]) 2019 m. birželio 5 d. Europos Parlamento ir Tarybos direktyva (ES) 2019/944 dėl elektros energijos vidaus rinkos bendrųjų taisyklių, kuria iš dalies keičiama Direktyva 2012/27/ES (OL L 158, 2019 6 14, p. 125).

(15) siekdamos išvengti didelio poveikio ir ypatingos svarbos poveikio subjektams nustatomų įpareigojimų valdyti kibernetinio saugumo riziką spragų ir tų įpareigojimų dubliavimo, nacionalinės institucijos pagal Direktyvą (ES) 2022/2555 ir kompetentingos institucijos pagal šį reglamentą turėtų bendradarbiauti kibernetinio saugumo rizikos valdymo priemonių įgyvendinimo ir tų priemonių laikymosi nacionaliniu lygmeniu priežiūros klausimais. Kompetentingos institucijos pagal Direktyvą (ES) 2022/2555 galėtų pripažinti, kad, jeigu subjektas laikosi šiame reglamente nustatytų kibernetinio saugumo rizikos valdymo reikalavimų, tai jis laikosi ir atitinkamų toje direktyvoje nustatytų reikalavimų, arba atvirkščiai;

(16) bendram požiūriui į vienalaikių elektros energijos sektoriaus krizių prevenciją ir valdymą būtinas bendras valstybių narių supratimas, kas sudaro vienalaikę elektros energijos sektoriaus krizę ir kada jos svarbus veiksnys yra kibernetinis išpuolis. Visų pirma turėtų būti palengvintas valstybių narių ir atitinkamų subjektų veiksmų koordinavimas situacijai suvaldyti, kai esama galimos didelio elektros energijos trūkumo arba negalėjimo tiekti elektros energijos klientams rizikos arba yra tiesioginė tokios rizikos grėsmė ir šią padėtį lėmė kibernetinis išpuolis;

(17) Europos Parlamento ir Tarybos reglamento (ES) 2019/881 ([8]) 1 konstatuojamojoje dalyje pripažįstama, kad tinklų ir informacinėms sistemoms bei elektroninių ryšių tinklams ir paslaugoms tenka gyvybiškai svarbus vaidmuo ir jie tapo ekonomikos veikimo pamatu tokiuose esminiuose sektoriuose kaip energetika, o 44 konstatuojamojoje dalyje paaiškinama, kad Europos Sąjungos kibernetinio saugumo agentūra (toliau – ENISA) turėtų bendradarbiauti su Energetikos reguliavimo institucijų bendradarbiavimo agentūra (toliau – ACER);

(18) Reglamentu (ES) 2019/943 perdavimo sistemos operatoriams (PSO) ir skirstymo sistemos operatoriams (SSO) priskiriamos konkrečios pareigos užtikrinti kibernetinį saugumą. Jų Europos asociacijos, t. y. Europos elektros energijos perdavimo sistemos operatorių tinklas (ENTSO-E) ir Europos skirstymo sistemos operatorių subjektas (ES SSO subjektas), atitinkamai pagal to reglamento 30 ir 55 straipsnius skatina kibernetinį saugumą bendradarbiaudamos su atitinkamomis valdžios institucijomis ir reguliuojamais subjektais;

(19) siekiant bendro požiūrio į vienalaikių elektros energijos sektoriaus krizių, kurių pagrindinės priežastys susijusios su kibernetiniu saugumu, prevenciją ir valdymą, reikia, kad visi atitinkami suinteresuotieji subjektai, nustatydami rizikos veiksnius, susijusius su elektros energijos tiekimo kibernetiniu saugumu, taikytų suderintus metodus ir apibrėžtis. Šiuo tikslu taip pat reikia sugebėti veiksmingai palyginti savo ir kaimyninių šalių subjektų rezultatus šioje srityje. Todėl reikia nustatyti procesus, funkcijas ir pareigas, kad būtų galima parengti ir atnaujinti rizikos valdymo metodikas, incidentų klasifikavimo skales ir kibernetinio saugumo priemones, pritaikytas kibernetinio saugumo rizikos veiksniams, kurie turi poveikį tarpvalstybiniams elektros energijos srautams;

(20) valstybės narės per šiam reglamentui įgyvendinti paskirtą kompetentingą instituciją privalo nustatyti subjektus, atitinkančius kriterijus, pagal kuriuos juos būtų galima priskirti prie didelio poveikio ir ypatingos svarbos poveikio subjektų. Siekiant tuo atžvilgiu pašalinti valstybių narių skirtumus ir visiems atitinkamiems subjektams užtikrinti teisinį tikrumą dėl kibernetinio saugumo rizikos valdymo priemonių ir pareigų pranešti, turėtų būti nustatyti tam tikri kriterijai, kuriais remiantis nustatomi subjektai, patenkantys į šio reglamento taikymo sritį. Tie kriterijai turėtų būti nustatyti ir nuolat atnaujinami parengiant ir tvirtinant šiame reglamente nustatytas nuostatas, sąlygas ir metodikas;

(21) šio reglamento nuostatos neturėtų daryti poveikio Sąjungos teisės nuostatų, kuriose numatytos specialios informacinių ir ryšių technologijų (toliau – IRT) produktų, paslaugų ir procesų sertifikavimo taisyklės, visų pirma Reglamento (ES) 2019/881 nuostatų dėl Europos kibernetinio saugumo sertifikavimo schemų kūrimo, taikymui. Taikant šį reglamentą IRT produktai turėtų apimti ir techninius įrenginius bei programinę įrangą, sudarančius sąlygas tiesiogiai sąveikauti su techniniu elektros energijos tinklu, visų pirma pramonines kontrolės sistemas, kurias galima naudoti energijai perduoti, skirstyti ir gaminti, taip pat atitinkamai informacijai rinkti ir perduoti. Minėtomis nuostatomis turėtų būti užtikrinta, kad IRT produktai, paslaugos ir procesai, perkami vykdant viešuosius pirkimus, atitiktų Reglamento (ES) 2019/881 51 straipsnyje nurodytus atitinkamus saugumo tikslus;

([8]) 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15).

(22) pastarieji kibernetiniai išpuoliai rodo, kad subjektai vis dažniau tampa tiekimo grandinės atakų taikiniu. Tokios tiekimo grandinės atakos paveikia ne tik joje veikiančius atskirus subjektus, bet ir turi grandininį poveikį didesniems išpuoliams prieš subjektus, su kuriais minėti subjektai yra susiję elektros energijos tinkle. Todėl buvo įtrauktos nuostatos ir rekomendacijos, padėsiančios sumažinti kibernetinio saugumo riziką, susijusią su tiekimo grandinės procesais, visų pirma viešaisiais pirkimais, turinčiais poveikį tarpvalstybiniams elektros energijos srautams;

(23) tinklų ir informacinių sistemų pažeidžiamumo išnaudojimas gali sukelti didelius energijos tiekimo sutrikimus ir padaryti žalą ekonomikai ir vartotojams, todėl toks pažeidžiamumas turėtų būti greitai identifikuojamas ir neutralizuojamas, kad būtų sumažinta rizika. Siekdami palengvinti veiksmingą šio reglamento įgyvendinimą, atitinkami subjektai ir kompetentingos institucijos turėtų bendradarbiauti vykdydami pratybas ir atlikdami bandomuosius veiksmus, kurie laikomi tinkamais tam tikslui pasiekti, t. y. be kita ko, keistis informacija apie kibernetines grėsmes, kibernetinius išpuolius, pažeidžiamumą, priemones ir metodus, taktiką, būdus ir procedūras, pasirengimą valdyti kibernetinio saugumo krizes ir atlikti kitus veiksmus. Technologijos nuolat vystomos, o elektros energijos sektorius sparčiai skaitmenizuojamas, todėl priimtomis nuostatomis neturėtų būti kenkiama inovacijoms, sudaroma kliūčių patekti į elektros energijos rinką ar trukdoma vėliau pasinaudoti novatoriškais sprendimais, kuriais prisidedama prie elektros energijos sistemos efektyvumo ir tvarumo;

(24) informacija, renkama siekiant stebėti šio reglamento įgyvendinimą, turėtų būti pagrįstai disponuojama vadovaujantis būtinybės žinoti principu. Suinteresuotiesiems subjektams turėtų būti suteikti įgyvendinami ir veiksmingi tokios informacijos pateikimo terminai. Neturėtų būti reikalaujama informaciją teikti du kartus;

(25) kibernetinio saugumo užtikrinimas neapsiriboja Sąjungos sienomis. Siekiant sistemos saugumo būtinas kaimyninių trečiųjų šalių dalyvavimas. Sąjunga ir jos valstybės narės turėtų stengtis padėti kaimyninėms trečiosioms šalims, kurių elektros energijos infrastruktūra sujungta su Europos tinklu, taikyti kibernetinio saugumo taisykles, panašias į išdėstytas šiame reglamente;

(26) siekdami ankstyvuoju etapu pagerinti saugumo koordinavimą, išbandyti būsimas privalomas nuostatas, sąlygas ir metodikas, ENTSO-E, ES SSO subjektas ir kompetentingos institucijos turėtų pradėti rengti neprivalomas gaires iš karto, kai tik įsigalios šis reglamentas. Šios gairės taps atskaitos scenarijumi būsimoms nuostatoms, sąlygoms ir metodikoms rengti. Tuo pačiu metu kompetentingos institucijos turėtų identifikuoti subjektus kaip kandidatus įgyti didelio poveikio ir ypatingos svarbos poveikio subjekto statusą, kad jie savanoriškai pradėtų vykdyti pareigas;

(27) šis reglamentas parengtas glaudžiai bendradarbiaujant su ACER, ENISA, ENTSO-E, ES SSO subjektu ir kitais suinteresuotaisiais subjektais, siekiant skaidriai ir kolektyviai priimti veiksmingas, subalansuotas ir proporcingas taisykles;

(28) šiuo reglamentu papildomos ir sustiprinamos krizių valdymo priemonės, nustatytos ES reagavimo į kibernetinio saugumo krizes sistemoje, kuri išdėstyta Komisijos rekomendacijoje (ES) 2017/1584 ([9]). Kibernetinis išpuolis taip pat gali sukelti Reglamento (ES) 2019/941 2 straipsnio 9 punkte apibrėžtą elektros energijos sektoriaus krizę, turinčią poveikį tarpvalstybiniams elektros energijos srautams, prie jos prisidėti arba su ja sutapti. Ta elektros energijos sektoriaus krizė gali virsti vienalaike elektros energijos sektoriaus krize, apibrėžta Reglamento (ES) 2019/941 2 straipsnio 10 punkte. Toks incidentas gali turėti poveikį ir kitiems nuo elektros energijos tiekimo saugumo priklausomiems sektoriams. Jeigu toks incidentas išaugtų į didelio masto kibernetinio saugumo incidentą, nurodytą Direktyvos (ES) 2022/2555 16 straipsnyje, turėtų būti taikomos to straipsnio nuostatos, kuriomis sukuriamas Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas (toliau – EU-CyCLONe). Siekdamos valdyti krizę Sąjungos lygmeniu, atitinkamos šalys turėtų kliautis ES integruotu politinio atsako į krizes mechanizmu (toliau – IPCR mechanizmas), nustatytu Tarybos įgyvendinimo sprendime (ES) 2018/1993 ([10]);

(29) šis reglamentas nedaro poveikio valstybių narių kompetencijai imtis priemonių, būtinų gyvybiniams jų saugumo interesams užtikrinti, tvarkai palaikyti bei visuomenės saugumui užtikrinti, ir sudaryti sąlygas tirti bei išsiaiškinti nusikalstamas veikas ir už jas patraukti baudžiamojon atsakomybėn, laikantis Sąjungos teisės. Pagal SESV 346 straipsnį jokia valstybė narė neprivalo teikti informacijos, kurios atskleidimas, jos nuomone, prieštarauja gyvybiniams jos saugumo interesams;

([9]) 2017 m. rugsėjo 13 d. Komisijos rekomendacija (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes (OL L 239, 2017 9 19, p. 36).

([10]) 2018 m. gruodžio 11 d. Tarybos įgyvendinimo sprendimas (ES) 2018/1993 dėl ES integruoto politinio atsako į krizes mechanizmo (OL L 320, 2018 12 17, p. 28).

(30) nors šis reglamentas iš esmės taikomas subjektams, vykdantiems elektros energijos gamybos atominėse elektrinėse veiklą, dalis šios veiklos gali būti susijusi su nacionaliniu saugumu;

(31) pagal šį reglamentą vykdomam asmens duomenų tvarkymui taikoma Sąjungos duomenų apsaugos teisė ir Sąjungos privatumo teisė. Visų pirma šis reglamentas nedaro poveikio Europos Parlamento ir Tarybos reglamento (ES) 2016/679 ([11]), Europos Parlamento ir Tarybos direktyvos 2002/58/EB ([12]) ir Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([13]) taikymui. Todėl šiuo reglamentu neturėtų būti daroma poveikio, *inter alia*, institucijų, kurios yra kompetentingos kontroliuoti, kaip laikomasi taikytinos Sąjungos duomenų apsaugos teisės ir Sąjungos privatumo teisės, užduotims ir įgaliojimams;

(32) tarptautinis bendradarbiavimas kibernetinio saugumo klausimais yra labai svarbus, todėl valstybių narių paskirtos kompetentingos institucijos, atsakingos už joms šiuo reglamentu pavestas užduotis, turėtų turėti galimybę dalyvauti tarptautinio bendradarbiavimo tinkluose. Taigi, siekiant, kad kompetentingos institucijos galėtų atlikti savo užduotis, joms turėtų būti suteikta galimybė keistis informacija, įskaitant asmens duomenis, su trečiųjų šalių kompetentingomis institucijomis, jeigu yra įvykdytos Sąjungos duomenų apsaugos teisėje numatytos asmens duomenų perdavimo į trečiąsias šalis sąlygos, įskaitant nurodytas Reglamento (ES) 2016/679 49 straipsnyje;

(33) didelio poveikio ar ypatingos svarbos poveikio subjektų vykdomas asmens duomenų tvarkymas tiek, kiek tai būtina ir proporcinga siekiant užtikrinti turto saugumą, galėtų būti laikomas teisėtu remiantis tuo, kad toks tvarkymas atitinka duomenų valdytojui taikomą teisinę prievolę pagal Reglamento (ES) 2016/679 6 straipsnio 1 dalies c punkto ir 6 straipsnio 3 dalies reikalavimus. Taip pat tvarkyti asmens duomenis gali reikėti teisėtais didelio poveikio ir ypatingos svarbos poveikio subjektų, taip pat jų vardu veikiančių saugumo technologijų tiekėjų ir paslaugų teikėjų interesais pagal Reglamento (ES) 2016/679 6 straipsnio 1 dalies f punktą, be kita ko, kai toks tvarkymas yra būtinas pagal dalijimosi kibernetinio saugumo informacija susitarimus arba savanoriškai pranešant atitinkamą informaciją pagal šį reglamentą. Taikant su kibernetinių išpuolių prevencija, atskleidimu, nustatymu, apribojimu, analize ir reagavimu į juos susijusias priemones, informuotumo apie konkrečias kibernetines grėsmes didinimo priemones, keičiantis informacija ištaisant pažeidžiamumą ir koordinuotai jį atskleidžiant, taip pat savanoriškai keičiantis informacija apie tuos kibernetinius išpuolius, kibernetines grėsmes ir pažeidžiamumą, užvaldymo rodiklius, taktiką, metodus ir procedūras, kibernetinio saugumo įspėjimus ir konfigūracijos priemones, gali reikėti tvarkyti tam tikrų kategorijų asmens duomenis, pavyzdžiui, IP adresus, universaliuosius išteklių adresus (URL), domenų vardus, el. pašto adresus ir, kai jose atskleidžiami asmens duomenys, laiko žymas. Kompetentingų institucijų, bendrųjų kontaktinių punktų ir CSIRT vykdomas asmens duomenų tvarkymas gali būti teisinė prievolė arba gali būti laikomas būtinu siekiant atlikti užduotį viešojo intereso labui arba vykdant duomenų valdytojui pagal Reglamento (ES) 2016/679 6 straipsnio 1 dalies c arba e punktą ir 6 straipsnio 3 dalį pavestas viešosios valdžios funkcijas, arba siekiant didelio poveikio ir ypatingos svarbos poveikio subjektų teisėtų interesų, kaip nurodyta to reglamento 6 straipsnio 1 dalies f punkte. Be to, nacionalinėje teisėje gali būti nustatytos taisyklės, pagal kurias kompetentingoms institucijoms, bendriesiems kontaktiniams punktams ir CSIRT būtų leidžiama tiek, kiek tai būtina ir proporcinga siekiant užtikrinti didelio poveikio ir ypatingos svarbos poveikio subjektų tinklų ir informacinių sistemų saugumą, tvarkyti specialių kategorijų asmens duomenis pagal Reglamento (ES) 2016/679 9 straipsnį, visų pirma numatant tinkamas ir konkrečias fizinių asmenų pagrindinių teisių ir interesų apsaugos priemones, įskaitant tokių duomenų pakartotinio naudojimo techninius apribojimus ir pažangiausių saugumo bei privatumo apsaugos priemonių, pavyzdžiui, pseudonimų suteikimo arba šifravimo, kai anoniminimas gali daryti didelį poveikį siekiamam tikslui, naudojimą;

([11]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1).

([12]) 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37).

([13]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39).

(34) daugeliu atvejų dėl kibernetinių išpuolių kyla pavojus asmens duomenų saugumui. Tokiomis aplinkybėmis kompetentingos institucijos turėtų bendradarbiauti ir keistis informacija visais svarbiais klausimais su institucijomis, nurodytomis Reglamente (ES) 2016/679 ir Direktyvoje 2002/58/EB;

(35) vadovaujantis Reglamento (ES) 2018/1725 42 straipsnio 1 dalimi buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir jis pateikė nuomonę 2023 m. lapkričio 17 d.,

PRIĖMĖ ŠĮ REGLAMENTĄ:

I skyrius

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas

Šiuo reglamentu nustatomas tinklo kodeksas, kuriame išdėstytos sektorinės tarpvalstybinių elektros energijos srautų kibernetinio saugumo aspektų taisyklės, įskaitant bendrų būtinųjų reikalavimų, planavimo, stebėsenos, ataskaitų teikimo ir krizių valdymo taisykles.

2 straipsnis

Taikymo sritis

1. Šis reglamentas taikomas toliau išvardytų subjektų veiklos tarpvalstybinių elektros energijos srautų kibernetinio saugumo aspektams, jei pagal 24 straipsnį tie subjektai identifikuoti kaip didelio poveikio arba ypatingos svarbos poveikio subjektai:

a) elektros energijos įmonių, apibrėžtų Direktyvos (ES) 2019/944 2 straipsnio 57 punkte;

b) paskirtųjų elektros energijos rinkos operatorių (PEERO), apibrėžtų Reglamento (ES) 2019/943 2 straipsnio 8 punkte;

c) Komisijos įgyvendinimo reglamento (ES) Nr. 1348/2014 ([14]) 2 straipsnio 4 punkte apibrėžtų organizuotos rinkos sistemų, arba organizuotų rinkų, kuriose organizuojami tarpvalstybiniams elektros energijos srautams aktualių produktų sandoriai;

d) šio reglamento 3 straipsnio 9 punkte nurodytų ypatingos svarbos IRT paslaugų teikėjų;

e) ENTSO-E, įsteigto pagal Reglamento (ES) 2019/943 28 straipsnį;

f) ES SSO subjekto, įsteigto pagal Reglamento (ES) 2019/943 52 straipsnį;

g) už balansą atsakingų šalių, apibrėžtų Reglamento (ES) 2019/943 2 straipsnio 14 punkte;

h) įkrovimo prieigų operatorių, nurodytų Direktyvos (ES) 2022/2555 I priede;

i) regioninių koordinavimo centrų, įsteigtų pagal Reglamento (ES) 2019/943 35 straipsnį;

j) valdomų saugumo paslaugų teikėjų, apibrėžtų Direktyvos (ES) 2022/2555 6 straipsnio 40 punkte;

k) bet kurio kito subjekto ar trečiosios šalies, kuriems buvo perduotos arba paskirtos pareigos pagal šį reglamentą.

2. Naudodamosi turimais įgaliojimais, už šiame reglamente nustatytų užduočių vykdymą yra atsakingos šios institucijos:

a) Europos Sąjungos energetikos reguliavimo institucijų bendradarbiavimo agentūra (ACER), įsteigta Europos Parlamento ir Tarybos reglamentu (ES) 2019/942 ([15]);

b) pagal 4 straipsnį valstybių narių paskirtos nacionalinės kompetentingos institucijos, atsakingos už joms pagal šį reglamentą paskirtų užduočių vykdymą, t. y. kompetentingos institucijos;

c) kiekvienos valstybės narės pagal Direktyvos (ES) 2019/944 57 straipsnio 1 dalį paskirtos nacionalinės reguliavimo institucijos (NRI);

([14]) 2014 m. gruodžio 17 d. Komisijos įgyvendinimo reglamentas (ES) Nr. 1348/2014 dėl duomenų teikimo, kuriuo įgyvendinamos Europos Parlamento ir Tarybos reglamento (ES) Nr. 1227/2011 dėl didmeninės energijos rinkos vientisumo ir skaidrumo 8 straipsnio 2 ir 6 dalys (OL L 363, 2014 12 18, p. 121).

([15]) 2019 m. birželio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/942, kuriuo įsteigiama Europos Sąjungos energetikos reguliavimo institucijų bendradarbiavimo agentūra (OL L 158, 2019 6 14, p. 22).

d) už pasirengimą valdyti riziką atsakingos kompetentingos institucijos, įsteigtos pagal Reglamento (ES) 2019/941 3 straipsnį;

e) reagavimo į kompiuterių saugumo incidentus tarnybos (CSIRT), paskirtos arba įsteigtos pagal Direktyvos (ES) 2022/2555 10 straipsnį;

f) už kibernetinį saugumą atsakingos kompetentingos institucijos (už kibernetinį saugumą atsakingos NKI), paskirtos arba įsteigtos pagal Direktyvos (ES) 2022/2555 8 straipsnį;

g) Europos Sąjungos kibernetinio saugumo agentūra, įsteigta pagal Reglamentą (ES) 2019/881;

h) bet kurios kitos institucijos ar trečioji šalis, kurioms pareigos buvo perduotos arba paskirtos pagal 4 straipsnio 3 dalį.

3. Šis reglamentas taikomas ir visiems subjektams, kurie nėra įsisteigę Sąjungoje, bet teikia paslaugas subjektams Sąjungoje, jeigu kompetentingos institucijos juos pagal 24 straipsnio 2 dalį yra identifikavusios kaip didelio poveikio arba ypatingos svarbos poveikio subjektus.

4. Šiuo reglamentu nedaroma poveikio valstybių narių pareigai užtikrinti nacionalinį saugumą ar jų įgaliojimams apsaugoti kitas esmines valstybės funkcijas, įskaitant valstybės teritorinio vientisumo užtikrinimą ir teisėtvarkos palaikymą.

5. Šiuo reglamentu nedaroma poveikio valstybių narių pareigai pagal Sutartis užtikrinti nacionalinį saugumą, susijusį su elektros energijos gamyba branduolinėse elektrinėse, įskaitant veiklą branduolinio sektoriaus vertės grandinėje.

6. Subjektai, kompetentingos institucijos, subjekto lygmens bendrieji kontaktiniai punktai ir CSIRT tvarko asmens duomenis tiek, kiek tai būtina šio reglamento tikslais, juos tvarko pagal Reglamentą (ES) 2016/679 ir toks tvarkymas visų pirma grindžiamas to reglamento 6 straipsniu.

3 straipsnis

Apibrėžtys

Vartojamų terminų apibrėžtys:

1) turtas – asmeniui, organizacijai arba valdžios sektoriui vertinga tinklų ir informacinių sistemų informacija, materiali ir nemateriali programinė įranga ir aparatinė įranga;

2) už pasirengimą valdyti riziką atsakinga kompetentinga institucija – kompetentinga institucija, paskirta pagal Reglamento (ES) 2019/941 3 straipsnį;

3) reagavimo į kompiuterių saugumo incidentus tarnyba – tarnyba, atsakinga už rizikos ir incidentų valdymą pagal Direktyvos (ES) 2022/2555 10 straipsnį;

4) ypatingos svarbos poveikio turtas – turtas, būtinas ypatingos svarbos poveikio procesui vykdyti;

5) ypatingos svarbos poveikio subjektas – ypatingos svarbos poveikio procesą vykdantis subjektas, kurį pagal 24 straipsnį identifikavo kompetentingos institucijos;

6) ypatingos svarbos poveikio perimetras – 2 straipsnio 1 dalyje nurodyto subjekto nustatytas visą ypatingos svarbos poveikio turtą apimantis perimetras, kuriame galima kontroliuoti prieigą prie šio turto ir kuriuo apibrėžiama sustiprintos kibernetinio saugumo kontrolės aprėptis;

7) ypatingos svarbos poveikio procesas – subjekto vykdomas veiklos procesas, kuriam nustatyti kibernetinių incidentų poveikio elektros energijos srautams indeksai viršija ypatingos svarbos poveikio slenkstį;

8) ypatingos svarbos poveikio slenkstis – 19 straipsnio 3 dalies b punkte nurodytos kibernetinių incidentų poveikio elektros energijos srautams indeksų vertės, kurias viršijus kibernetinis išpuolis, nutaikytas į veiklos procesą, visiškai sutrikdytų tarpvalstybinius elektros energijos srautus;

9) ypatingos svarbos IRT paslaugų teikėjas – subjektas, teikiantis IRT paslaugą arba vykdantis IRT procesą, kurie yra būtini ypatingos svarbos poveikio arba didelio poveikio procesui, veikiančiam tarpvalstybinių elektros energijos srautų kibernetinio saugumo aspektus, ir kuriuos sutrikdžius galėtų būti sukeltas kibernetinis išpuolis, kurio poveikis viršytų ypatingos svarbos poveikio arba didelio poveikio slenkstį;

10) tarpvalstybinis elektros energijos srautas – tarpvalstybinis srautas, apibrėžtas Reglamento (ES) 2019/943 2 straipsnio 3 punkte;

11) kibernetinis išpuolis – kibernetinis išpuolis, apibrėžtas Reglamento (ES) 2022/2554 3 straipsnio 14 punkte;

12) kibernetinis saugumas – kibernetinis saugumas, apibrėžtas Reglamento (ES) 2019/881 2 straipsnio 1 punkte;

13) kibernetinio saugumo kontrolė – veiksmai ar procedūros, atliekami siekiant išvengti kibernetinio saugumo rizikos, ją aptikti, neutralizuoti arba kuo labiau sumažinti;

14) kibernetinio saugumo incidentas – incidentas, apibrėžtas Direktyvos (ES) 2022/2555 6 straipsnio 6 punkte;

15) kibernetinio saugumo valdymo sistema – subjekto bendrai valdoma politika, procedūros, gairės, taip pat susiję ištekliai ir veikla, kuriais siekiama apsaugoti jo informacinį turtą nuo kibernetinių grėsmių, sistemingai kuriant, įgyvendinant, valdant, stebint, peržiūrint, užtikrinant ir gerinant organizacijos tinklų ir informacinių sistemų saugumą;

16) kibernetinio saugumo operacijų centras – specialus centras, kuriame vieno ar daugiau ekspertų techninė grupė, naudodamasi kibernetinio saugumo IT sistemomis, atlieka su saugumu susijusias užduotis (kibernetinio saugumo operacijų centro (KSOC) paslaugos), pvz., reaguoja į kibernetinius išpuolius, šalina saugumo konfigūracijos klaidas, vykdo saugumo stebėseną, analizuoja registracijos žurnalus ir aptinka kibernetinius išpuolius;

17) kibernetinė grėsmė – kibernetinė grėsmė, apibrėžta Reglamento (ES) 2019/881 2 straipsnio 8 punkte;

18) kibernetinio saugumo pažeidžiamumo valdymas – pažeidžiamumo identifikavimo ir šalinimo praktika;

19) subjektas – subjektas, apibrėžtas Direktyvos (ES) 2022/2555 6 straipsnio 38 punkte;

20) išankstinis perspėjimas – informacija, būtina siekiant nurodyti, jog įtariama, kad didelis incidentas kilo dėl neteisėtų ar piktavališkų veiksmų arba kad jo poveikis galėtų būti tarpvalstybinis;

21) kibernetinių incidentų poveikio elektros energijos srautams indeksas (KIPEI) – indeksas arba klasifikacijos skalė, pagal kuriuos įvertinami galimi kibernetinių išpuolių padariniai veiklos procesams, susijusiems su tarpvalstybiniais elektros energijos srautais;

22) Europos kibernetinio saugumo sertifikavimo schema – schema, apibrėžta Reglamento (ES) 2019/881 2 straipsnio 9 punkte;

23) didelio poveikio subjektas – didelio poveikio procesą vykdantis subjektas, kurį pagal 24 straipsnį identifikavo kompetentingos institucijos;

24) didelio poveikio procesas – subjekto vykdomas veiklos procesas, kuriam nustatyti kibernetinių incidentų poveikio elektros energijos srautams indeksai viršija didelio poveikio slenkstį;

25) didelio poveikio turtas – turtas, būtinas didelio poveikio procesui vykdyti;

26) didelio poveikio slenkstis – 19 straipsnio 3 dalies b punkte nurodytos kibernetinių incidentų poveikio elektros energijos srautams indeksų vertės, kurias viršijus sėkmingas kibernetinis išpuolis, nutaikytas į veiklos procesą, labai sutrikdytų tarpvalstybinius elektros energijos srautus;

27) didelio poveikio perimetras – 2 straipsnio 1 dalyje nurodyto subjekto nustatytas visą didelio poveikio turtą apimantis perimetras, kuriame galima kontroliuoti prieigą prie šio turto ir kuriuo apibrėžiama būtinosios kibernetinio saugumo kontrolės aprėptis;

28) IRT produktas – IRT produktas, apibrėžtas Reglamento (ES) 2019/881 2 straipsnio 12 punkte;

29) IRT paslauga – IRT paslauga, apibrėžta Reglamento (ES) 2019/881 2 straipsnio 13 punkte;

30) IRT procesas – IRT procesas, apibrėžtas Reglamento (ES) 2019/881 2 straipsnio 14 punkte;

31) senoji sistema – senoji IRT sistema, apibrėžta Reglamento (ES) 2022/2554 3 straipsnio 3 punkte;

32) nacionalinis bendrasis kontaktinis punktas – kiekvienos valstybės narės pagal Direktyvos (ES) 2022/2555 8 straipsnio 3 dalį paskirtas arba įsteigtas bendrasis kontaktinis punktas;

33) TIS kibernetinių krizių valdymo institucijos – institucijos, paskirtos arba įsteigtos pagal Direktyvos (ES) 2022/2555 9 straipsnio 1 dalį;

34) iniciatorius – subjektas, inicijuojantis keitimosi informacija, dalijimosi informacija arba informacijos išsaugojimo įvykį;

35) viešojo pirkimo specifikacijos – subjektų nustatytos naujų arba atnaujintų IRT produktų, procesų ar paslaugų pirkimo specifikacijos;

36) atstovas – Sąjungoje įsisteigęs fizinis arba juridinis asmuo, kuris yra aiškiai paskirtas veikti didelio arba ypatingos svarbos poveikio subjekto, neįsisteigusio Sąjungoje, bet teikiančio paslaugas subjektams Sąjungoje, vardu ir į kurį kompetentinga institucija arba CSIRT, užuot kreipusis į patį didelio arba ypatingos svarbos poveikio subjektą, gali kreiptis dėl to subjekto pareigų pagal šį reglamentą;

37) rizika – rizika, apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 9 punkte;

38) rizikos poveikio matrica – atliekant rizikos vertinimą naudojama matrica, skirta kiekvienos vertinamos rizikos poveikio lygiui nustatyti;

39) vienalaikė elektros energijos sektoriaus krizė – elektros energijos sektoriaus krizė, apibrėžta Reglamento (ES) 2019/941 2 straipsnio 10 punkte;

40) subjekto lygmens bendrasis kontaktinis punktas – pagal 38 straipsnio 1 dalies c punktą paskirtas subjekto lygmens bendrasis kontaktinis punktas;

41) suinteresuotasis subjektas – organizacijos ar proceso sėkme ir nuolatiniu veikimu suinteresuota šalis, pvz., darbuotojai, direktoriai, akcininkai, reguliavimo institucijos, asociacijos, tiekėjai ir klientai;

42) standartas – standartas, apibrėžtas Europos Parlamento ir Tarybos reglamento (ES) Nr. 1025/2012 ([16]) 2 straipsnio 1 punkte;

43) sistemos eksploatavimo regionas – sistemos eksploatavimo regionas, nustatytas pagal Reglamento (ES) 2019/943 36 straipsnį priimto ACER sprendimo Nr. 05-2022 dėl sistemos eksploatavimo regionų nustatymo I priede;

44) sistemų operatoriai – skirstymo sistemos operatorius (SSO) ir perdavimo sistemos operatorius (PSO), apibrėžti atitinkamai Direktyvos (ES) 2019/944 2 straipsnio 29 punkte ir 35 punkte;

45) Sąjungos masto ypatingos svarbos poveikio procesas – elektros energijos sektoriaus procesas, kuris gali apimti daug subjektų ir kuriam kibernetinis išpuolis gali padaryti ypatingos svarbos poveikį, kaip nustatyta atliekant Sąjungos masto kibernetinio saugumo rizikos vertinimą;

46) Sąjungos masto didelio poveikio procesas – elektros energijos sektoriaus procesas, kuris gali apimti daug subjektų ir kuriam kibernetinis išpuolis gali padaryti didelį poveikį, kaip nustatyta atliekant Sąjungos masto kibernetinio saugumo rizikos vertinimą;

47) nepašalintas aktyviai išnaudojamas pažeidžiamumas – pažeidžiamumas, kuris dar nėra viešai atskleistas ir pašalintas ir kuriuo, kaip matyti iš patikimų įrodymų, pasinaudodamas subjektas be sistemos savininko leidimo paleido kenkėjišką programos kodą;

48) pažeidžiamumas – pažeidžiamumas, apibrėžtas Direktyvos (ES) 2022/2555 6 straipsnio 15 punkte.

4 straipsnis

Kompetentinga institucija

1. Kiekviena valstybė narė kuo greičiau ir bet kuriuo atveju ne vėliau kaip 2024 m. gruodžio 13 d. paskiria nacionalinę valdžios ar reguliavimo instituciją, atsakingą už šiuo reglamentu jai pavestų užduočių vykdymą (toliau – kompetentinga institucija). Kol kompetentingai institucijai bus pavesta vykdyti užduotis pagal šį reglamentą, jos užduotis pagal šį reglamentą vykdo kiekvienos valstybės narės pagal Direktyvos (ES) 2019/944 57 straipsnio 1 dalį paskirta reguliavimo institucija.

2. Valstybės narės nedelsdamos praneša Komisijai, ACER, ENISA, pagal Direktyvos (ES) 2022/2555 14 straipsnį įsteigtai TIS bendradarbiavimo grupei ir pagal 2012 m. lapkričio 15 d. Komisijos sprendimo ([17]) 1 straipsnį įsteigtai Elektros energijos srities veiklos koordinavimo grupei pagal šio straipsnio 1 dalį paskirtos kompetentingos institucijos pavadinimą ir kontaktinius duomenis, taip pat visus vėlesnius jų pakeitimus.

([16]) 2012 m. spalio 25 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1025/2012 dėl Europos standartizacijos, kuriuo iš dalies keičiamos Tarybos direktyvos 89/686/EEB ir 93/15/EEB ir Europos Parlamento ir Tarybos direktyvos 94/9/EB, 94/25/EB, 95/16/EB, 97/23/EB, 98/34/EB, 2004/22/EB, 2007/23/EB, 2009/23/EB ir 2009/105/EB ir panaikinamas Tarybos sprendimas 87/95/EEB ir Europos Parlamento ir Tarybos sprendimas Nr. 1673/2006/EB (OL L 316, 2012 11 14, p. 12).

([17]) 2012 m. lapkričio 15 d. Komisijos sprendimas, kuriuo įsteigiama Elektros energijos srities veiklos koordinavimo grupė (2012/C 353/02) (OL C 353, 2012 11 17, p. 2).

3. Valstybės narės gali leisti savo kompetentingai institucijai šiuo reglamentu jai pavestas užduotis, išskyrus 5 straipsnyje išvardytas užduotis, perduoti kitoms nacionalinėms institucijoms. Kiekviena kompetentinga institucija stebi, kaip institucijos, kurioms ji perdavė užduotis, taiko šį reglamentą. Kompetentinga institucija praneša Komisijai, ACER, Elektros energijos srities veiklos koordinavimo grupei, ENISA ir TIS bendradarbiavimo grupei institucijų, kurioms perduota užduotis, pavadinimus, kontaktinius duomenis, paskirtas užduotis ir visus vėlesnius jų pakeitimus.

5 straipsnis

Atitinkamų institucijų ir įstaigų bendradarbiavimas nacionaliniu lygmeniu

Kompetentingos institucijos koordinuoja ir užtikrina tinkamą už kibernetinį saugumą atsakingų kompetentingų institucijų, kibernetinių krizių valdymo institucijų, NRI, už pasirengimą valdyti riziką atsakingų kompetentingų institucijų ir CSIRT bendradarbiavimą, kad būtų vykdomos atitinkamos šiame reglamente nustatytos pareigos. Kompetentingos institucijos taip pat koordinuoja veiksmus su visomis kitomis įstaigomis ar institucijomis, kurias nustato kiekviena valstybė narė, siekdamos užtikrinti sklandžias procedūras ir išvengti užduočių ir pareigų dubliavimo. Kompetentingos institucijos gali nurodyti atitinkamoms NRI prašyti ACER pateikti nuomonę pagal 8 straipsnio 3 dalį.

6 straipsnis

Nuostatos ir sąlygos ar metodikos arba planai

1. PSO, bendradarbiaudami su ES SSO subjektu, parengia nuostatų ir sąlygų arba metodikų pasiūlymus pagal 2 dalį arba planų pasiūlymus pagal 3 dalį.

2. Visos kompetentingos institucijos tvirtina šias nuostatas ir sąlygas arba metodikas ir visus jų pakeitimus:

a) kibernetinio saugumo rizikos vertinimo metodikas pagal 18 straipsnio 1 dalį;

b) išsamaus tarpvalstybinių elektros energijos srautų kibernetinio saugumo rizikos vertinimo ataskaitą pagal 23 straipsnį;

c) būtinosios ir sustiprintos kibernetinio saugumo kontrolės pagal 29 straipsnį, elektros energijos kibernetinio saugumo kontrolės priemonių ir standartų atitiktį pagal 34 straipsnį, įskaitant būtinosios ir sustiprintos kontrolės priemones tiekimo grandinėje pagal 33 straipsnį;

d) kibernetinio saugumo viešojo pirkimo rekomendaciją pagal 35 straipsnį;

e) kibernetinių išpuolių klasifikavimo skalės metodiką pagal 37 straipsnio 8 dalį.

3. Regioninių kibernetinio saugumo rizikos mažinimo planų pasiūlymus pagal 22 straipsnį turi patvirtinti visos atitinkamo sistemos eksploatavimo regiono kompetentingos institucijos.

4. 2 dalyje išvardytų nuostatų ir sąlygų ar metodikų pasiūlymuose arba 3 dalyje nurodytų planų pasiūlymuose pateikiamas siūlomas jų įgyvendinimo tvarkaraštis ir tikėtino jų poveikio šio reglamento tikslams aprašymas.

5. ES SSO subjektas gali pateikti atitinkamiems PSO pagrįstą nuomonę likus 3 savaitėms iki nuostatų ir sąlygų ar metodikų arba planų pasiūlymo pateikimo kompetentingoms institucijoms termino. Už nuostatų ir sąlygų ar metodikų arba planų pasiūlymą atsakingi PSO, prieš pateikdami jį tvirtinti kompetentingoms institucijoms, atsižvelgia į ES SSO subjekto pagrįstą nuomonę. Kai į ES SSO subjekto nuomonę neatsižvelgiama, PSO nurodo motyvus.

6. Kartu rengdami nuostatas, sąlygas bei metodikas ir planus, dalyvaujantys PSO glaudžiai bendradarbiauja. PSO, padedami ENTSO-E ir bendradarbiaudami su ES SSO subjektu, reguliariai informuoja kompetentingas institucijas ir ACER apie nuostatų ir sąlygų ar metodikų arba planų rengimo pažangą.

7 straipsnis

PSO balsavimo taisyklės

1. Kai PSO, priimdami sprendimus dėl nuostatų ir sąlygų arba metodikų pasiūlymų, negali susitarti, jie sprendimą priima kvalifikuota balsų dauguma. Kvalifikuota balsų dauguma balsuojant dėl tokių pasiūlymų apskaičiuojama taip:

a) PSO, atstovaujantys ne mažiau kaip 55 % valstybių narių, ir

b) PSO, atstovaujantys valstybėms narėms, kurių gyventojai sudaro bent 65 % Sąjungos gyventojų.

2. Sprendimus dėl 6 straipsnio 2 dalyje išvardytų nuostatų ir sąlygų arba metodikų pasiūlymų blokuojančią mažumą sudaro PSO, atstovaujantys ne mažiau kaip keturioms valstybėms narėms; priešingu atveju laikoma, kad kvalifikuota balsų dauguma pasiekta.

3. Kai sistemos eksploatavimo regiono PSO, priimdami sprendimus dėl 6 straipsnio 2 dalyje išvardytų planų pasiūlymų, negali susitarti, o atitinkamą sistemos eksploatavimo regioną sudaro daugiau nei penkios valstybės narės, jie sprendimus priima kvalifikuota balsų dauguma. Balsuojant dėl 6 straipsnio 2 dalyje išvardytų pasiūlymų kvalifikuotą balsų daugumą sudaro:

a) PSO, atstovaujantys ne mažiau kaip 72 % susijusių valstybių narių, ir

b) PSO, atstovaujantys valstybėms narėms, kurių gyventojai sudaro ne mažiau kaip 65 % atitinkamo regiono gyventojų.

4. Sprendimus dėl planų pasiūlymų blokuojančią mažumą sudaro bent minimalus skaičius PSO, atstovaujančių daugiau kaip 35 % dalyvaujančių valstybių narių gyventojų, prie jo pridėjus PSO, atstovaujančių bent vienai papildomai susijusiai valstybei narei, skaičių; priešingu atveju laikoma, kad kvalifikuota balsų dauguma pasiekta.

5. Kai PSO priima sprendimus dėl nuostatų ir sąlygų arba metodikų pasiūlymų pagal 6 straipsnio 2 dalį, kiekvienai valstybei narei skiriamas vienas balsas. Jei valstybės narės teritorijoje yra daugiau nei vienas PSO, balsavimo teises PSO paskirsto valstybė narė.

6. Jei PSO, bendradarbiaudami su ES SSO subjektu, per šiame reglamente nustatytus terminus atitinkamoms kompetentingoms institucijoms nepateikia pradinio arba iš dalies pakeisto pasiūlymo dėl nuostatų ir sąlygų ar metodikų arba planų, jie toms institucijoms ir ACER pateikia atitinkamus nuostatų ir sąlygų ar metodikų arba planų projektus. Jie paaiškina, kodėl nepavyko pasiekti susitarimo. Kompetentingos institucijos kartu imasi atitinkamų veiksmų, kad būtų priimtos reikiamos nuostatos ir sąlygos ar metodikos arba reikiami planai. Tai gali būti daroma, pvz., prašant iš dalies pakeisti projektus pagal šią dalį, persvarstant ir užbaigiant tuos projektus arba, jei projektų nepateikta, nustatant ir patvirtinant reikiamas nuostatas ir sąlygas ar metodikas arba planus.

8 straipsnis

Pasiūlymų teikimas kompetentingoms institucijoms

1. PSO nuostatų ir sąlygų ar metodikų arba planų pasiūlymus atitinkamoms kompetentingoms institucijoms pateikia per atitinkamus 18, 23, 29, 33, 34, 35 ir 37 straipsniuose nustatytus terminus. Kompetentingos institucijos gali kartu pratęsti šiuos terminus išskirtinėmis aplinkybėmis, ypač tais atvejais, kai termino laikytis neįmanoma dėl su PSO arba su ES SSO subjektu nesusijusių aplinkybių.

2. Nuostatų ir sąlygų, metodikų arba planų pasiūlymai pagal 1 dalį pateikiami ACER susipažinti tuo pačiu metu, kaip ir kompetentingoms institucijoms.

3. NRI bendru prašymu ACER per šešis mėnesius nuo nuostatų ir sąlygų ar metodikų arba planų pasiūlymo gavimo pateikia nuomonę dėl jo ir apie ją praneša NRI ir kompetentingoms institucijoms. NRI, už kibernetinį saugumą atsakingos NKI ir visos kitos kompetentingomis institucijomis paskirtos institucijos tarpusavyje derina savo veiksmus prieš NRI prašant ACER pateikti nuomonę. ACER į tokią nuomonę gali įtraukti rekomendacijas. Prieš pateikdama nuomonę dėl 6 straipsnio 2 dalyje išvardytų pasiūlymų, ACER konsultuojasi su ENISA.

4. Kompetentingos institucijos konsultuojasi, glaudžiai bendradarbiauja ir koordinuoja veiksmus tarpusavyje, kad pasiektų susitarimą dėl siūlomų nuostatų ir sąlygų, metodikų arba planų. Prieš patvirtindamos nuostatas ir sąlygas ar metodikas arba planus, jos, pasikonsultavusios su ENTSO-E ir ES SSO subjektu, prireikus pataiso ir užbaigia pasiūlymus, siekdamos užtikrinti, kad jie atitiktų šį reglamentą ir padėtų užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje.

5. Kompetentingos institucijos sprendimą dėl nuostatų ir sąlygų ar metodikų arba planų priima per šešis mėnesius nuo tada, kai nuostatas ir sąlygas ar metodikas arba planus gauna atitinkama kompetentinga institucija arba, kai taikytina, paskutinė atitinkama kompetentinga institucija.

6. Kai ACER pateikia nuomonę, atitinkamos kompetentingos institucijos į tą nuomonę atsižvelgia ir priima savo sprendimus per šešis mėnesius nuo ACER nuomonės gavimo.

7. Jeigu kompetentingos institucijos kartu pareikalauja iš dalies pakeisti siūlomas nuostatas ir sąlygas ar metodikas arba planus, kad juos patvirtintų, PSO, bendradarbiaudami su ES SSO subjektu, parengia pasiūlymą dėl tokio nuostatų ir sąlygų ar metodikų arba planų keitimo. PSO iš dalies pakeistą pasiūlymą pateikia tvirtinti per du mėnesius nuo kompetentingų institucijų prašymo gavimo. Kompetentingos institucijos sprendimą dėl iš dalies pakeistų nuostatų ir sąlygų ar metodikų arba planų priima per du mėnesius nuo jų pateikimo.

8. Jei per 5 arba 7 dalyje nurodytą laikotarpį kompetentingoms institucijoms susitarti nepavyksta, jos apie tai praneša Komisijai. Komisija gali imtis tinkamų veiksmų, kad būtų galima patvirtinti reikiamas nuostatas ir sąlygas ar metodikas arba planus.

9. PSO, padedami ENTSO-E ir ES SSO subjekto, savo interneto svetainėse paskelbia nuostatas ir sąlygas ar metodikas arba planus, kai juos patvirtina atitinkamos kompetentingos institucijos, išskyrus atvejus, kai pagal 47 straipsnį tokia informacija laikoma konfidencialia.

10. Kompetentingos institucijos gali kartu prašyti PSO ir ES SSO subjekto pateikti pasiūlymus iš dalies pakeisti patvirtintas nuostatas ir sąlygas ar metodikas arba patvirtintus planus ir nustatyti tų pasiūlymų pateikimo terminą. PSO, bendradarbiaudami su ES SSO subjektu, gali siūlyti pakeitimus kompetentingoms institucijoms ir savo iniciatyva. Pasiūlymai iš dalies pakeisti nuostatas ir sąlygas ar metodikas arba planus rengiami ir tvirtinami šiame straipsnyje nustatyta tvarka.

11. Bent kas trejus metus nuo pirmojo atitinkamų nuostatų ir sąlygų arba metodikų arba atitinkamų planų patvirtinimo PSO, bendradarbiaudami su ES SSO subjektu, peržiūri patvirtintų nuostatų ir sąlygų ar metodikų arba planų veiksmingumą ir nepagrįstai nedelsdami praneša peržiūros išvadas kompetentingoms institucijoms ir ACER.

9 straipsnis

Konsultacijos

1. PSO, padedami ENTSO-E ir bendradarbiaudami su ES SSO subjektu, konsultuojasi su suinteresuotaisiais subjektais, įskaitant ACER, ENISA ir kiekvienos valstybės narės kompetentingą instituciją, dėl 6 straipsnio 2 dalyje išvardytų nuostatų ir sąlygų arba metodikų ir 6 straipsnio 3 dalyje nurodytų planų pasiūlymų projektų. Konsultacijos trunka ne trumpiau kaip vieną mėnesį.

2. 6 straipsnio 2 dalyje išvardytų nuostatų ir sąlygų arba metodikų pasiūlymai, kuriuos PSO pateikia bendradarbiaudami su ES SSO subjektu, skelbiami ir pateikiami konsultuotis Sąjungos lygmeniu. 6 straipsnio 3 dalyje nurodytų planų pasiūlymai, kuriuos PSO pateikia bendradarbiaudami su ES SSO subjektu, pateikiami konsultuotis bent regiono lygmeniu.

3. PSO, padedami ENTSO-E, ir ES SSO subjektas, atsakingas už nuostatų ir sąlygų ar metodikų arba planų pasiūlymą, prieš pateikdami jį tvirtinti reguliavimo institucijoms, tinkamai atsižvelgia į suinteresuotųjų subjektų nuomones, pareikštas per konsultacijas, surengtas pagal 1 dalį. Visais atvejais kartu su pasiūlymu pateikiamas ir laiku (prieš paskelbiant nuostatų ir sąlygų arba metodikų pasiūlymą arba tuo pačiu metu) paskelbiamas tvirtas sprendimo atsižvelgti arba neatsižvelgti į konsultacijų metu pareikštas nuomones pagrindimas.

10 straipsnis

Suinteresuotųjų subjektų dalyvavimas

ACER, glaudžiai bendradarbiaudama su ENTSO-E ir ES SSO subjektu, organizuoja suinteresuotųjų subjektų dalyvavimą, įskaitant reguliarius susitikimus su suinteresuotaisiais subjektais, kad nustatytų problemas ir pasiūlytų su šio reglamento įgyvendinimu susijusius patobulinimus.

11 straipsnis

Išlaidų susigrąžinimas

1. PSO ir SSO, kuriems taikomas tinklo tarifų reguliavimas, vykdant šiame reglamente nustatytas pareigas patiriamas išlaidas, įskaitant ENTSO-E ir ES SSO subjekto išlaidas, įvertina atitinkama kiekvienos valstybės narės NRI.

2. Išlaidos, įvertintos kaip pagrįstos, veiksmingos ir proporcingos, susigrąžinamos taikant tinklo tarifus ar kitus tinkamus mechanizmus, kuriuos nustato atitinkama NRI.

3. Atitinkamų NRI prašymu 1 dalyje nurodyti PSO ir SSO per NRI nustatytą pagrįstą laikotarpį pateikia informaciją, reikalingą patirtoms išlaidoms įvertinti.

12 straipsnis

Stebėsena

1. ACER stebi šio reglamento įgyvendinimą pagal Reglamento (ES) 2019/943 32 straipsnio 1 dalį ir Reglamento (ES) 2019/942 4 straipsnio 2 dalį. Vykdydama šią stebėseną ACER gali bendradarbiauti su ENISA ir prašyti ENTSO-E ir ES SSO subjekto paramos. ACER apie šio reglamento įgyvendinimą reguliariai informuoja Elektros energijos srities veiklos koordinavimo grupę ir TIS bendradarbiavimo grupę.

2. ACER bent kas trejus metus nuo šio reglamento įsigaliojimo skelbia ataskaitą, kurioje:

a) peržiūri taikytinų su didelio poveikio ir ypatingos svarbos poveikio subjektais susijusių kibernetinio saugumo rizikos valdymo priemonių įgyvendinimo padėtį;

b) nustato, ar siekiant išvengti rizikos elektros energijos sektoriui gali reikėti papildomų taisyklių dėl bendrų reikalavimų, planavimo, stebėsenos, ataskaitų teikimo ir krizių valdymo, ir

c) identifikuoja sritis, kurias persvarstant šį reglamentą reikėtų patobulinti, arba nustato nereglamentuojamas sritis ir naujus prioritetus, kurie gali atsirasti dėl technologinių pokyčių.

3. Iki 2025 m. birželio 13 d. ACER, bendradarbiaudama su ENISA ir pasikonsultavusi su ENTSO-E ir ES SSO subjektu, gali paskelbti gaires dėl ACER praneštinos stebėsenai vykdyti reikalingos informacijos, taip pat dėl jos rinkimo proceso ir dažnumo, grindžiamų pagal 5 dalį apibrėžtais veiklos rodikliais.

4. Kompetentingos institucijos gali susipažinti su atitinkama ACER turima informacija, kurią ji surinko pagal šį straipsnį.

5. ACER, bendradarbiaudama su ENISA ir padedama ENTSO-E ir ES SSO subjekto, paskelbia su tarpvalstybinių elektros energijos srautų kibernetinio saugumo aspektais susijusius neprivalomus veiklos rodiklius veiklos patikimumui įvertinti.

6. Šio reglamento 2 straipsnio 1 dalyje išvardyti subjektai pateikia ACER informaciją, kurios ACER reikia 2 dalyje išvardytoms užduotims atlikti.

13 straipsnis

Lyginamoji analizė

1. Iki 2025 m. birželio 13 d. ACER, bendradarbiaudama su ENISA, parengia neprivalomą kibernetinio saugumo lyginamosios analizės vadovą. Vadove NRI paaiškinami pagal šio straipsnio 2 dalį atliekamos įgyvendintų kibernetinio saugumo kontrolės priemonių lyginamosios analizės principai, atsižvelgiant į kontrolės įgyvendinimo sąnaudas ir tokiai kontrolei įgyvendinti naudojamų procesų, produktų, paslaugų, sistemų ir sprendinių funkcijų veiksmingumą. ACER, rengdama neprivalomą kibernetinio saugumo lyginamosios analizės vadovą, atsižvelgia į esamas lyginamosios analizės ataskaitas. Neprivalomą kibernetinio saugumo lyginamosios analizės vadovą ACER pateikia susipažinti NRI.

2. Per 12 mėnesių nuo lyginamosios analizės vadovo parengimo pagal 1 dalį NRI atlieka lyginamąją analizę, kad įvertintų, ar dabartinės investicijos į kibernetinį saugumą:

a) mažina poveikio tarpvalstybiniams elektros energijos srautams riziką;

b) duoda norimus rezultatus ir didina elektros energijos sistemų plėtojimo efektyvumą;

c) yra efektyvios ir integruotos į bendrą turto ir paslaugų viešąjį pirkimą.

3. Atlikdamos lyginamąją analizę, NRI gali atsižvelgti į ACER parengtą neprivalomą kibernetinio saugumo lyginamosios analizės vadovą ir visų pirma įvertina:

a) vidutines su kibernetiniu saugumu susijusias išlaidas, patiriamas siekiant sumažinti tarpvalstybinius elektros energijos srautus veikiančią riziką, ypač susijusią su didelio poveikio ir ypatingos svarbos poveikio subjektais;

b) bendradarbiaudamos su ENTSO-E ir ES SSO subjektu – vidutines kibernetinio saugumo paslaugų, sistemų ir produktų, kurie labai padeda gerinti ir užtikrinti kibernetinio saugumo rizikos valdymo priemones įvairiuose sistemos eksploatavimo regionuose, kainas;

c) šiam reglamentui įgyvendinti tinkamų kibernetinio saugumo paslaugų, sistemų ir sprendinių prieinamumą ir jų sąnaudų bei funkcijų palyginamumo lygį, nustatant galimas priemones, būtinas išlaidų efektyvumui didinti, visų pirma tais atvejais, kai gali reikėti investicijų į kibernetinio saugumo technologijas.

4. Visa su lyginamąja analize susijusi informacija tvarkoma ir apdorojama laikantis šiame reglamente nustatytų duomenų klasifikavimo reikalavimų, būtinosios kibernetinio saugumo kontrolės priemonių ir vadovaujantis tarpvalstybinių elektros energijos srautų kibernetinio saugumo rizikos vertinimo ataskaita. 2 ir 3 dalyse nurodyta lyginamoji analizė viešai neskelbiama.

5. Nedarant poveikio 47 straipsnyje išdėstytiems konfidencialumo reikalavimams ir būtinybei užtikrinti subjektų, kuriems taikomos šio reglamento nuostatos, saugumą, šio straipsnio 2 ir 3 dalyse nurodyta lyginamąja analize dalijamasi su visomis NRI, visomis kompetentingomis institucijomis, ACER, ENISA ir Komisija.

14 straipsnis

Susitarimai su PSO už Sąjungos ribų

1. Per 18 mėnesių nuo šio reglamento įsigaliojimo trečiosios valstybės kaimynystėje esančio sistemos eksploatavimo regiono PSO stengiasi su kaimyninės trečiosios valstybės PSO sudaryti susitarimus, kurie atitiktų aktualią Sąjungos teisę ir kuriuose būtų nustatytas bendradarbiavimo su tais PSO kibernetiniam saugumui užtikrinti pagrindas ir bendradarbiavimo kibernetinio saugumo srityje tvarka.

2. Apie susitarimus, sudarytus pagal 1 dalį, PSO informuoja kompetentingą instituciją.

15 straipsnis

Teisiniai atstovai

1. Subjektai, kurie nėra įsisteigę Sąjungoje, bet teikia paslaugas subjektams Sąjungoje ir kuriems pagal 24 straipsnio 6 dalį pranešta, kad jie yra didelio poveikio arba ypatingos svarbos poveikio subjektai, per tris mėnesius nuo to pranešimo gavimo raštu paskiria atstovą Sąjungoje ir apie tai informuoja pranešusiąją kompetentingą instituciją.

2. Šis įgaliotasis atstovas paskiriamas tam, kad bet kuri kompetentinga institucija arba CSIRT Sąjungoje dėl didelio poveikio ar ypatingos svarbos poveikio subjekto pareigų pagal šį reglamentą galėtų kreiptis ne tik į patį didelio poveikio ar ypatingos svarbos poveikio subjektą, bet ir į jo atstovą arba tik į atstovą. Didelio poveikio arba ypatingos svarbos poveikio subjektas savo teisiniam atstovui suteikia reikiamus įgaliojimus ir pakankamus išteklius, kad būtų užtikrintas veiksmingas ir savalaikis bendradarbiavimas su atitinkamomis kompetentingomis institucijomis arba CSIRT.

3. Atstovas turi būti įsisteigęs vienoje iš valstybių narių, kuriose subjektas siūlo savo paslaugas. Toks subjektas laikomas priklausančiu valstybės narės, kurioje yra įsisteigęs jo atstovas, jurisdikcijai. Didelio poveikio arba ypatingos svarbos poveikio subjektai savo teisinio atstovo vardą ir pavardę (pavadinimą), pašto adresą, e. pašto adresą ir telefono numerį nurodo valstybės narės, kurioje tas teisinis atstovas gyvena ar yra įsisteigęs, kompetentingai institucijai.

4. Paskirtą teisinį atstovą turi būti galima laikyti atsakingu dėl pareigų pagal šį reglamentą nevykdymo, nedarant poveikio paties didelio poveikio arba ypatingos svarbos poveikio subjekto atsakomybei ir teisiniams veiksmams, kurie gali būti inicijuojami prieš jį.

5. Jei Sąjungoje nėra pagal šį straipsnį paskirto atstovo, bet kuri valstybė narė, kurioje subjektas teikia paslaugas, gali imtis teisinių veiksmų prieš subjektą dėl šiame reglamente nustatytų pareigų nevykdymo.

6. Teisinio atstovo paskyrimas Sąjungoje pagal 1 dalį neprilyginamas įsisteigimui Sąjungoje.

16 straipsnis

ENTSO-E ir ES SSO subjekto bendradarbiavimas

1. ENTSO-E ir ES SSO subjektas bendradarbiauja atlikdami kibernetinio saugumo rizikos vertinimus pagal 19 ir 21 straipsnius ir visų pirma vykdydami šias užduotis:

a) rengdami kibernetinio saugumo rizikos vertinimo metodikas pagal 18 straipsnio 1 dalį;

b) rengdami išsamaus tarpvalstybinių elektros energijos srautų kibernetinio saugumo rizikos vertinimo ataskaitą pagal 23 straipsnį;

c) kurdami bendrą elektros energijos kibernetinio saugumo sistemą pagal III skyrių;

d) rengdami kibernetinio saugumo viešojo pirkimo rekomendaciją pagal 35 straipsnį;

e) rengdami kibernetinių išpuolių klasifikavimo skalės metodiką pagal 37 straipsnio 8 dalį;

f) rengdami preliminarų kibernetinių incidentų poveikio elektros energijos srautams indeksą (KIPEI) pagal 48 straipsnio 1 dalies a punktą;

g) rengdami preliminarų konsoliduotą didelio poveikio ir ypatingos svarbos poveikio subjektų sąrašą pagal 48 straipsnio 3 dalį;

h) rengdami preliminarų Sąjungos masto didelio poveikio ir ypatingos svarbos poveikio procesų sąrašą pagal 48 straipsnio 4 dalį;

i) rengdami preliminarų Europos ir tarptautinių standartų ir kontrolės priemonių sąrašą pagal 48 straipsnio 6 dalį;

j) atlikdami Sąjungos masto kibernetinio saugumo rizikos vertinimą pagal 19 straipsnį;

k) atlikdami regioninius kibernetinio saugumo rizikos vertinimus pagal 21 straipsnį;

l) nustatydami regioninius kibernetinio saugumo rizikos mažinimo planus pagal 22 straipsnį;

m) rengdami gaires dėl IRT produktams, paslaugoms ir procesams taikomų Europos kibernetinio saugumo sertifikavimo schemų pagal 36 straipsnį;

n) rengdami šio reglamento įgyvendinimo gaires, konsultuodamiesi su ACER ir ENISA.

2. ENTSO-E ir ES SSO subjekto bendradarbiavimas gali būti vykdomas kibernetinio saugumo rizikos darbo grupės forma.

3. ENTSO-E ir ES SSO subjektas reguliariai informuoja ACER, ENISA, TIS bendradarbiavimo grupę ir Elektros energijos srities veiklos koordinavimo grupę apie pažangą, padarytą įgyvendinant Sąjungos masto ir regioninius kibernetinio saugumo rizikos vertinimus pagal 19 ir 21 straipsnius.

17 straipsnis

ACER ir kompetentingų institucijų bendradarbiavimas

ACER, bendradarbiaudama su kiekviena kompetentinga institucija, stebi:

(1) kibernetinio saugumo valdymo priemonių įgyvendinimą pagal 12 straipsnio 2 dalies a punktą ir ataskaitų teikimo pareigų vykdymą pagal 27 ir 39 straipsnius ir

(2) nuostatų ir sąlygų, metodikų arba planų priėmimo procesą ir įgyvendinimą pagal 6 straipsnio 2 ir 3 dalis. ACER, ENISA ir kiekvienos kompetentingos institucijos bendradarbiavimas gali būti vykdomas kibernetinio saugumo rizikos stebėsenos įstaigos forma.

II SKYRIUS

RIZIKOS VERTINIMAS IR ATITINKAMOS KIBERNETINIO SAUGUMO RIZIKOS IDENTIFIKAVIMAS

18 straipsnis

Kibernetinio saugumo rizikos vertinimo metodikos

1. Iki 2025 m. skovo 13 d. PSO, padedami ENTSO-E, bendradarbiaudami su ES SSO subjektu ir pasikonsultavę su TIS bendradarbiavimo grupe, pateikia Sąjungos, regioninio ir valstybių narių lygmens kibernetinio saugumo rizikos vertinimo metodikų pasiūlymus.

2. Į Sąjungos, regioninio ir valstybių narių lygmens kibernetinio saugumo rizikos vertinimo metodikas įtraukiama:

a) kibernetinių grėsmių, į kurias reikia atsižvelgti, sąrašas, į kurį įtraukiamos bent šios tiekimo grandinės grėsmės:

i) didelis ir netikėtas tiekimo grandinės sutrikimas;

ii) IRT produktų, paslaugų ar procesų neprieinamumas tiekimo grandinėje;

iii) kibernetiniai išpuoliai, inicijuoti per tiekimo grandinės dalyvius;

iv) neskelbtinos informacijos nutekėjimas tiekimo grandinėje, įskaitant tiekimo grandinės sekimą;

v) per tiekimo grandinės dalyvius IRT produktuose, paslaugose ar procesuose įdiegiami trūkumai ar užpakalinės durys;

b) kriterijai, pagal kuriuos kibernetinio saugumo rizika vertinama kaip didelė arba kritinė, naudojant nustatytus padarinių ir tikimybės slenksčius;

c) kibernetinio saugumo rizikos, kylančios dėl senųjų sistemų, grandininio kibernetinių išpuolių poveikio ir tinklo eksploatavimo sistemų tikralaikiškumo, analizės metodas;

d) kibernetinio saugumo rizikos, kylančios dėl priklausomybės nuo vienintelio IRT produktų, paslaugų ar procesų tiekėjo, analizės metodas.

3. Sąjungos, regioninio ir valstybių narių lygmens kibernetinio saugumo rizikos vertinimo metodikose kibernetinio saugumo rizika vertinama pagal tą pačią rizikos poveikio matricą. Rizikos poveikio matricoje:

a) įvertinami kibernetinių išpuolių padariniai pagal šiuos kriterijus:

i) apkrovos praradimas;

ii) elektros energijos gamybos sumažėjimas;

iii) pirminio dažnio rezervo pajėgumo praradimas;

iv) pajėgumo atkurti elektros tinklo veikimą po visiško arba dalinio išjungimo nesiremiant išoriniu perdavimo tinklu (paleidimas po visuotinės avarijos) praradimas;

v) numatoma elektros energijos tiekimo vartotojams atjungimo trukmė ir mastas pagal vartotojų skaičių ir

vi) visi kiti kiekybiniai ar kokybiniai kriterijai, kurie pagrįstai galėtų būti kibernetinio išpuolio poveikio tarpvalstybiniams elektros energijos srautams rodiklis;

b) įvertinama incidento tikimybė kaip kibernetinių išpuolių dažnumas per metus.

4. Sąjungos lygmens kibernetinio saugumo rizikos vertinimo metodikose aprašoma, kaip bus nustatytos didelio poveikio ir ypatingos svarbos poveikio slenksčių KIPEI vertės. KIPEI turi užtikrinti galimybę subjektams įvertinti rizikos poveikį savo veiklos procesui pagal 2 dalies b punkte nurodytus kriterijus, atliekant poveikio veiklai vertinimus pagal 26 straipsnio 4 dalies c punkto i papunktį.

5. ENTSO-E, koordinuodamas veiksmus su ES SSO subjektu, informuoja Elektros energijos srities veiklos koordinavimo grupę apie kibernetinio saugumo rizikos vertinimo metodikų, parengtų pagal 1 dalį, pasiūlymus.

19 straipsnis

Sąjungos masto kibernetinio saugumo rizikos vertinimas

1. Per 9 mėnesius nuo kibernetinio saugumo rizikos vertinimo metodikų patvirtinimo pagal 8 straipsnį ir vėliau kas trejus metus ENTSO-E, bendradarbiaudamas su ES SSO subjektu ir konsultuodamasis su TIS bendradarbiavimo grupe, atlieka, nedarant poveikio Direktyvos (ES) 2022/2555 22 straipsnio taikymui, Sąjungos masto kibernetinio saugumo rizikos vertinimą ir parengia Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaitos projektą. Šiuo tikslu jie naudoja metodikas, parengtas pagal 18 straipsnį ir patvirtintas pagal 8 straipsnį, kad nustatytų, išanalizuotų ir įvertintų galimus kibernetinių išpuolių, veikiančių elektros energijos sistemos eksploatavimo saugumą ir sutrikdančių tarpvalstybinius elektros energijos srautus, padarinius. Atliekant Sąjungos masto kibernetinio saugumo rizikos vertinimą neatsižvelgiama į kibernetinių išpuolių teisinę, finansinę žalą ar žalą reputacijai.

2. Į Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaitą įtraukiami šie elementai:

a) Sąjungos masto didelio poveikio procesai ir Sąjungos masto ypatingos svarbos poveikio procesai;

b) rizikos poveikio matrica, kurią subjektai ir kompetentingos institucijos naudoja kibernetinio saugumo rizikai, identifikuotai valstybių narių lygmens kibernetinio saugumo rizikos vertinime, atliktame pagal 20 straipsnį, ir subjekto lygmens kibernetinio saugumo rizikos vertinime, atliktame pagal 26 straipsnio 2 dalies b punktą, įvertinti.

3. Aptariant Sąjungos masto didelio poveikio procesus ir Sąjungos masto ypatingos svarbos poveikio procesus, Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaitoje pateikiama:

a) galimų kibernetinio išpuolio padarinių vertinimas remiantis pagal 18 straipsnio 2, 3 ir 4 dalis parengtoje ir pagal 8 straipsnį patvirtintoje kibernetinio saugumo rizikos vertinimo metodikoje nustatytais rodikliais;

b) KIPEI ir didelio poveikio ir ypatingos svarbos poveikio slenksčiai, kuriuos kompetentingos institucijos naudoja pagal 24 straipsnio 1 ir 2 dalis, kad identifikuotų didelio poveikio ir ypatingos svarbos poveikio subjektus, dalyvaujančius Sąjungos masto didelio poveikio procesuose ir Sąjungos masto ypatingos svarbos poveikio procesuose.

4. ENTSO-E, bendradarbiaudamas su ES SSO subjektu, Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaitos projektą su Sąjungos masto kibernetinio saugumo rizikos vertinimo rezultatais pateikia ACER, kad ji pareikštų savo nuomonę. ACER nuomonę dėl ataskaitos projekto pateikia per tris mėnesius nuo jo gavimo. ENTSO-E ir ES SSO subjektas, rengdami galutinę tos ataskaitos redakciją, kuo labiau atsižvelgia į ACER nuomonę.

5. Per tris mėnesius nuo ACER nuomonės gavimo ENTSO-E, bendradarbiaudamas su ES SSO subjektu, galutinę Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaitą pateikia ACER, Komisijai, ENISA ir kompetentingoms institucijoms.

20 straipsnis

Valstybės narės kibernetinio saugumo rizikos vertinimas

1. Kiekviena kompetentinga institucija atlieka valstybės narės kibernetinio saugumo rizikos visiems didelio poveikio ir ypatingos svarbos poveikio subjektams vertinimą pagal metodikas, parengtas pagal 18 straipsnį ir patvirtintas pagal 8 straipsnį. Valstybės narės kibernetinio saugumo rizikos vertinime identifikuojama ir analizuojama kibernetinių išpuolių, paveikiančių elektros energijos sistemos eksploatavimo saugumą ir sutrikdančių tarpvalstybinius elektros energijos srautus, rizika. Atliekant valstybės narės kibernetinio saugumo rizikos vertinimą neatsižvelgiama į kibernetinių išpuolių teisinę, finansinę žalą ar žalą reputacijai.

2. Per 21 mėnesį nuo pranešimo apie didelio poveikio ir ypatingos svarbos poveikio subjektus pagal 24 straipsnio 6 dalį ir po to kas trejus metus, pasikonsultavusi su už elektros energijos srautų kibernetinį saugumą atsakinga NKI, kiekviena kompetentinga institucija, padedama CSIRT, pateikia ENTSO-E ir ES SSO subjektui valstybės narės kibernetinio saugumo rizikos vertinimo ataskaitą, kurioje pateikiama ši informacija apie kiekvieną didelio poveikio ir ypatingos svarbos poveikio veiklos procesą:

a) būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemonių įgyvendinimo pagal 29 straipsnį padėtis;

b) sąrašas visų kibernetinių išpuolių, apie kuriuos pranešta per ankstesnius trejus metus pagal 38 straipsnio 3 dalį;

c) informacijos apie kibernetines grėsmes, apie kurias pranešta per ankstesnius trejus metus pagal 38 straipsnio 6 dalį, santrauka;

d) kiekvieno Sąjungos masto didelio poveikio arba ypatingos svarbos poveikio proceso – informacijos ir atitinkamo turto konfidencialumo, vientisumo ir prieinamumo pažeidimo rizikos vertinimas;

e) kai reikia – papildomų subjektų, kurie pagal 24 straipsnio 1, 2, 3 ir 5 dalis identifikuoti kaip didelio poveikio arba ypatingos svarbos poveikio subjektai, sąrašas.

3. Valstybės narės kibernetinio saugumo rizikos vertinimo ataskaitoje atsižvelgiama į valstybės narės pasirengimo valdyti riziką planą, parengtą pagal Reglamento (ES) 2019/941 10 straipsnį.

4. Valstybės narės kibernetinio saugumo rizikos vertinimo ataskaitoje pagal 2 dalies a–d punktus pateikiama informacija nesiejama su konkrečiais subjektais ar turtu. Į valstybės narės kibernetinio saugumo rizikos vertinimo ataskaitą įtraukiamas ir laikinų nukrypti leidžiančių nuostatų, kurias valstybių narių kompetentingos institucijos leido taikyti pagal 30 straipsnį, rizikos vertinimas.

5. ENTSO-E ir ES SSO subjektas gali prašyti kompetentingų institucijų pateikti papildomos informacijos, susijusios su 2 dalies a ir c punktuose nurodytomis užduotimis.

6. Kompetentingos institucijos užtikrina, kad jų teikiama informacija būtų tiksli ir teisinga.

21 straipsnis

Regioniniai kibernetinio saugumo rizikos vertinimai

1. ENTSO-E, bendradarbiaudamas su ES SSO subjektu ir konsultuodamasis su atitinkamu regioniniu koordinavimo centru, atlieka kiekvieno sistemos eksploatavimo regiono kibernetinio saugumo rizikos vertinimą pagal metodikas, parengtas pagal 19 straipsnį ir patvirtintas pagal 8 straipsnį, kad identifikuotų, išanalizuotų ir įvertintų kibernetinių išpuolių, paveikiančių elektros energijos sistemos eksploatavimo saugumą ir sutrikdančių tarpvalstybinius elektros energijos srautus, riziką. Atliekant regioninius kibernetinio saugumo rizikos vertinimus neatsižvelgiama į kibernetinių išpuolių teisinę, finansinę žalą ar žalą reputacijai.

2. Per 30 mėnesių nuo pranešimo apie didelio poveikio ir ypatingos svarbos poveikio subjektus pagal 24 straipsnio 6 dalį ir po to kas trejus metus ENTSO-E, bendradarbiaudamas su ES SSO subjektu ir konsultuodamasis su TIS bendradarbiavimo grupe, parengia kiekvieno sistemos eksploatavimo regiono kibernetinio saugumo rizikos vertinimo ataskaitą.

3. Regioninio kibernetinio saugumo rizikos vertinimo ataskaitoje atsižvelgiama į aktualią informaciją, pateiktą Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaitose ir valstybių narių kibernetinio saugumo rizikos vertinimo ataskaitose.

4. Atliekant regioninį kibernetinio saugumo rizikos vertinimą atsižvelgiama į regioninius su kibernetiniu saugumu susijusius elektros energijos sektoriaus krizės scenarijus, nustatytus pagal Reglamento (ES) 2019/941 6 straipsnį.

22 straipsnis

Regioniniai kibernetinio saugumo rizikos mažinimo planai

1. Per 36 mėnesius nuo pranešimo apie didelio poveikio ir ypatingos svarbos poveikio subjektus pagal 24 straipsnio 6 dalį ir ne vėliau kaip 2031 m. birželio 13 d., o po to kas trejus metus PSO, padedami ENTSO-E, bendradarbiaudami su ES SSO subjektu ir konsultuodamiesi su regioniniais koordinavimo centrais ir TIS bendradarbiavimo grupe, parengia kiekvieno sistemos eksploatavimo regiono kibernetinio saugumo rizikos mažinimo planą.

2. Į regioninius kibernetinio saugumo rizikos mažinimo planus įtraukiama:

a) būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemonės, kurias sistemos eksploatavimo regione taiko didelio poveikio ir ypatingos svarbos poveikio subjektai;

b) liekamoji kibernetinio saugumo rizika sistemos eksploatavimo regionuose pritaikius a punkte nurodytas kontrolės priemones.

3. ENTSO-E regioninius rizikos mažinimo planus pateikia atitinkamiems perdavimo sistemos operatoriams, kompetentingoms institucijoms ir Elektros energijos srities veiklos koordinavimo grupei. Elektros energijos srities veiklos koordinavimo grupė gali rekomenduoti pakeitimų.

4. PSO, padedami ENTSO-E, bendradarbiaudami su ES SSO subjektu ir pasikonsultavę su TIS bendradarbiavimo grupe, atnaujina regioninius rizikos mažinimo planus kas trejus metus, nebent dėl aplinkybių juos reikėtų atnaujinti dažniau.

23 straipsnis

Išsamaus tarpvalstybinių elektros energijos srautų kibernetinio saugumo rizikos vertinimo ataskaita

1. Per 40 mėnesių nuo pranešimo apie didelio poveikio ir ypatingos svarbos poveikio subjektus pagal 24 straipsnio 6 dalį, o vėliau kas trejus metus PSO, padedami ENTSO-E, bendradarbiaudami su ES SSO subjektu ir pasikonsultavę su TIS bendradarbiavimo grupe, pateikia Elektros energijos srities veiklos koordinavimo grupei tarpvalstybinių elektros energijos srautų kibernetinio saugumo rizikos vertinimo rezultatų ataskaitą (toliau – išsamaus tarpvalstybinių elektros energijos srautų kibernetinio saugumo rizikos vertinimo ataskaita).

2. Išsamaus tarpvalstybinių elektros energijos srautų kibernetinio saugumo rizikos vertinimo ataskaita grindžiama Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaita, valstybių narių kibernetinio saugumo rizikos vertinimo ataskaitomis ir regioninio kibernetinio saugumo rizikos vertinimo ataskaitomis ir joje pateikiama ši informacija:

a) Sąjungos masto didelio poveikio ir ypatingos svarbos poveikio procesų, nustatytų Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaitoje pagal 19 straipsnio 2 dalies a punktą, sąrašas, įskaitant kibernetinio saugumo rizikos, įvertintos regioninio kibernetinio saugumo rizikos vertinimo ataskaitose pagal 21 straipsnio 2 dalį ir 19 straipsnio 3 dalies a punktą, tikimybės ir poveikio įvertinimą;

b) dabartinės kibernetinės grėsmės, ypač daug dėmesio skiriant elektros energijos sistemai kylančioms grėsmėms ir rizikai;

c) ankstesniojo laikotarpio kibernetiniai išpuoliai Sąjungos lygmeniu, kritiškai apžvelgiant, kaip tokie kibernetiniai išpuoliai galėjo paveikti tarpvalstybinius elektros energijos srautus;

d) bendra kibernetinio saugumo priemonių įgyvendinimo padėtis;

e) informacijos srautų įgyvendinimo pagal 37 ir 38 straipsnius padėtis;

f) informacijos sąrašas arba konkretūs informacijos klasifikavimo pagal 46 straipsnį kriterijai;

g) identifikuota ir akcentuota rizika, kuri gali kilti dėl nesaugaus tiekimo grandinės valdymo;

h) pagal 44 straipsnį organizuotų regioninių ir tarpregioninių kibernetinio saugumo pratybų rezultatai ir sukaupta patirtis;

i) bendros tarpvalstybinės kibernetinio saugumo rizikos elektros energijos sektoriuje raidos nuo paskutinių regioninių kibernetinio saugumo rizikos vertinimų analizė;

j) visa kita informacija, kuri gali būti naudinga nustatant galimus šio reglamento patobulinimus arba poreikį persvarstyti šį reglamentą ar bet kurią iš jo priemonių, ir

k) apibendrinta ir suanoniminta informacija apie nukrypti leidžiančias nuostatas, kuriomis leista pasinaudoti pagal 30 straipsnio 3 dalį.

3. 2 straipsnio 1 dalyje išvardyti subjektai gali padėti rengti išsamaus tarpvalstybinių elektros energijos srautų kibernetinio saugumo rizikos vertinimo ataskaitą, užtikrindami informacijos konfidencialumą pagal 47 straipsnį. PSO, padedami ENTSO-E ir bendradarbiaudami su ES SSO subjektu, konsultuojasi su šiais subjektais nuo ankstyvojo etapo.

4. Išsamaus tarpvalstybinių elektros energijos srautų kibernetinio saugumo rizikos vertinimo ataskaitai galioja informacijos, kuria keičiamasi, apsaugos taisyklės pagal 46 straipsnį. Nedarant poveikio 10 straipsnio 4 dalies ir 47 straipsnio 4 dalies taikymui, ENTSO-E ir ES SSO subjektas parengia viešą tos ataskaitos versiją, kurioje nėra informacijos, galinčios padaryti žalą 2 straipsnio 1 dalyje išvardytiems subjektams. Viešoji šios ataskaitos versija skelbiama tik gavus TIS bendradarbiavimo grupės ir Elektros energijos srities veiklos koordinavimo grupės sutikimą. ENTSO-E, koordinuodamas veiksmus su ES SSO subjektu, atsako už ataskaitos viešosios versijos parengimą ir paskelbimą.

24 straipsnis

Didelio poveikio ir ypatingos svarbos poveikio subjektų identifikavimas

1. Kiekviena kompetentinga institucija, naudodamasi KIPEI ir didelio poveikio ir ypatingos svarbos poveikio slenksčiais, įtrauktais į Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaitą pagal 19 straipsnio 3 dalies b punktą, identifikuoja didelio poveikio ir ypatingos svarbos poveikio subjektus savo valstybėje narėje, dalyvaujančius Sąjungos masto didelio poveikio ir ypatingos svarbos poveikio procesuose. Kompetentingos institucijos gali prašyti informacijos iš savo valstybėje narėje veikiančio subjekto, kad galėtų nustatyti jo KIPEI vertes. Jei nustatytas subjekto KIPEI viršija didelio poveikio arba ypatingos svarbos poveikio slenkstį, tas subjektas įtraukiamas į 20 straipsnio 2 dalyje nurodytoje valstybės narės kibernetinio saugumo rizikos vertinimo ataskaitoje pateikiamą sąrašą.

2. Kiekviena kompetentinga institucija, naudodamasi KIPEI ir didelio poveikio ir ypatingos svarbos poveikio slenksčiais, įtrauktais į Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaitą pagal 19 straipsnio 3 dalies b punktą, identifikuoja didelio poveikio ir ypatingos svarbos poveikio subjektus, kurie nėra įsisteigę Sąjungoje, bet joje veikia. Kompetentinga institucija gali prašyti informacijos iš Sąjungoje neįsisteigusio subjekto, kad galėtų nustatyti jo KIPEI vertes.

3. Kiekviena kompetentinga institucija gali identifikuoti papildomus subjektus savo valstybėje narėje kaip didelio poveikio arba ypatingos svarbos poveikio subjektus, jei jie atitinka šiuos kriterijus:

a) subjektas priklauso subjektų grupei, kurioje kyla didelė rizika, kad kibernetinis išpuolis subjektus paveiks tuo pačiu metu;

b) visos subjektų grupės KIPEI suvestinės vertės viršija didelio poveikio arba ypatingos svarbos poveikio slenkstį.

4. Jei kompetentinga institucija pagal 3 dalį identifikuoja papildomus subjektus, visi šių subjektų vykdomi procesai, kurių visos grupės suvestinis KIPEI viršija didelio poveikio slenkstį, laikomi didelio poveikio procesais, o visi šių subjektų vykdomi procesai, kurių visos grupės suvestiniai KIPEI viršija ypatingos svarbos poveikio slenkstį, laikomi ypatingos svarbos poveikio procesais.

5. Jei kompetentinga institucija identifikuoja 3 dalies a punkte nurodytus subjektus daugiau nei vienoje valstybėje narėje, ji informuoja kitas kompetentingas institucijas, ENTSO-E ir ES SSO subjektą. ENTSO-E, bendradarbiaudamas su ES SSO subjektu ir remdamasis iš visų kompetentingų institucijų gauta informacija, kompetentingoms institucijoms pateikia daugiau nei vienoje valstybėje narėje veikiančių subjektų santalkos, dėl kurios ne viename taške gali sutrikti tarpvalstybiniai elektros energijos srautai ir į kurią gali būti nukreiptas kibernetinis išpuolis, analizę. Jeigu kelių valstybių narių subjektų grupė identifikuojama kaip santalka, kurios KIPEI viršija didelio poveikio arba ypatingos svarbos poveikio slenkstį, visos susijusios kompetentingos institucijos, remdamosi suvestiniu subjektų grupės KIPEI, tokiai grupei priklausančius subjektus identifikuoja kaip didelio poveikio arba ypatingos svarbos poveikio subjektus atitinkamoje valstybėje narėje ir tie subjektai įtraukiami į Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaitą.

6. Kiekviena kompetentinga institucija per devynis mėnesius nuo ENTSO-E ir ES SSO subjekto pranešimo apie Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaitą pagal 19 straipsnio 5 dalį ir bet kuriuo atveju ne vėliau kaip 2028 m. birželio 13 d. praneša į sąrašą įtrauktiems subjektams, kad jie identifikuoti kaip didelio poveikio arba ypatingos svarbos poveikio subjektai jos valstybėje narėje.

7. Kai kompetentingai institucijai pagal 27 straipsnio c punktą pranešama, kad paslaugų teikėjas yra ypatingos svarbos IRT paslaugų teikėjas, ta kompetentinga institucija apie tai praneša valstybių narių, kurių teritorijoje yra būstinė arba atstovas, kompetentingoms institucijoms. Pastaroji kompetentinga institucija praneša paslaugų teikėjui, kad jis identifikuotas kaip ypatingos svarbos paslaugų teikėjas.

25 straipsnis

Nacionalinės patikros schemos

1. Kompetentingos institucijos gali nustatyti nacionalinę patikros schemą, skirtą patikrinti, ar pagal 24 straipsnio 1 dalį identifikuoti ypatingos svarbos poveikio subjektai įgyvendino nacionalinės teisės aktų sistemą, įtrauktą į 34 straipsnyje nurodytą atitikties matricą. Nacionalinė patikros schema gali būti grindžiama kompetentingos institucijos atliekamu patikrinimu, nepriklausomais saugumo auditais arba tos pačios valstybės narės ypatingos svarbos poveikio subjektų tarpusavio vertinimais, atliekamais prižiūrint kompetentingai institucijai.

2. Jei kompetentinga institucija nusprendžia nustatyti nacionalinę patikros schemą, ta kompetentinga institucija užtikrina, kad patikra būtų atliekama laikantis šių reikalavimų:

a) bet kuri tarpusavio vertinimą, auditą ar patikrinimą atliekanti šalis turi būti nepriklausoma nuo tikrinamo ypatingos svarbos poveikio subjekto ir neturėti interesų konfliktų;

b) tarpusavio vertinimą, auditą ar patikrinimą atliekantys darbuotojai turi turėti įrodomų žinių apie:

   i) kibernetinį saugumą elektros energijos sektoriuje;

   ii) kibernetinio saugumo valdymo sistemas;

   iii) audito principus;

   iv) kibernetinio saugumo rizikos vertinimą;

   v) bendrą elektros energijos srautų kibernetinio saugumo sistemą;

   vi) nacionalinės teisės aktų ir reguliavimo sistemą ir Europos bei tarptautinius standartus, susijusius su patikros apimtimi;

   vii) su patikros apimtimi susijusius ypatingos svarbos poveikio procesus;

c) tarpusavio vertinimą, auditą ar patikrinimą atliekančiai šaliai suteikiama pakankamai laiko šiai veiklai atlikti;

d) tarpusavio vertinimą, auditą ar patikrinimą atliekanti šalis imasi tinkamų priemonių, kad apsaugotų patikros metu surinktą informaciją, atsižvelgdama į jos konfidencialumo lygį, ir

e) tarpusavio vertinimai, auditai ar patikrinimai atliekami bent kartą per metus, o pagal visą patikros apimtį – bent kas trejus metus.

3. Jei kompetentinga institucija nusprendžia nustatyti nacionalinę patikros schemą, ji kasmet praneša ACER, kaip dažnai atliko patikrinimus pagal tą schemą.

26 straipsnis

Subjekto lygmens kibernetinio saugumo rizikos valdymas

1. Kiekvienas didelio poveikio ir ypatingos svarbos poveikio subjektas, kurį kompetentingos institucijos identifikavo pagal 24 straipsnio 1 dalį, valdo viso savo turto kibernetinio saugumo riziką savo didelio poveikio ir ypatingos svarbos poveikio perimetruose. Kiekvienas didelio poveikio ir ypatingos svarbos poveikio subjektas kas trejus metus atlieka rizikos valdymą, kurį sudaro 2 dalyje nurodyti etapai.

2. Kiekvienas didelio poveikio ir ypatingos svarbos poveikio subjektas savo kibernetinio saugumo rizikos valdymą grindžia metodu, kuriuo apsaugomos jo tinklų ir informacinės sistemos; rizikos valdymą sudaro šie etapai:

a) konteksto nustatymas;

b) subjekto lygmens kibernetinio saugumo rizikos vertinimas;

c) veiksmai su kibernetinio saugumo rizika;

d) kibernetinio saugumo rizikos priėmimas.

3. Konteksto nustatymo etapu kiekvienas didelio poveikio ir ypatingos svarbos poveikio subjektas:

a) nustato kibernetinio saugumo rizikos vertinimo apimtį, apimančią ENTSO-E ir ES SSO subjekto identifikuotus didelio poveikio ir ypatingos svarbos poveikio procesus, taip pat kitus procesus, kurie gali būti didelį arba ypatingos svarbos poveikį tarpvalstybiniams elektros energijos srautams turinčių kibernetinių išpuolių taikiniai, ir

b) nustato rizikos vertinimo ir rizikos priimtinumo kriterijus pagal 19 straipsnio 2 dalyje nurodytą rizikos poveikio matricą, kurią subjektai ir kompetentingos institucijos naudoja kibernetinio saugumo rizikai įvertinti Sąjungos, regioninio ir valstybių narių lygmens kibernetinio saugumo rizikos vertinimo metodikose, kurias parengia ENTSO-E ir ES SSO subjektas.

4. Kibernetinio saugumo rizikos vertinimo etapu kiekvienas didelio poveikio ir ypatingos svarbos poveikio subjektas:

a) identifikuoja kibernetinio saugumo riziką, atsižvelgdamas į:

i) visą turtą, kuriuo remiami Sąjungos masto didelio poveikio ir ypatingos svarbos poveikio procesai, įvertindamas galimą poveikį tarpvalstybiniams elektros energijos srautams, jei turtui iškiltų pavojus;

ii) galimas kibernetines grėsmes, atsižvelgdamas į kibernetines grėsmes, identifikuotas naujausioje išsamaus tarpvalstybinių elektros energijos srautų kibernetinio saugumo rizikos vertinimo ataskaitoje, nurodytoje 23 straipsnyje, ir į grėsmes tiekimo grandinėje;

iii) pažeidžiamumą, įskaitant senųjų sistemų pažeidžiamumą;

iv) galimus kibernetinių išpuolių scenarijus, įskaitant kibernetinius išpuolius, paveikiančius elektros energijos sistemos eksploatavimo saugumą ir sutrikdančius tarpvalstybinius elektros energijos srautus;

v) Sąjungos lygmeniu atliktus aktualius rizikos vertinimus, įskaitant koordinuojamus ypatingos svarbos tiekimo grandinių rizikos vertinimus pagal Direktyvos (ES) 2022/2555 22 straipsnį, ir

vi) įgyvendintas kontrolės priemones;

b) išanalizuoja a punkte identifikuotos kibernetinio saugumo rizikos tikimybę ir padarinius ir nustato kibernetinio saugumo rizikos lygį pagal 19 straipsnio 2 dalyje nurodytą rizikos poveikio matricą, naudojamą kibernetinio saugumo rizikai vertinti Sąjungos, regioninio ir valstybių narių lygmens kibernetinio saugumo rizikos vertinimo metodikose, kurias parengia PSO, padedami ENTSO-E ir bendradarbiaudami su ES SSO subjektu;

c) suklasifikuoja turtą pagal galimus padarinius, jei kiltų pavojus kibernetiniam saugumui, ir nustato didelio poveikio ir ypatingos svarbos poveikio perimetrus atlikdamas šiuos veiksmus:

i) naudodamas KIPEI atlieka visų procesų, kuriems taikomas kibernetinio saugumo rizikos vertinimas, poveikio veiklai vertinimą;

ii) priskiria procesą prie didelio poveikio procesų arba ypatingos svarbos poveikio procesų, jei jo KIPEI viršija atitinkamai didelio poveikio arba ypatingos svarbos poveikio slenkstį;

iii) nustato, kad visas didelio poveikio ir ypatingos svarbos poveikio turtas yra būtinas atitinkamai didelio poveikio ir ypatingos svarbos poveikio procesams;

iv) nustato didelio poveikio ir ypatingos svarbos poveikio perimetrus, apimančius atitinkamai visą didelio poveikio ir ypatingos svarbos poveikio turtą, kad būtų galima kontroliuoti prieigą prie perimetrų;

d) įvertina įvairių rūšių kibernetinio saugumo rizikos pirmenybę pagal rizikos vertinimo kriterijus ir rizikos priimtinumo kriterijus, nurodytus 3 dalies b punkte.

5. Veiksmų su kibernetinio saugumo rizika etapu kiekvienas didelio poveikio ir ypatingos svarbos poveikio subjektas parengia subjekto lygmens rizikos mažinimo planą, pasirinkdamas veiksmų su rizika galimybes, tinkamas rizikai valdyti ir liekamajai rizikai nustatyti.

6. Kibernetinio saugumo rizikos priėmimo etapu kiekvienas didelio poveikio ir ypatingos svarbos poveikio subjektas nusprendžia, ar priimti liekamąją riziką, remdamasis pagal 3 dalies b punktą nustatytais rizikos priimtinumo kriterijais.

7. Kiekvienas didelio poveikio ir ypatingos svarbos poveikio subjektas 1 dalyje nurodytą turtą registruoja turto inventoriuje. Tas turto inventorius nėra rizikos vertinimo ataskaitos dalis.

8. Kompetentinga institucija patikrinimų metu gali tikrinti inventoriuje nurodytą turtą.

27 straipsnis

Subjekto lygmens rizikos vertinimo ataskaitų teikimas

Kiekvienas didelio poveikio ir ypatingos svarbos poveikio subjektas per 12 mėnesių nuo pranešimo apie didelio poveikio ir ypatingos svarbos poveikio subjektus pagal 24 straipsnio 6 dalį ir vėliau kas trejus metus kompetentingai institucijai pateikia ataskaitą, kurioje nurodoma ši informacija:

1) sąrašas kontrolės priemonių, atrinktų įtraukti į subjekto lygmens rizikos mažinimo planą pagal 26 straipsnio 5 dalį, nurodant dabartinę kiekvienos kontrolės priemonės įgyvendinimo padėtį;

2) kiekvieno Sąjungos masto didelio poveikio arba ypatingos svarbos poveikio proceso – informacijos ir atitinkamo turto konfidencialumo, vientisumo ir prieinamumo pažeidimo rizikos vertinimas. Šios rizikos įvertis pateikiamas pagal 19 straipsnio 2 dalyje nurodytą rizikos poveikio matricą;

3) jų ypatingos svarbos poveikio procesams reikalingų ypatingos svarbos IRT paslaugų teikėjų sąrašas.

III SKYRIUS

BENDRA ELEKTROS ENERGIJOS SRAUTŲ KIBERNETINIO SAUGUMO SISTEMA

28 straipsnis

Bendros elektros energijos srautų kibernetinio saugumo sistemos sandara, veikimas ir peržiūra

1. Bendrą elektros energijos srautų kibernetinio saugumo sistemą sudaro šios kontrolės priemonės ir kibernetinio saugumo valdymo sistema:

a) pagal 29 straipsnį parengtos būtinosios kibernetinio saugumo kontrolės priemonės;

b) pagal 29 straipsnį parengtos sustiprintos kibernetinio saugumo kontrolės priemonės;

c) pagal 34 straipsnį parengta atitikties matrica, kuria a ir b punktuose nurodytos kontrolės priemonės susiejamos su atrinktais Europos ir tarptautiniais standartais ir nacionalinės teisės aktų ar reguliavimo sistemomis;

d) pagal 32 straipsnį sukurta kibernetinio saugumo valdymo sistema.

2. Visi didelio poveikio subjektai savo didelio poveikio perimetre taiko būtinosios kibernetinio saugumo kontrolės priemones pagal 1 dalies a punktą.

3. Visi ypatingos svarbos poveikio subjektai savo ypatingos svarbos poveikio perimetre taiko sustiprintos kibernetinio saugumo kontrolės priemones pagal 1 dalies b punktą.

4. Per 7 mėnesius nuo pirmosios Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaitos projekto pateikimo pagal 19 straipsnio 4 dalį 1 dalyje nurodyta bendra elektros energijos srautų kibernetinio saugumo sistema papildoma būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemonėmis tiekimo grandinėje, parengtomis pagal 33 straipsnį.

29 straipsnis

Būtinoji ir sustiprinta kibernetinio saugumo kontrolė

1. Per 7 mėnesius nuo pirmosios Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaitos projekto pateikimo pagal 19 straipsnio 4 dalį PSO, padedami ENTSO-E ir bendradarbiaudami su ES SSO subjektu, parengia būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemonių pasiūlymą.

2. Per 6 mėnesius nuo kiekvienos regioninio kibernetinio saugumo rizikos vertinimo ataskaitos projekto pateikimo pagal 21 straipsnio 2 dalį PSO, padedami ENTSO-E ir bendradarbiaudami su ES SSO subjektu, pasiūlo kompetentingai institucijai būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemonių pakeitimus. Pasiūlymas pateikiamas pagal 8 straipsnio 10 dalį ir jame atsižvelgiama į riziką, identifikuotą regioniniame rizikos vertinime.

3. Būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemones turi būti įmanoma patikrinti dalyvaujant nacionalinėje patikros schemoje pagal 31 straipsnyje nustatytą procedūrą arba pavedant trečiajai šaliai atlikti nepriklausomą saugumo auditą, atitinkantį 25 straipsnio 2 dalyje išvardytus reikalavimus.

4. Pagal 1 dalį parengtos pradinės būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemonės grindžiamos rizika, identifikuota 19 straipsnio 5 dalyje nurodytoje Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaitoje. Pagal 2 dalį parengtos būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemonės iš dalies keičiamos remiantis 21 straipsnio 2 dalyje nurodyta regioninio kibernetinio saugumo rizikos vertinimo ataskaita.

5. Būtinosios kibernetinio saugumo kontrolės priemonės apima kontrolės priemones informacijai, kuria keičiamasi pagal 46 straipsnį, apsaugoti.

6. Per 12 mėnesių po būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemonių patvirtinimo pagal 8 straipsnio 5 dalį arba po kiekvieno jų atnaujinimo pagal 8 straipsnio 10 dalį 2 straipsnio 1 dalyje išvardyti subjektai, pagal 24 straipsnį identifikuoti kaip ypatingos svarbos poveikio ir didelio poveikio subjektai, subjekto lygmens rizikos mažinimo plano rengimo pagal 26 straipsnio 5 dalį metu didelio poveikio perimetre pradeda taikyti būtinosios kibernetinio saugumo kontrolės priemones, o ypatingos svarbos poveikio perimetre – sustiprintos kibernetinio saugumo kontrolės priemones.

30 straipsnis

Nuostatos, leidžiančios nukrypti nuo reikalavimo taikyti būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemones

1. 2 straipsnio 1 dalyje išvardyti subjektai gali prašyti atitinkamos kompetentingos institucijos leisti nukrypti nuo pareigos taikyti 29 straipsnio 6 dalyje nurodytas būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemones. Kompetentinga institucija gali leisti pasinaudoti tokia nukrypti leidžiančia nuostata dėl vienos iš šių priežasčių:

a) išimtinėmis aplinkybėmis, kai subjektas gali įrodyti, kad tinkamos kibernetinio saugumo kontrolės įgyvendinimo išlaidos gerokai viršija naudą. ACER ir ENTSO-E, bendradarbiaudami su SSO subjektu, gali kartu parengti kibernetinio saugumo kontrolės išlaidų vertinimo gaires, kad padėtų subjektams;

b) kai subjektas pateikia subjekto lygmens veiksmų su rizika planą, kuriuo kibernetinio saugumo rizika naudojant alternatyvias kontrolės priemones sumažinama iki lygio, priimtino pagal 26 straipsnio 3 dalies b punkte nurodytus rizikos priimtinumo kriterijus.

2. Per tris mėnesius nuo 1 dalyje nurodyto prašymo gavimo kiekviena kompetentinga institucija nusprendžia, ar leisti pasinaudoti nuo reikalavimo taikyti būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemones nukrypti leidžiančia nuostata. Leidimas pasinaudoti nuo reikalavimo taikyti būtinosios arba sustiprintos kibernetinio saugumo kontrolės priemones nukrypti leidžiančia nuostata suteikiamas ne ilgiau kaip trejiems metams su galimybe jį pratęsti.

3. Apibendrinta ir suanoniminta informacija apie leidimus pasinaudoti nukrypti leidžiančiomis nuostatomis įtraukiama kaip priedas į 23 straipsnyje nurodytą išsamaus tarpvalstybinių elektros energijos srautų kibernetinio saugumo rizikos vertinimo ataskaitą. Prireikus ENTSO-E ir ES SSO subjektas kartu atnaujina sąrašą.

31 straipsnis

Bendros elektros energijos srautų kibernetinio saugumo sistemos patikra

1. Ne vėliau kaip praėjus 24 mėnesiams nuo 28 straipsnio 1 dalies a, b ir c punktuose nurodytų kontrolės priemonių patvirtinimo ir to straipsnio d punkte nurodytos kibernetinio saugumo valdymo sistemos sukūrimo kiekvienas pagal 24 straipsnio 1 dalį identifikuotas ypatingos svarbos poveikio subjektas kompetentingos institucijos prašymu turi gebėti įrodyti, kad laikosi kibernetinio saugumo valdymo sistemos ir būtinosios arba sustiprintos kibernetinio saugumo kontrolės priemonių.

2. Kiekvienas ypatingos svarbos poveikio subjektas vykdo 1 dalyje nurodytą pareigą pavesdamas trečiajai šaliai atlikti nepriklausomą saugumo auditą, atitinkantį 25 straipsnio 2 dalyje išvardytus reikalavimus, arba dalyvaudamas nacionalinėje patikros schemoje pagal 25 straipsnio 1 dalį.

3. Patikra, ar ypatingos svarbos poveikio subjektas laikosi kibernetinio saugumo valdymo sistemos ir būtinosios arba sustiprintos kibernetinio saugumo kontrolės priemonių, apima visą turtą, kurį apima ypatingos svarbos poveikio subjekto ypatingos svarbos poveikio perimetras.

4. Patikra, ar ypatingos svarbos poveikio subjektas laikosi kibernetinio saugumo valdymo sistemos ir būtinosios arba sustiprintos kibernetinio saugumo kontrolės priemonių, pakartojama ne vėliau kaip praėjus 36 mėnesiams po pirmosios patikros ir po to reguliariai kartojama kas trejus metus.

5. Kiekvienas pagal 24 straipsnį identifikuotas ypatingos svarbos poveikio subjektas įrodo, kad laikosi 28 straipsnio 1 dalies a, b ir c punktuose nurodytų kontrolės priemonių ir yra sukūręs to straipsnio d punkte nurodytą kibernetinio saugumo valdymo sistemą, kompetentingai institucijai pranešdamas atitikties patikros rezultatus.

32 straipsnis

Kibernetinio saugumo valdymo sistema

1. Per 24 mėnesius nuo kompetentingos institucijos pranešimo, kad pagal 24 straipsnio 6 dalį subjektas identifikuotas kaip didelio poveikio arba ypatingos svarbos poveikio subjektas, kiekvienas didelio poveikio ir ypatingos svarbos poveikio subjektas sukuria kibernetinio saugumo valdymo sistemą ir po to ją kas trejus metus peržiūri, siekdamas:

a) nustatyti kibernetinio saugumo valdymo sistemos taikymo sritį, atsižvelgdamas į sąsajas su kitais subjektais ir priklausomybę nuo jų;

b) užtikrinti, kad visa jo vyresnioji vadovybė būtų informuota apie atitinkamas teisines pareigas ir aktyviai prisidėtų prie kibernetinio saugumo valdymo sistemos įgyvendinimo laiku priimdama sprendimus ir greitai reaguodama;

c) užtikrinti kibernetinio saugumo valdymo sistemai būtinų išteklių prieinamumą;

d) nustatyti kibernetinio saugumo politiką, kuri dokumentuojama ir apie kurią pranešama subjekto viduje ir šalims, kurias veikia saugumo rizika;

e) priskirti atsakomybę už su kibernetiniu saugumu susijusias funkcijas ir apie ją pranešti;

f) vykdyti subjekto lygmens kibernetinio saugumo rizikos valdymą, kaip apibrėžta 26 straipsnyje;

g) nustatyti ir teikti išteklius, kurių reikia kibernetinio saugumo valdymo sistemai įgyvendinti, prižiūrėti ir nuolat tobulinti, atsižvelgdamas į būtiną kompetenciją ir informuotumą apie kibernetinio saugumo išteklius;

h) nustatyti vidaus ir išorės komunikaciją, kuri yra aktuali kibernetiniam saugumui;

i) kurti, atnaujinti ir kontroliuoti dokumentais pagrįstą informaciją, aktualią kibernetinio saugumo valdymo sistemai;

j) vertinti kibernetinio saugumo valdymo sistemos veikimą ir veiksmingumą;

k) planiniais intervalais atlikti vidaus auditą, siekdamas užtikrinti, kad kibernetinio saugumo valdymo sistema būtų veiksmingai įgyvendinama ir prižiūrima;

l) planiniais intervalais peržiūrėti kibernetinio saugumo valdymo sistemos įgyvendinimą ir kontroliuoti ir ištaisyti išteklių ir veiklos neatitiktį kibernetinio saugumo valdymo sistemos politikai, procedūroms ir gairėms.

2. Kibernetinio saugumo valdymo sistemos taikymo sritis apima visą turtą didelio poveikio ir ypatingos svarbos poveikio subjekto didelio poveikio ir ypatingos svarbos poveikio perimetre.

3. Kompetentingos institucijos, neprimesdamos ir nediskriminuodamos tam tikros rūšies technologijų naudojimo, skatina naudoti Europos ar tarptautinius standartus ir specifikacijas, susijusias su valdymo sistemomis ir aktualias tinklų ir informacinių sistemų saugumui.

33 straipsnis

Būtinoji ir sustiprinta kibernetinio saugumo kontrolė tiekimo grandinėje

1. Per 7 mėnesius nuo pirmosios Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaitos projekto pateikimo pagal 19 straipsnio 4 dalį PSO, padedami ENTSO-E ir bendradarbiaudami su ES SSO subjektu, parengia pasiūlymą dėl būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemonių tiekimo grandinėje, kuriomis būtų mažinama rizika tiekimo grandinėje, identifikuota atliekant Sąjungos masto kibernetinio saugumo rizikos vertinimus, ir kurios papildytų pagal 29 straipsnį parengtas būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemones. Būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemonės tiekimo grandinėje rengiamos kartu su būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemonėmis pagal 29 straipsnį. Būtinoji ir sustiprinta kibernetinio saugumo kontrolė tiekimo grandinėje apima visą visų IRT produktų, paslaugų ir procesų gyvavimo ciklą didelio poveikio arba ypatingos svarbos poveikio subjekto didelio poveikio arba ypatingos svarbos poveikio perimetruose. Rengiant pasiūlymą dėl būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemonių tiekimo grandinėje konsultuojamasi su TIS bendradarbiavimo grupe.

2. Būtinąją kibernetinio saugumo kontrolę tiekimo grandinėje sudaro didelio poveikio ir ypatingos svarbos poveikio subjektų kontrolės priemonės:

a) į kurias įtrauktos rekomenduojamos susijusių IRT produktų, paslaugų ir procesų viešojo pirkimo kibernetinio saugumo specifikacijos, kurios apima bent:

   i) asmens patikrinimus, taikomus tiekėjo darbuotojams, dalyvaujantiems tiekimo grandinėje ir dirbantiems su neskelbtina informacija arba turintiems prieigą prie subjekto didelio poveikio arba ypatingos svarbos poveikio turto. Asmens patikrinimas gali apimti subjekto darbuotojų ar rangovų tapatybės ir patikimumo patikrinimą pagal nacionalinę teisę ir procedūras bei aktualią ir taikytiną Sąjungos teisę, įskaitant Reglamentą (ES) 2016/679 ir Europos Parlamento ir Tarybos direktyvą (ES) 2016/680 ([18]). Asmens patikrinimai turi būti proporcingi ir griežtai apsiriboti tuo, kas būtina. Jie atliekami vieninteliu tikslu – įvertinti galimą saugumo riziką atitinkamam subjektui. Jie turi būti proporcingi veiklos reikalavimams, informacijos, prie kurios bus suteikiama prieiga, neskelbtinumui ir numanomai rizikai ir juos gali atlikti pats subjektas, atranką vykdanti išorės įmonė arba tai gali būti valstybinis asmens patikimumo patikrinimas;

   ii) saugaus ir kontroliuojamo IRT produktų, paslaugų ir procesų projektavimo, kūrimo ir gamybos procesus, kuriais skatinamas IRT produktų, paslaugų ir procesų projektavimas ir kūrimas, apimantis tinkamas technines priemones kibernetiniam saugumui užtikrinti;

   iii) tinklų ir informacinių sistemų sandarą, kurioje įrenginiai nelaikomi patikimais, net jei jie yra saugiame perimetre, reikalaujama tikrinti visas gaunamas užklausas ir taikomas minimaliosios prieigos teisės principas;

   iv) tiekėjo prieigą prie subjekto turto;

([18]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (OL L 119, 2016 5 4, p. 89).

v) sutartines tiekėjo pareigas apsaugoti subjekto neskelbtiną informaciją ir apriboti prieigą prie jos;

vi) pagrindines kibernetinio saugumo viešųjų pirkimų specifikacijas tiekėjo subrangovams;

vii) kibernetinio saugumo specifikacijų taikymo atsekamumą nuo IRT produktų, paslaugų ar procesų kūrimo ir gamybos iki pateikimo;

viii) saugumo naujinių palaikymą per visą IRT produktų, paslaugų ar procesų naudojimo laikotarpį;

ix) teisę atlikti tiekėjo projektavimo, kūrimo ir gamybos procesų kibernetinio saugumo auditą ir

x) tiekėjo rizikos profilio vertinimą;

b) kuriomis reikalaujama, kad tokie subjektai, su tiekėjais, bendradarbiavimo partneriais ir kitomis tiekimo grandinės šalimis sudarydami sutartis, apimančias įprastą IRT produktų tiekimą, IRT paslaugų teikimą ir IRT procesus, taip pat neplanuotus įvykius ir aplinkybes, pvz., sutarčių nutraukimą ir perdavimą sutarties partnerio aplaidumo atvejais, atsižvelgtų į a punkte nurodytas viešojo pirkimo rekomendacijas;

c) kuriomis reikalaujama, kad tokie subjektai atsižvelgtų į atitinkamų koordinuojamų ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimų, atliktų pagal Direktyvos (ES) 2022/2555 22 straipsnio 1 dalį, rezultatus;

d) kurios apima kriterijus, pagal kuriuos atrenkami tiekėjai, kurie gali įvykdyti a punkte nurodytas kibernetinio saugumo specifikacijas ir kurių kibernetinio saugumo lygis atitinka jų tiekiamo IRT produkto, teikiamos IRT paslaugos ar IRT procesų kibernetinio saugumo riziką;

e) į kurias įtraukti kriterijai, pagal kuriuos būtų diversifikuojami IRT produktų tiekimo, paslaugų teikimo ir procesų šaltiniai ir mažinama susaistymo su pardavėju rizika;

f) į kurias įtraukti kriterijai, pagal kuriuos būtų reguliariai stebimos, peržiūrimos arba audituojamos tiekėjų vidaus veiklos procesų kibernetinio saugumo specifikacijos per visą kiekvieno IRT produkto, IRT paslaugos ir IRT proceso gyvavimo ciklą.

3. Kibernetinio saugumo viešojo pirkimo rekomendacijoje, nurodytoje 2 dalies a punkte, kibernetinio saugumo specifikacijoms didelio poveikio arba ypatingos svarbos poveikio subjektai taiko Europos Parlamento ir Tarybos direktyvoje 2014/24/ES ([19]) nustatytus viešųjų pirkimų principus pagal 35 straipsnio 4 dalį arba nustato savo specifikacijas, remdamiesi subjekto lygmens kibernetinio saugumo rizikos vertinimo rezultatais.

4. Sustiprintos kibernetinio saugumo kontrolės priemonės tiekimo grandinėje apima ypatingos svarbos poveikio subjektų kontrolės priemones, kuriomis siekiama viešojo pirkimo metu patikrinti, ar IRT produktai, paslaugos ir procesai, kurie bus naudojami kaip ypatingos svarbos poveikio turtas, atitinka kibernetinio saugumo specifikacijas. IRT produktas, paslauga arba procesas tikrinami taikant 31 straipsnyje nurodytą Europos kibernetinio saugumo sertifikavimo schemą arba vykdant subjekto pasirinktą ir organizuojamą tikrinimo veiklą. Tikrinimo veiklos išsamumas ir apimtis turi būti pakankami, kad būtų galima užtikrinti, jog IRT produktas, paslauga ar procesas gali būti naudojami rizikai, nustatytai atliekant subjekto lygmens rizikos vertinimą, sumažinti. Ypatingos svarbos poveikio subjektas dokumentais pagrindžia veiksmus, kurių imtasi nustatytai rizikai sumažinti.

5. Atitinkamo IRT produkto, paslaugų ir procesų viešajam pirkimui taikomos būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemonės tiekimo grandinėje. Būtinoji ir sustiprinta tiekimo grandinės kibernetinio saugumo kontrolė taikoma viešojo pirkimo procesams, kuriuos vykdo subjektai, pagal 24 straipsnį identifikuoti kaip ypatingos svarbos poveikio ir didelio poveikio subjektai, ir kurie pradedami praėjus šešiems mėnesiams nuo 29 straipsnyje nurodytų būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemonių patvirtinimo arba atnaujinimo.

([19]) 2014 m. vasario 26 d. Europos Parlamento ir Tarybos direktyva 2014/24/ES dėl viešųjų pirkimų, kuria panaikinama Direktyva 2004/18/EB (OL L 94, 2014 3 28, p. 65).

6. Per 6 mėnesius nuo kiekvienos regioninio kibernetinio saugumo rizikos vertinimo ataskaitos projekto pateikimo pagal 21 straipsnio 2 dalį PSO, padedami ENTSO-E ir bendradarbiaudami su ES SSO subjektu, pasiūlo kompetentingai institucijai būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemonių tiekimo grandinėje pakeitimus. Pasiūlymas pateikiamas pagal 8 straipsnio 10 dalį ir jame atsižvelgiama į riziką, identifikuotą regioniniame rizikos vertinime.

34 straipsnis

Elektros energijos srautų kibernetinio saugumo kontrolės priemonių ir standartų atitikties matrica

1. Per 7 mėnesius nuo pirmosios Sąjungos masto kibernetinio saugumo rizikos vertinimo ataskaitos projekto pateikimo pagal 19 straipsnio 4 dalį PSO, padedami ENTSO-E, bendradarbiaudami su ES SSO subjektu ir pasikonsultavę su ENISA, parengia pasiūlymą dėl matricos, pagal kurią 28 straipsnio 1 dalies a ir b punktuose nurodytos kontrolės priemonės susiejamos su atrinktais Europos ir tarptautiniais standartais, taip pat atitinkamomis techninėmis specifikacijomis (atitikties matrica). ENTSO-E ir ES SSO subjektas dokumentais patvirtina įvairių kontrolės priemonių lygiavertiškumą 28 straipsnio 1 dalies a ir b punktuose nustatytoms kontrolės priemonėms.

2. Kompetentingos institucijos gali pateikti ENTSO-E ir ES SSO subjektui 28 straipsnio 1 dalies a ir b punktuose nustatytų kontrolės priemonių atitikties lentelę su nuoroda į susijusias nacionalinės teisės aktų ar reguliavimo sistemas, įskaitant aktualius valstybių narių nacionalinius standartus pagal Direktyvos (ES) 2022/2555 25 straipsnį. Jei valstybės narės kompetentinga institucija pateikia tokią atitikties lentelę, ENTSO-E ir ES SSO subjektas šią nacionalinę lentelę įtraukia į atitikties matricą.

3. Per 6 mėnesius nuo pirmosios regioninio kibernetinio saugumo rizikos vertinimo ataskaitos projekto pateikimo pagal 21 straipsnio 2 dalį PSO, padedami ENTSO-E, bendradarbiaudami su ES SSO subjektu ir pasikonsultavę su ENISA, pasiūlo kompetentingai institucijai atitikties matricos pakeitimus. Pasiūlymas pateikiamas pagal 8 straipsnio 10 dalį ir jame atsižvelgiama į riziką, identifikuotą regioniniame rizikos vertinime.

IV SKYRIUS

KIBERNETINIO SAUGUMO VIEŠOJO PIRKIMO REKOMENDACIJOS

35 straipsnis

Kibernetinio saugumo viešojo pirkimo rekomendacijos

1. PSO, padedami ENTSO-E ir bendradarbiaudami su ES SSO subjektu, darbo programoje, kuri turi būti parengta ir atnaujinama kiekvieną kartą, kai patvirtinama regioninio kibernetinio saugumo rizikos vertinimo ataskaita, parengia neprivalomų kibernetinio saugumo viešojo pirkimo rekomendacijų rinkinius, kuriais didelio poveikio ir ypatingos svarbos poveikio subjektai gali remtis pirkdami didelio poveikio ir ypatingos svarbos poveikio perimetrų IRT produktus, paslaugas ir procesus. Ši darbo programa apima:

a) didelio poveikio ir ypatingos svarbos poveikio subjektų didelio poveikio ir ypatingos svarbos poveikio perimetre naudojamų IRT produktų, paslaugų ir procesų rūšių aprašymą ir klasifikavimą;

b) sąrašą IRT produktų, paslaugų ir procesų, dėl kurių, remiantis atitinkamomis regioninio kibernetinio saugumo rizikos vertinimo ataskaitomis ir didelio poveikio ir ypatingos svarbos poveikio subjektų prioritetais, parengiamas neprivalomų kibernetinio saugumo rekomendacijų rinkinys.

2. ENTSO-E, bendradarbiaudamas su ES SSO subjektu, per 6 mėnesius nuo regioninio kibernetinio saugumo rizikos vertinimo ataskaitos patvirtinimo arba atnaujinimo pateikia ACER tos darbo programos santrauką.

3. PSO, padedami ENTSO-E ir bendradarbiaudami su ES SSO subjektu, stengiasi užtikrinti, kad neprivalomos kibernetinio saugumo viešojo pirkimo rekomendacijos, parengtos remiantis atitinkamu regioniniu kibernetinio saugumo rizikos vertinimu, būtų panašios arba palyginamos visuose sistemos eksploatavimo regionuose. Kibernetinio saugumo viešojo pirkimo rekomendacijų rinkiniai apima bent 33 straipsnio 2 dalies a punkte nurodytas specifikacijas. Kai įmanoma, specifikacijos parenkamos iš Europos ir tarptautinių standartų.

4. PSO, padedami ENTSO-E ir bendradarbiaudami su ES SSO subjektu, užtikrina, kad kibernetinio saugumo viešojo pirkimo rekomendacijos:

a) atitiktų viešųjų pirkimų principus pagal Direktyvą 2014/24/ES ir

b) būtų suderinamos su naujausiomis turimomis IRT produktui, paslaugai ar procesui aktualiomis Europos kibernetinio saugumo sertifikavimo schemomis ir į jas būtų atsižvelgta.

36 straipsnis

Europos kibernetinio saugumo sertifikavimo schemų naudojimo IRT produktų, paslaugų ir procesų viešajam pirkimui gairės

1. Pagal 35 straipsnį parengtos neprivalomos kibernetinio saugumo viešojo pirkimo rekomendacijos gali apimti sektorines Europos kibernetinio saugumo sertifikavimo schemų naudojimo gaires, kai yra tinkama schema tam tikros rūšies IRT produktams, paslaugoms ar procesams, kuriuos naudoja ypatingos svarbos poveikio subjektai, nedarant poveikio Europos kibernetinio saugumo sertifikavimo schemų sukūrimo sistemai pagal Reglamento (ES) 2019/881 46 straipsnį.

2. PSO, padedami ENTSO-E ir bendradarbiaudami su ES SSO subjektu, glaudžiai bendradarbiauja su ENISA, teikdami sektorines gaires, įtrauktas į neprivalomas kibernetinio saugumo viešojo pirkimo rekomendacijas pagal 1 dalį.

V SKYRIUS

INFORMACIJOS SRAUTAI, KIBERNETINIAI IŠPUOLIAI IR KRIZIŲ VALDYMAS

37 straipsnis

Dalijimosi informacija taisyklės

1. Kompetentinga institucija, gavusi informacijos, susijusios su praneštinu kibernetiniu išpuoliu:

a) įvertina tos informacijos konfidencialumo lygį ir apie savo vertinimo rezultatus nepagrįstai nedelsdama ir ne vėliau kaip per 24 valandas nuo informacijos gavimo informuoja subjektą;

b) stengiasi sužinoti, ar apie panašų kibernetinį išpuolį Sąjungoje nepranešta kitoms kompetentingoms institucijoms, kad gautą informaciją, susijusią su praneštinu kibernetiniu išpuoliu, būtų galima susieti su informacija, pateikta apie kitus kibernetinius išpuolius, papildyti turimą informaciją ir stiprinti ir koordinuoti kibernetinio saugumo atsaką;

c) atsako už verslo paslapčių pašalinimą ir informacijos anoniminimą pagal atitinkamas nacionalines ir Sąjungos taisykles;

d) nepagrįstai nedelsdama ir ne vėliau kaip per 24 valandas nuo informacijos apie praneštiną kibernetinį išpuolį gavimo pasidalija informacija su nacionaliniais bendraisiais kontaktiniais punktais, CSIRT ir visomis kompetentingomis institucijomis, pagal 4 straipsnį paskirtomis kitose valstybėse narėse, ir toms institucijoms ar įstaigoms reguliariai teikia atnaujintą informaciją;

e) nepagrįstai nedelsdama ir ne vėliau kaip per 24 valandas nuo informacijos gavimo pagal 1 dalies a punktą, suanoniminusi informaciją ir pašalinusi iš jos verslo paslaptis pagal 1 dalies c punktą, išplatina informaciją apie kibernetinį išpuolį savo valstybėje narėje veikiantiems ypatingos svarbos poveikio ir didelio poveikio subjektams ir reguliariai jiems teikia atnaujintą informaciją, kad jie galėtų veiksmingai organizuoti savo gynybą;

f) gali prašyti, kad pranešantysis didelio poveikio arba ypatingos svarbos poveikio subjektas saugiai išplatintų informaciją apie praneštiną kibernetinį išpuolį kitiems subjektams, kurie gali būti paveikti, kad būtų didinamas elektros energijos sektoriaus informuotumas apie padėtį ir užkirstas kelias pavojui, kad gali įvykti tarpvalstybinių elektros energijos srautų kibernetinio saugumo incidentas;

g) suanoniminusi ir pašalinusi verslo paslaptis, pasidalija su ENISA apibendrinamąja ataskaita, kurioje pateikia informaciją apie kibernetinį išpuolį.

2. CSIRT, sužinojusi apie nepašalintą aktyviai išnaudojamą pažeidžiamumą:

a) naudodamasi tinkamu saugiu informacijos mainų kanalu, nedelsdama pasidalija šia informacija su ENISA, nebent kituose Sąjungos teisės aktuose nurodyta kitaip;

b) padeda susijusiam subjektui užtikrinti, kad gamintojas ar tiekėjas veiksmingai, koordinuotai ir greitai imtųsi nepašalinto aktyviai išnaudojamo pažeidžiamumo valdymo arba veiksmingų ir efektyvių rizikos mažinimo valdymo priemonių;

c) pasidalija turima informacija su pardavėju ir prašo gamintojo arba tiekėjo, kai įmanoma, sudaryti informuotinų CSIRT valstybėse narėse, kuriose aktyviai išnaudojamas nepašalintas pažeidžiamumas, sąrašą;

d) pasidalija turima informacija su CSIRT, nustatytomis pagal ankstesnį punktą, remdamasi būtinybės žinoti principu;

e) pasidalija nepašalinto aktyviai išnaudojamo pažeidžiamumo, apie kurį pranešta, poveikio švelninimo strategijomis ir priemonėmis, kai jų esama.

3. Kompetentinga institucija, sužinojusi apie nepašalintą aktyviai išnaudojamą pažeidžiamumą:

a) koordinuodama veiksmus su CSIRT savo valstybėje narėje, pasidalija nepašalinto aktyviai išnaudojamo pažeidžiamumo, apie kurį pranešta, poveikio švelninimo strategijomis ir priemonėmis, kai jų esama;

b) dalijasi informacija su CSIRT valstybėje narėje, kurioje buvo pranešta apie nepašalintą aktyviai išnaudojamą pažeidžiamumą.

4. Jei kompetentinga institucija sužino apie nepašalintą pažeidžiamumą, bet neturi įrodymų, kad jis jau aktyviai išnaudojamas, ji nepagrįstai nedelsdama koordinuoja veiksmus su CSIRT pažeidžiamumui koordinuotai atskleisti, kaip nustatyta Direktyvos (ES) 2022/2555 12 straipsnio 1 dalyje.

5. Jei CSIRT gauna su kibernetinėmis grėsmėmis susijusią informaciją iš vieno ar kelių didelio poveikio arba ypatingos svarbos poveikio subjektų pagal 38 straipsnio 6 dalį, ji nepagrįstai nedelsdama ir ne vėliau kaip per keturias valandas nuo informacijos gavimo išplatina tą informaciją ir bet kokią kitą informaciją, kuri yra svarbi siekiant išvengti rizikos, ją nustatyti, į ją reaguoti arba ją sumažinti, ypatingos svarbos poveikio ir didelio poveikio subjektams savo valstybėje narėje ir, kai tinkama, visoms atitinkamoms CSIRT ir savo nacionaliniam bendrajam kontaktiniam punktui.

6. Jei kompetentinga institucija iš vieno ar kelių didelio poveikio arba ypatingos svarbos poveikio subjektų gauna informacijos, susijusios su kibernetinėmis grėsmėmis, 5 dalies tikslais ji perduoda šią informaciją CSIRT.

7. Atitinkamoms kompetentingoms institucijoms susitarus, kompetentingos institucijos gali visiškai arba iš dalies perduoti 3 ir 4 dalyse nurodytas pareigas, susijusias su vienu ar daugiau didelio poveikio ar ypatingos svarbos poveikio subjektų, veikiančių daugiau nei vienoje valstybėje narėje, kitai kompetentingai institucijai vienoje iš tų valstybių narių.

8. PSO, padedami ENTSO-E ir bendradarbiaudami su ES SSO subjektu, ne vėliau kaip 2025 m. birželio 13 d. parengia kibernetinių išpuolių klasifikavimo skalės metodiką. PSO, padedami ENTSO-E ir ES SSO subjekto, gali prašyti kompetentingų institucijų konsultuotis su ENISA ir už kibernetinį saugumą atsakingomis jų kompetentingomis institucijomis, kad padėtų parengti tokią klasifikavimo skalę. Metodikoje kibernetinio išpuolio sunkumas klasifikuojamas pagal 5 lygius, iš kurių du aukščiausi lygiai yra „didelis“ ir „kritinis“. Klasifikavimas grindžiamas šių parametrų vertinimu:

a) galimo poveikio, atsižvelgiant į paveikiamą turtą ir perimetrus, nustatytus pagal 26 straipsnio 4 dalies c punktą, ir

b) kibernetinio išpuolio kritiškumą.

9. Iki 2026 m. birželio 13 d. ENTSO-E, bendradarbiaudamas su ES SSO subjektu, atlieka galimybių studiją, kad įvertintų galimybę ir finansines išlaidas, kurių reikia bendrai priemonei, kuria naudodamiesi visi subjektai galėtų dalytis informacija su atitinkamomis nacionalinėmis institucijomis, sukurti.

10. Galimybių studijoje išnagrinėjama galimybė sukurti tokią bendrą priemonę siekiant:

a) remti ypatingos svarbos poveikio ir didelio poveikio subjektus teikiant atitinkamą su saugumu susijusią informaciją tarpvalstybinių elektros energijos srautų operacijoms, pvz., beveik tikruoju laiku pranešant apie kibernetinius išpuolius, teikiant išankstinius perspėjimus, susijusius su kibernetinio saugumo klausimais ir neatskleistu elektros energijos sistemoje naudojamos įrangos pažeidžiamumu;

b) eksploatuoti ją tinkamoje ir labai patikimoje aplinkoje;

c) sudaryti sąlygas rinkti duomenis iš ypatingos svarbos poveikio ir didelio poveikio subjektų, palengvinti konfidencialios informacijos pašalinimą ir duomenų anoniminimą bei greitą jų išplatinimą ypatingos svarbos poveikio ir didelio poveikio subjektams.

11. ENTSO-E, bendradarbiaudamas su ES SSO subjektu:

a) vertindamas galimybes konsultuojasi su ENISA ir TIS bendradarbiavimo grupe, nacionaliniais bendraisiais kontaktiniais punktais ir pagrindinių suinteresuotųjų subjektų atstovais;

b) pateikia galimybių studijos rezultatus ACER ir TIS bendradarbiavimo grupei.

12. ENTSO-E, bendradarbiaudamas su ES SSO subjektu, gali išanalizuoti ypatingos svarbos poveikio ir didelio poveikio subjektų siūlomas iniciatyvas ir sudaryti palankesnes sąlygas įvertinti ir išbandyti tokias dalijimosi informacija priemones.

38 straipsnis

Didelio poveikio ir ypatingos svarbos poveikio subjektų vaidmuo dalijantis informacija

1. Kiekvienas didelio poveikio ir ypatingos svarbos poveikio subjektas:

a) nustato bent šiuos viso savo turto, esančio kibernetinio saugumo perimetre, nustatytame pagal 26 straipsnio 4 dalies c punktą, KSOC pajėgumus:

   i) užtikrinti, kad atitinkamose tinklų ir informacinėse sistemose bei taikomosiose programose būtų daromi saugumo įrašai saugumo stebėsenai vykdyti, kad būtų galima aptikti anomalijas ir rinkti informaciją apie kibernetinius išpuolius;

   ii) vykdyti saugumo stebėseną, įskaitant įsilaužimo aptikimą ir tinklų bei informacinių sistemų pažeidžiamumo vertinimą;

   iii) analizuoti ir, jei reikia, imtis visų veiksmų, kurių reikia atsižvelgiant į jo pareigą ir gebėjimą apsaugoti subjektą;

   iv) rinkti informaciją ir ja dalytis, kaip apibūdinta šiame straipsnyje;

b) turi teisę pirkti visus šiuos pajėgumus arba jų dalį pagal a punktą per valdomų saugumo paslaugų teikėjus (VSPT). Ypatingos svarbos poveikio ir didelio poveikio subjektai išlieka atsakingi už VSPT ir prižiūri jų pastangas;

c) paskiria vieną subjekto lygmens bendrąjį kontaktinį punktą dalytis informacija.

2. Vykdydama Reglamento (ES) 2019/881 6 straipsnio 2 dalyje nustatytą užduotį ENISA gali paskelbti neprivalomas gaires dėl tokių pajėgumų užtikrinimo arba subrangos sutarties su VSPT sudarymo.

3. Kiekvienas ypatingos svarbos poveikio ir didelio poveikio subjektas nepagrįstai nedelsdamas ir ne vėliau kaip per keturias valandas nuo tada, kai sužinojo, kad incidentas yra praneštinas, pasidalija atitinkama informacija apie praneštiną kibernetinį išpuolį su savo CSIRT ir savo kompetentinga institucija.

4. Informacija, susijusi su kibernetiniu išpuoliu, laikoma praneština, kai kibernetinio išpuolio kritiškumą įvertinęs paveiktas subjektas nustato, kad pagal kibernetinio išpuolio klasifikavimo skalės metodiką pagal 37 straipsnio 8 dalį jis yra „didelis“ arba „kritinis“. Pagal 1 dalies c punktą paskirtas subjekto lygmens bendrasis kontaktinis punktas praneša incidento klasifikavimo rezultatą.

5. Kai ypatingos svarbos poveikio ir didelio poveikio subjektai perduoda CSIRT aktualią informaciją, susijusią su nepašalintu aktyviai išnaudojamu pažeidžiamumu, ši gali perduoti šią informaciją savo kompetentingai institucijai. Atsižvelgdama į praneštos informacijos slaptumo lygį, CSIRT gali informacijos neatskleisti arba atidėti jos perdavimą dėl pagrįstų su kibernetiniu saugumu susijusių priežasčių.

6. Kiekvienas ypatingos svarbos poveikio ir didelio poveikio subjektas savo CSIRT nepagrįstai nedelsdamas pateikia visą informaciją, susijusią su praneština kibernetine grėsme, kurios poveikis gali būti tarpvalstybinis. Informacija, susijusi su kibernetine grėsme, laikoma praneština, kai įvykdyta bent viena iš šių sąlygų:

a) tai yra kitam ypatingos svarbos poveikio ar didelio poveikio subjektui siekiant išvengti rizikos, ją nustatyti, į ją reaguoti ar sušvelninti jos poveikį aktuali informacija;

b) dėl nustatytų metodų, taktikos ir procedūrų, naudojamų vykdant išpuolį, gauta informacija, pvz., paveikti URL arba IP adresai, maišos vertės ar bet koks kitas požymis, yra naudinga išpuolio aplinkybėms nustatyti ir išpuoliui susieti;

c) kibernetinė grėsmė gali būti toliau vertinama ir jos aplinkybės papildomos remiantis informacija, kurią pateikia paslaugų teikėjai arba trečiosios šalys, kuriems šis reglamentas netaikomas.

7. Kiekvienas ypatingos svarbos poveikio subjektas ir didelio poveikio subjektas, dalydamiesi informacija pagal šį straipsnį, nurodo:

a) kad informacija pateikiama pagal šį reglamentą;

b) ar informacija yra susijusi su:

i) praneštinu kibernetiniu išpuoliu, nurodytu 3 dalyje;

ii) 4 dalyje nurodytu nepašalintu aktyviai išnaudojamu pažeidžiamumu, apie kurį viešai nežinoma;

iii) praneština kibernetine grėsme, nurodyta 5 dalyje;

c) praneštino kibernetinio išpuolio atveju – kibernetinio išpuolio lygį pagal 37 straipsnio 8 dalyje nurodytą kibernetinių išpuolių klasifikavimo skalės metodiką ir informaciją, kuria remiantis nustatytas toks lygis, įskaitant bent jau kibernetinio išpuolio kritiškumą.

8. Kai ypatingos svarbos poveikio arba didelio poveikio subjektas praneša apie didelį incidentą pagal Direktyvos (ES) 2022/2555 23 straipsnį ir pranešime apie incidentą pagal tą straipsnį pateikiama aktuali informacija, kaip reikalaujama pagal šio straipsnio 3 dalį, subjekto pranešimas pagal tos direktyvos 23 straipsnio 1 dalį laikomas informacijos pranešimu pagal šio straipsnio 3 dalį.

9. Kiekvienas ypatingos svarbos poveikio ir didelio poveikio subjektas pranešime savo kompetentingai institucijai arba CSIRT aiškiai nurodo konkrečią informaciją, kuria dalijasi tik su kompetentinga institucija arba CSIRT, tais atvejais, kai toks dalijimasis informacija galėtų būti kibernetinio išpuolio šaltinis. Kiekvienas ypatingos svarbos poveikio ir didelio poveikio subjektas turi teisę kompetentingai CSIRT pateikti nekonfidencialią informacijos versiją.

39 straipsnis

Kibernetinių išpuolių aptikimas ir susijusios informacijos tvarkymas

1. Ypatingos svarbos poveikio ir didelio poveikio subjektai, pasinaudodami reikiama atitinkamos kompetentingos institucijos, ENTSO-E ir ES SSO subjekto parama, plėtoja būtinus pajėgumus, kad galėtų tinkamai reaguoti į aptiktus kibernetinius išpuolius. Ypatingos svarbos poveikio ir didelio poveikio subjektams atitinkamoje valstybėje narėje paskirta CSIRT gali padėti vykdydama savo užduotį, pavestą pagal Direktyvos (ES) 2022/2555 11 straipsnio 5 dalies a punktą. Ypatingos svarbos poveikio ir didelio poveikio subjektai įgyvendina veiksmingus kibernetinių išpuolių, kurie paveiks arba gali paveikti tarpvalstybinius elektros energijos srautus, aptikimo, klasifikavimo ir reagavimo į juos procesus, kad kuo labiau sumažintų jų poveikį.

2. Jei kibernetinis išpuolis paveikia tarpvalstybinius elektros energijos srautus, paveiktų ypatingos svarbos poveikio ir didelio poveikio subjektų bendrieji kontaktiniai punktai bendradarbiauja, kad tarpusavyje dalytųsi informacija, koordinuojami valstybės narės, kurioje pirmą kartą pranešta apie kibernetinį išpuolį, kompetentingos institucijos.

3. Ypatingos svarbos poveikio ir didelio poveikio subjektai:

a) užtikrina, kad jų pačių subjekto lygmens bendrasis kontaktinis punktas pagal būtinybės žinoti principą turėtų galimybę susipažinti su informacija, kurią jie gavo iš nacionalinio bendrojo kontaktinio punkto per savo kompetentingą instituciją;

b) jei dar nėra to padarę pagal Direktyvos (ES) 2022/2555 3 straipsnio 4 dalį, valstybės narės, kurioje jie yra įsisteigę, kompetentingai institucijai ir nacionaliniam bendrajam kontaktiniam punktui pateikia sąrašą savo kibernetinio saugumo subjekto lygmens bendrųjų kontaktinių punktų:

   i) iš kurių ta kompetentinga institucija ir nacionalinis bendrasis kontaktinis punktas gali tikėtis gauti pranešimus apie praneštinus kibernetinius išpuolius;

   ii) kuriems prireikus informaciją gali teikti kompetentingos institucijos ir nacionaliniai bendrieji kontaktiniai punktai;

c) nustato kibernetinių išpuolių valdymo procedūras, įskaitant funkcijas ir pareigas, užduotis ir reagavimą, grindžiamus stebima kibernetinio išpuolio raida ypatingos svarbos poveikio ir didelio poveikio perimetruose;

d) bent kartą per metus išbando bendras kibernetinių išpuolių valdymo procedūras, išbandydami bent vieną scenarijų, pagal kurį tiesiogiai ar netiesiogiai paveikiami tarpvalstybiniai elektros energijos srautai. Tą metinį bandymą ypatingos svarbos poveikio ir didelio poveikio subjektai gali atlikti per 43 straipsnyje nurodytas reguliarias pratybas. Taip pat metiniu bandymu pagal reagavimo į kibernetinius išpuolius planą gali būti laikoma bet kokia tiesioginio reagavimo į kibernetinį išpuolį veikla, kurios pagrindinė priežastis yra kibernetinis saugumas ir kurią vykdant šalinami padariniai pagal 37 straipsnio 8 dalyje nurodytą kibernetinio išpuolio klasifikavimo skalės metodiką priskiriami bent 2 lygiui.

4. 1 dalyje nurodytas užduotis pagal Reglamento (ES) 2019/943 37 straipsnio 2 dalį valstybės narės gali perduoti ir regioniniams koordinavimo centrams.

40 straipsnis

Krizių valdymas

1. Kai kompetentinga institucija nustato, kad elektros energijos sektoriaus krizė yra susijusi su kibernetiniu išpuoliu, paveikiančiu daugiau nei vieną valstybę narę, paveiktų valstybių narių kompetentingos institucijos, už kibernetinį saugumą atsakingos NKI, už pasirengimą valdyti riziką atsakingos NKI ir TIS kibernetinių krizių valdymo institucijos kartu sudaro *ad hoc* tarpvalstybinio krizės koordinavimo grupę.

2. *Ad hoc* tarpvalstybinio krizės koordinavimo grupė:

a) koordinuoja efektyvų visos aktualios kibernetinio saugumo informacijos gavimą ir tolesnę jos sklaidą krizės valdymo procese dalyvaujantiems subjektams;

b) organizuoja visų krizės paveiktų subjektų ir kompetentingų institucijų bendravimą, kad būtų sumažintas dubliavimas ir padidintas analizių ir techninių priemonių veiksmingumas siekiant išspręsti vienalaikę elektros energijos sektoriaus krizę, kurios pagrindinė priežastis yra kibernetinis saugumas;

c) bendradarbiaudama su kompetentingomis CSIRT teikia reikiamas ekspertines žinias, įskaitant operatyvines konsultacijas nuo incidento nukentėjusiems subjektams dėl galimų rizikos mažinimo priemonių įgyvendinimo;

d) Komisijai ir Elektros energijos srities veiklos koordinavimo grupei praneša ir reguliariai atnaujina informaciją apie incidento padėtį, vadovaudamasi 46 straipsnyje nustatytais apsaugos principais;

e) konsultuojasi su atitinkamomis valdžios institucijomis, agentūromis ar subjektais, kai tokios konsultacijos galėtų būti naudingos siekiant sušvelninti elektros energijos sektoriaus krizę.

3. Kai kibernetinis išpuolis pripažįstamas arba numatoma, kad jis bus pripažintas didelio masto kibernetinio saugumo incidentu, *ad hoc* tarpvalstybinio krizės koordinavimo grupė pagal Direktyvos (ES) 2022/2555 9 straipsnio 1 dalį nedelsdama informuoja incidento paveiktų valstybių narių nacionalines kibernetinių krizių valdymo institucijas, taip pat Komisiją ir EU-CyCLONe. Tokiu atveju *ad hoc* tarpvalstybinio krizės koordinavimo grupė padeda EU-CyCLONe dėl sektoriaus ypatumų.

4. Ypatingos svarbos poveikio ir didelio poveikio subjektai parengia ir užtikrina pajėgumus, vidaus gaires, parengties planus ir darbuotojus, kurie galėtų dalyvauti aptinkant ir švelninant tarpvalstybines krizes, ir užsitikrina galimybę jais naudotis. Ypatingos svarbos poveikio arba didelio poveikio subjektas, kurį paveikė vienalaikė elektros energijos sektoriaus krizė, bendradarbiaudamas su savo kompetentinga institucija ištiria pagrindinę tokios krizės priežastį, kad nustatytų, kokiu mastu krizė yra susijusi su kibernetiniu išpuoliu.

5. 4 dalyje nurodytas užduotis pagal Reglamento (ES) 2019/943 37 straipsnio 2 dalį valstybės narės gali perduoti ir regioniniams koordinavimo centrams.

41 straipsnis

Kibernetinio saugumo krizių valdymo ir reagavimo į jas planai

1. Per 24 mėnesius nuo Sąjungos masto rizikos vertinimo ataskaitos pateikimo ACER, ji, glaudžiai bendradarbiaudama su ENISA, ENTSO-E, ES SSO subjektu, už kibernetinį saugumą atsakingomis NKI, kompetentingomis institucijomis, už pasirengimą valdyti riziką atsakingomis NKI, NRI ir TIS nacionalinėmis kibernetinių krizių valdymo institucijomis, parengia Sąjungos lygmens elektros energijos sektoriaus kibernetinio saugumo krizių valdymo ir reagavimo į jas planą.

2. Per 12 mėnesių po to, kai ACER parengia Sąjungos lygmens elektros energijos sektoriaus kibernetinio saugumo krizių valdymo ir reagavimo į jas planą pagal 1 dalį, kiekviena kompetentinga institucija parengia nacionalinį tarpvalstybinių elektros energijos srautų kibernetinio saugumo krizių valdymo ir reagavimo į jas planą, atsižvelgdama į Sąjungos lygmens kibernetinio saugumo krizių valdymo planą ir nacionalinį pasirengimo valdyti riziką planą, parengtą pagal Reglamento (ES) 2019/941 10 straipsnį. Šis planas turi derėti su reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planu pagal Direktyvos (ES) 2022/2555 9 straipsnio 4 dalį. Kompetentinga institucija koordinuoja veiksmus su ypatingos svarbos poveikio ir didelio poveikio subjektais ir už pasirengimą valdyti riziką atsakingomis NKI savo valstybėje narėje.

3. Nacionalinis reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planas, kurio reikalaujama pagal Direktyvos (ES) 2022/2555 9 straipsnio 4 dalį, laikomas nacionaliniu kibernetinio saugumo krizių valdymo planu pagal šį straipsnį, jei į jį įtrauktos tarpvalstybinių elektros energijos srautų krizių valdymo ir reagavimo į jas nuostatos.

4. 1 ir 2 dalyse nurodytas užduotis pagal Reglamento (ES) 2019/943 37 straipsnio 2 dalį valstybės narės gali perduoti ir regioniniams koordinavimo centrams.

5. Ypatingos svarbos poveikio ir didelio poveikio subjektai užtikrina, kad jų su kibernetiniu saugumu susijusių krizių valdymo procesai:

a) turėtų suderinamas tarpvalstybinių kibernetinio saugumo incidentų valdymo, apibrėžto Direktyvos (ES) 2022/2555 6 straipsnio 8 punkte, procedūras, oficialiai įtrauktas į jų krizių valdymo planus;

b) būtų bendrosios krizių valdymo veiklos dalis.

6. Per 12 mėnesių nuo pranešimo apie didelio poveikio ir ypatingos svarbos poveikio subjektus pagal 24 straipsnio 6 dalį ir vėliau kas trejus metus ypatingos svarbos poveikio ir didelio poveikio subjektai parengia subjekto lygmens kibernetinio saugumo krizių valdymo planą ir įtraukia jį į savo bendruosius krizių valdymo planus. Į šį planą įtraukiama bent ši informacija:

a) krizės paskelbimo taisyklės, išdėstytos Reglamento (ES) 2019/941 14 straipsnio 2 ir 3 dalyse;

b) aiškūs vaidmenys ir atsakomybė už krizių valdymą, įskaitant kitų atitinkamų ypatingos svarbos poveikio ir didelio poveikio subjektų vaidmenį;

c) naujausia kontaktinė informacija, taip pat komunikacijos ir dalijimosi informacija krizės metu, įskaitant susisiekimą su CSIRT, taisyklės.

7. Krizių valdymo priemonės pagal Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies c punktą laikomos elektros energijos sektoriaus subjekto lygmens krizių valdymo planu pagal šį straipsnį, jei atitinka visus 6 dalyje išvardytus reikalavimus.

8. Krizių valdymo planai išbandomi per 43, 44 ir 45 straipsniuose nurodytas kibernetinio saugumo pratybas.

9. Ypatingos svarbos poveikio ir didelio poveikio subjektai savo subjekto lygmens krizių valdymo planus įtraukia į savo ypatingos svarbos poveikio ir didelio poveikio procesams taikomus veiklos tęstinumo planus. Į subjekto lygmens krizių valdymo planus įtraukiama:

a) procesai, priklausantys nuo IT paslaugų prieinamumo, vientisumo ir patikimumo;

b) visos vietos, įskaitant aparatinės ir programinės įrangos vietas, kuriose užtikrinamas veiklos tęstinumas;

c) visi vidaus vaidmenys ir pareigos, susiję su veiklos tęstinumo procesais.

10. Ypatingos svarbos poveikio ir didelio poveikio subjektai bent kas trejus metus ir prireikus atnaujina savo subjekto lygmens krizių valdymo planus.

11. ACER bent kas trejus metus ir prireikus atnaujina pagal 1 dalį parengtą Sąjungos lygmens elektros energijos sektoriaus kibernetinio saugumo krizių valdymo ir reagavimo į jas planą.

12. Kiekviena kompetentinga institucija bent kas trejus metus ir prireikus atnaujina pagal 2 dalį parengtą nacionalinį tarpvalstybinių elektros energijos srautų kibernetinio saugumo krizių valdymo ir reagavimo į jas planą.

13. Ypatingos svarbos poveikio ir didelio poveikio subjektai savo veiklos tęstinumo planus išbando bent kartą per trejus metus arba po esminių ypatingos svarbos poveikio proceso pakeitimų. Veiklos tęstinumo plano bandymų rezultatai dokumentuojami. Ypatingos svarbos poveikio ir didelio poveikio subjektai savo veiklos tęstinumo plano bandymą gali įtraukti į kibernetinio saugumo pratybas.

14. Ypatingos svarbos poveikio ir didelio poveikio subjektai prireikus ir bent kartą per trejus metus atnaujina savo veiklos tęstinumo planą, atsižvelgdami į bandymo rezultatus.

15. Jei per bandymą nustatoma veiklos tęstinumo plano trūkumų, ypatingos svarbos poveikio ir didelio poveikio subjektas tuos trūkumus ištaiso per 180 kalendorinių dienų po bandymo ir atlieka naują bandymą, kad įrodytų, jog taisomosios priemonės yra veiksmingos.

16. Jei ypatingos svarbos poveikio arba didelio poveikio subjektas negali ištaisyti trūkumų per 180 kalendorinių dienų, jis savo kompetentingai institucijai pagal 27 straipsnį pateikiamoje ataskaitoje nurodo priežastis.

42 straipsnis

Elektros energijos sektoriaus kibernetinio saugumo ankstyvojo perspėjimo pajėgumai

1. Kompetentingos institucijos bendradarbiauja su ENISA, kad padėtų valstybėms narėms pagal Reglamento (ES) 2019/881 6 straipsnio 2 ir 7 dalis plėtoti elektros energijos sektoriaus kibernetinio saugumo ankstyvojo perspėjimo pajėgumus

2. Elektros energijos sektoriaus kibernetinio saugumo ankstyvojo perspėjimo pajėgumai sudaro sąlygas ENISA, vykdant Reglamento (ES) 2019/881 7 straipsnio 7 dalyje išvardytas užduotis:

a) rinkti informaciją, kuria savanoriškai dalijasi:

   i) CSIRT, kompetentingos institucijos;

   ii) šio reglamento 2 straipsnyje išvardyti subjektai;

   iii) bet kuris kitas subjektas, norintis savanoriškai pasidalyti aktualia informacija;

b) įvertinti ir klasifikuoti surinktą informaciją;

c) įvertinti ENISA prieinamą informaciją, kad galėtų nustatyti kibernetinės rizikos sąlygas ir atitinkamus rodiklius, susijusius su tarpvalstybinių elektros energijos srautų aspektais;

d) identifikuoti sąlygas ir rodiklius, kurie dažnai koreliuoja su kibernetiniais išpuoliais elektros energijos sektoriuje;

e) nustatyti, ar reikia atlikti tolesnę analizę ir imtis prevencinių veiksmų vertinant ir identifikuojant rizikos veiksnius;

f) informuoti kompetentingas institucijas apie identifikuotą riziką ir rekomenduojamus konkrečių susijusių subjektų prevencinius veiksmus;

g) informuoti visus atitinkamus 2 straipsnyje išvardytus subjektus apie informacijos vertinimo pagal šios dalies b, c ir d punktus rezultatus;

h) periodiškai įtraukti aktualią informaciją į informuotumo apie padėtį ataskaitą, rengiamą pagal Reglamento (ES) 2019/881 7 straipsnio 6 dalį;

i) Iš surinktos informacijos išvesti, kai įmanoma, taikytinus duomenis, kurie rodo galimą saugumo pažeidimą arba kibernetinį išpuolį (užvaldymo rodikliai).

3. CSIRT, vykdydamos savo užduotis, nustatytas Direktyvos (ES) 2022/2555 11 straipsnio 3 dalies b punkte, nedelsdamos išplatina iš ENISA gautą informaciją atitinkamiems subjektams.

4. ACER stebi elektros energijos sektoriaus kibernetinio saugumo ankstyvojo perspėjimo pajėgumų veiksmingumą. ENISA padeda ACER, teikdama visą būtiną informaciją pagal Reglamento (ES) 2019/881 6 straipsnio 2 dalį ir 7 straipsnio 1 dalį. Šios stebėsenos veiklos analizė yra pagal šio reglamento 12 straipsnį vykdomos stebėsenos dalis.

VI SKYRIUS

ELEKTROS ENERGIJOS SEKTORIAUS KIBERNETINIO SAUGUMO PRATYBŲ SISTEMA

43 straipsnis

Subjektų ir valstybių narių lygmens kibernetinio saugumo pratybos

1. Ne vėliau kaip metų, einančių po pranešimo apie ypatingos svarbos poveikio subjektus, gruodžio 31 d., o vėliau kas trejus metus kiekvienas ypatingos svarbos poveikio subjektas atlieka kibernetinio saugumo pratybas, apimančias vieną ar daugiau scenarijų, kai kibernetiniai išpuoliai tiesiogiai ar netiesiogiai paveikia tarpvalstybinius elektros energijos srautus ir yra susiję su rizika, identifikuota atliekant valstybių narių ir subjektų lygmens kibernetinio saugumo rizikos vertinimus pagal 20 ir 27 straipsnius.

2. Nukrypstant nuo 1 dalies, už pasirengimą valdyti riziką atsakinga NKI, pasikonsultavusi su kompetentinga institucija ir atitinkama kibernetinių krizių valdymo institucija, paskirta arba įsteigta pagal Direktyvos (ES) 2022/2555 9 straipsnį, gali nuspręsti kibernetinio saugumo pratybas, aprašytas 1 dalyje, surengti valstybės narės lygmeniu, užuot rengus subjekto lygmens kibernetinio saugumo pratybas. Apie tai kompetentinga institucija informuoja:

a) visus savo valstybės narės ypatingos svarbos poveikio subjektus, NRI, CSIRT ir už kibernetinį saugumą atsakingą NKI – ne vėliau kaip metų, einančių prieš subjekto lygmens kibernetinio saugumo pratybas, birželio 30 d.;

b) kiekvieną subjektą, kuris turi dalyvauti valstybės narės lygmens kibernetinio saugumo pratybose, – ne vėliau kaip likus 6 mėnesiams iki tų pratybų.

3. Už pasirengimą valdyti riziką atsakinga NKI, padedama savo CSIRT, organizuoja 2 dalyje aprašytas valstybės narės lygmens kibernetinio saugumo pratybas atskirai arba kartu su kitomis kibernetinio saugumo pratybomis toje valstybėje narėje. Kad galėtų sugrupuoti šias pratybas, už pasirengimą valdyti riziką atsakinga NKI 1 dalyje nurodytas valstybės narės lygmens kibernetinio saugumo pratybas gali atidėti vieniems metams.

4. Subjekto lygmens ir valstybės narės lygmens kibernetinio saugumo pratybos turi derėti su nacionalinėmis kibernetinio saugumo krizių valdymo sistemomis pagal Direktyvos (ES) 2022/2555 9 straipsnio 4 dalies d punktą.

5. Iki 2026 m. gruodžio 31 d. ir vėliau kas trejus metus ENTSO-E, bendradarbiaudamas su ES SSO subjektu, pateikia pratybų scenarijaus šabloną, skirtą 1 dalyje nurodytoms subjekto lygmens ir valstybės narės lygmens kibernetinio saugumo pratyboms atlikti. Šiame šablone atsižvelgiama į naujausią subjektų ir valstybės narės lygmens kibernetinio saugumo rizikos vertinimą ir pateikiami pagrindiniai sėkmės kriterijai. ENTSO-E ir ES SSO subjektas į tokio šablono rengimą įtraukia ACER ir ENISA.

44 straipsnis

Regioninės ir tarpregioninės kibernetinio saugumo pratybos

1. Iki 2029 m. gruodžio 31 d. ir vėliau kas trejus metus kiekviename sistemos eksploatavimo regione ENTSO-E, bendradarbiaudamas su ES SSO subjektu, organizuoja regionines kibernetinio saugumo pratybas. Regioninėse kibernetinio saugumo pratybose dalyvauja sistemos eksploatavimo regiono ypatingos svarbos poveikio subjektai. ENTSO-E, bendradarbiaudamas su ES SSO subjektu, tuo pačiu laikotarpiu vietoj regioninių kibernetinio saugumo pratybų gali organizuoti tarpregionines kibernetinio saugumo pratybas daugiau nei viename sistemos eksploatavimo regione. Per pratybas turėtų būti atsižvelgiama į kitus esamus Sąjungos lygmens kibernetinio saugumo rizikos vertinimus ir scenarijus.

2. ENISA padeda ENTSO-E ir ES SSO subjektui rengti ir organizuoti regionines ir tarpregionines kibernetinio saugumo pratybas.

3. ENTSO-E, koordinuodamas veiksmus su ES SSO subjektu, informuoja ypatingos svarbos poveikio subjektus, kurie turi dalyvauti regioninėse arba tarpregioninėse kibernetinio saugumo pratybose, iki pratybų likus šešiems mėnesiams.

4. Reguliarių Sąjungos lygmens kibernetinio saugumo pratybų pagal Reglamento (ES) 2019/881 7 straipsnio 5 dalį arba bet kokių privalomų kibernetinio saugumo pratybų, susijusių su elektros energijos sektoriumi toje pačioje geografinėje teritorijoje, organizatorius gali pakviesti dalyvauti ENTSO-E ir ES SSO subjektą. Tokiais atvejais 1 dalyje nustatyta pareiga netaikoma su sąlyga, kad tose pačiose pratybose dalyvauja visi sistemos eksploatavimo regiono ypatingos svarbos poveikio subjektai.

5. Jei ENTSO-E ir ES SSO subjektas dalyvauja 4 dalyje nurodytose kibernetinio saugumo pratybose, jie gali 1 dalyje nurodytas regionines arba tarpregionines kibernetinio saugumo pratybas atidėti vieniems metams.

6. Iki 2027 m. gruodžio 31 d. ir vėliau kas trejus metus ENTSO-E, bendradarbiaudamas su ES SSO subjektu, pateikia pratybų scenarijaus šabloną, skirtą regioninėms ir tarpregioninėms kibernetinio saugumo pratyboms atlikti. Šiame šablone atsižvelgiama į naujausią regioninio lygmens kibernetinio saugumo rizikos vertinimą ir pateikiami pagrindiniai sėkmės kriterijai. ENTSO-E konsultuojasi su Komisija ir gali prašyti ACER, ENISA ir Jungtinio tyrimų centro rekomendacijų dėl regioninių ir tarpregioninių kibernetinio saugumo pratybų organizavimo ir vykdymo.

45 straipsnis

Subjekto, valstybės narės, regioninių ir tarpregioninių kibernetinio saugumo pratybų rezultatai

1. 43 straipsnio 1 ir 2 dalyse ir 44 straipsnio 1 dalyje nurodytose kibernetinio saugumo pratybose ypatingos svarbos poveikio subjekto prašymu dalyvauja ypatingos svarbos paslaugų teikėjai, teikiantys paslaugas ypatingos svarbos poveikio subjektui teritorijoje, kurią apima atitinkamos kibernetinio saugumo pratybos.

2. 43 straipsnio 1 ir 2 dalyse ir 44 straipsnio 1 dalyje nurodytų kibernetinio saugumo pratybų organizatoriai, gavę ENISA rekomendacijas, jei jų prašo, taip pat pagal Reglamento (ES) 2019/881 7 straipsnio 5 dalį, analizuoja ir užbaigia aktualias kibernetinio saugumo pratybas, pateikdami visiems dalyviams skirtą ataskaitą, kurioje apibendrinama įgyta patirtis. Ataskaitoje pateikiama:

a) pratybų scenarijai, posėdžių ataskaitos, pagrindinės pozicijos, bet kurio elektros energijos vertės grandinės lygmens laimėjimai ir įgyta patirtis;

b) ar buvo įvykdyti pagrindiniai sėkmės reikalavimai;

c) atitinkamose kibernetinio saugumo pratybose dalyvaujantiems subjektams skirtos rekomendacijos, kaip ištaisyti, pritaikyti ar pakeisti kibernetinio saugumo krizės procesus, procedūras, susijusius valdymo modelius ir visus esamus sutartinius įsipareigojimus su ypatingos svarbos paslaugų teikėjais.

3. CSIRT tinklo, TIS bendradarbiavimo grupės arba EU-CyCLONe prašymu 43 straipsnio 1 ir 2 dalyse ir 44 straipsnio 1 dalyje nurodytų kibernetinio saugumo pratybų organizatoriai dalijasi atitinkamų kibernetinio saugumo pratybų rezultatais. Organizatoriai su kiekvienu pratybose dalyvaujančiu subjektu dalijasi šio straipsnio 2 dalies a ir b punktuose nurodyta informacija. Organizatoriai tos dalies c punkte nurodytomis rekomendacijomis dalijasi tik su subjektais, kuriems jos skirtos.

4. 43 straipsnio 1 ir 2 dalyse ir 44 straipsnio 1 dalyje nurodytų kibernetinio saugumo pratybų organizatoriai reguliariai imasi tolesnių veiksmų su pratybose dalyvaujančiais subjektais dėl rekomendacijų pagal šio straipsnio 2 dalies c punktą įgyvendinimo.

VII SKYRIUS

INFORMACIJOS APSAUGA

46 straipsnis

Informacijos, kuria keičiamasi, apsaugos principai

1. 2 straipsnio 1 dalyje išvardyti subjektai užtikrina, kad pagal šį reglamentą teikiama, gaunama ir perduodama informacija, taip pat informacija, kuria keičiamasi, būtų prieinama tik pagal būtinybės žinoti principą ir laikantis atitinkamų Sąjungos ir nacionalinių informacijos saugumo taisyklių.

2. 2 straipsnio 1 dalyje išvardyti subjektai užtikrina, kad pagal šį reglamentą teikiama, gaunama ir perduodama informacija, taip pat informacija, kuria keičiamasi, būtų tvarkoma ir sekama per visą jos gyvavimo ciklą ir kad jos gyvavimo ciklui pasibaigus ji galėtų būti atskleista tik anonimine forma.

3. 2 straipsnio 1 dalyje išvardyti subjektai užtikrina, kad būtų įdiegtos visos būtinos organizacinio ir techninio pobūdžio apsaugos priemonės, kad būtų išsaugotas pagal šį reglamentą pateiktos, gautos ir perduotos informacijos, taip pat informacijos, kuria pasikeista, konfidencialumas, vientisumas, prieinamumas ir neginčijamumas, nepriklausomai nuo naudojamų priemonių. Apsaugos priemonės:

a) turi būti proporcingos;

b) jomis turi būti atsižvelgta į kibernetinio saugumo riziką, susijusią su žinomomis ankstesnėmis ir naujomis grėsmėmis, kurios gali būti aktualios tokiai informacijai taikant šį reglamentą;

c) kiek įmanoma, turi būti grindžiamos nacionaliniais, Europos ar tarptautiniais standartais ir geriausia praktika;

d) turi būti dokumentuojamos.

4. 2 straipsnio 1 dalyje išvardyti subjektai užtikrina, kad bet kuris asmuo, kuriam suteikta prieiga prie pagal šį reglamentą teikiamos, gautos ar perduodamos informacijos, taip pat informacijos, kuria keičiamasi pagal šį reglamentą, būtų informuotas apie taikomas subjekto lygmens saugumo taisykles ir apie informacijos apsaugai aktualias priemones ir procedūras. Tie subjektai užtikrina, kad atitinkamas asmuo pripažintų atsakomybę užtikrinti informacijos apsaugą, kaip nurodyta jį informuojant.

5. 2 straipsnio 1 dalyje išvardyti subjektai užtikrina, kad prieiga prie pagal šį reglamentą teikiamos, gautos ar perduodamos informacijos, taip pat informacijos, kuria keičiamasi, būtų suteikiama tik asmenims:

a) kuriems su ta informacija susipažinti leidžiama atsižvelgiant į jų funkcijas ir tik vykdant pavestas užduotis;

b) kurių etikos ir sąžiningumo principus galėjo įvertinti subjektas ir dėl kurių nėra įrodymų, kad pagal subjekto geriausią praktiką ir standartinius saugumo reikalavimus ir, kai būtina, nacionalinius įstatymus ir kitus teisės aktus atlikus asmens patikimumo patikrinimą buvo gauti neigiami rezultatai.

6. 2 straipsnio 1 dalyje išvardyti subjektai turi gauti raštišką fizinio ar juridinio asmens, kuris pirmasis sukūrė arba pateikė informaciją, sutikimą, prieš pateikdami tą informaciją trečiajai šaliai, kuriai šis reglamentas netaikomas.

7. 2 straipsnio 1 dalyje nurodytas subjektas gali svarstyti galimybę šia informacija dalytis nesilaikant šio straipsnio 1 ir 4 dalių, kad būtų užkirstas kelias vienalaikei elektros energijos sektoriaus krizei, kurios pagrindinė priežastis yra kibernetinis saugumas, arba bet kokiai tarpvalstybinei krizei Sąjungoje kitame sektoriuje. Tokiu atveju jis:

a) konsultuojasi su kompetentinga institucija ir gauna jos leidimą dalytis tokia informacija;

b) suanonimina tokią informaciją neprarasdamas elementų, būtinų siekiant informuoti visuomenę apie neišvengiamą ir didelį pavojų tarpvalstybiniams elektros energijos srautams ir galimas švelninimo priemones;

c) apsaugo informacijos rengėjo ir subjektų, kurie tokią informaciją tvarkė pagal šį reglamentą, tapatybę.

8. Nukrypstant nuo šio straipsnio 6 dalies, kompetentingos institucijos gali teikti pagal šį reglamentą pateiktą, gautą ar perduotą informaciją, taip pat informaciją, kuria pasikeista, 2 straipsnio 1 dalyje nenurodytai trečiajai šaliai be išankstinio raštiško informacijos rengėjo sutikimo, tačiau apie tai kuo anksčiau jį informuoja. Prieš atskleisdama bet kokią pagal šį reglamentą pateiktą, gautą ar perduotą informaciją, taip pat informaciją, kuria pasikeista, 2 straipsnio 1 dalyje nenurodytai trečiajai šaliai, atitinkama kompetentinga institucija pagrįstai užtikrina, kad ta trečioji šalis žinotų galiojančias saugumo taisykles, ir gauna pagrįstą patikinimą, kad ta trečioji šalis gali apsaugoti gautą informaciją pagal šio straipsnio 1–5 dalis. Kompetentinga institucija tokią informaciją suanonimina, neprarasdama elementų, būtinų siekiant informuoti visuomenę apie neišvengiamą ir didelį pavojų tarpvalstybiniams elektros energijos srautams ir galimas švelninimo priemones, ir apsaugo informacijos rengėjo tapatybę. Šiuo atveju 2 straipsnio 1 dalyje nenurodyta trečioji šalis apsaugo gautą informaciją pagal subjekto lygmeniu jau galiojančias nuostatas arba, jei tai neįmanoma, atitinkamos kompetentingos institucijos pateiktas nuostatas ir nurodymus.

9. Šis straipsnis netaikomas 2 straipsnio 1 dalyje nenurodytiems subjektams, kuriems informacija teikiama pagal šio straipsnio 6 dalį. Šiuo atveju taikoma šio straipsnio 7 dalis arba kompetentinga institucija gali pateikti tam subjektui rašytines nuostatas, taikytinas tais atvejais, kai informacija gaunama pagal šį reglamentą.

47 straipsnis

Informacijos konfidencialumas

1. Bet kokiai pagal šį reglamentą teikiamai, gautai ar perduodamai informacijai, taip pat informacijai, kuria keičiamasi, taikomos šio reglamento šio straipsnio 2–5 dalyse nustatytos profesinės paslapties sąlygos ir Reglamento (ES) 2019/943 65 straipsnyje nustatyti reikalavimai. Bet kokia informacija, kurią šio reglamento 2 straipsnyje išvardyti subjektai pateikė, gavo ar perdavė, taip pat informacija, kuria buvo pasikeista šiam reglamentui įgyvendinti, apsaugoma atsižvelgiant į informacijos rengėjo taikomo informacijos konfidencialumo lygį.

2. Pareiga saugoti profesinę paslaptį taikoma 2 straipsnyje išvardytiems subjektams.

3. Už kibernetinį saugumą atsakingos NKI, NRI, už pasirengimą valdyti riziką atsakingos NKI ir CSIRT keičiasi visa savo užduotims atlikti būtina informacija.

4. Visa informacija, kurią 23 straipsniui įgyvendinti gauna ar perduoda 2 straipsnio 1 dalyje išvardyti subjektai, taip pat informacija, kuria jie keičiasi tarpusavyje, suanoniminama ir apibendrinama.

5. Informacijos, kurią bet kuris subjektas ar institucija, kuriems taikomas šis reglamentas, gauna vykdydami savo pareigas, negalima atskleisti jokiam kitam subjektui ar institucijai, nedarant poveikio atvejams, nustatytiems nacionalinės teisės aktuose, kitose šio reglamento nuostatose arba kituose atitinkamuose Sąjungos teisės aktuose.

6. Nedarant poveikio nacionalinės ar Sąjungos teisės aktų taikymui, institucija, subjektas arba fizinis asmuo, gavęs informaciją pagal šį reglamentą, negali jos naudoti jokiais kitais tikslais, išskyrus pagal šį reglamentą nustatytų pareigų vykdymą.

7. ACER, pasikonsultavusi su ENISA, visomis kompetentingomis institucijomis, ENTSO-E ir ES SSO subjektu, iki 2025 m. birželio 13 d. paskelbia gaires dėl 2 straipsnio 1 dalyje išvardytų subjektų keitimosi informacija mechanizmų, visų pirma numatomų informacijos srautų, ir informacijos anoniminimo bei apibendrinimo įgyvendinant šį straipsnį metodų.

8. Informacija, kuri yra konfidenciali pagal Sąjungos ir nacionalines taisykles, keičiamasi su Komisija ir kitomis atitinkamomis institucijomis tik kai ja keistis būtina taikant šį reglamentą. Keičiamasi tik tokia informacija, kuri yra būtina ir proporcinga atsižvelgiant į to keitimosi tikslą. Keičiantis informacija išsaugomas tos informacijos konfidencialumas ir apsaugomas ypatingos svarbos poveikio arba didelio poveikio subjektų saugumas ir komerciniai interesai.

VIII SKYRIUS

BAIGIAMOSIOS NUOSTATOS

48 straipsnis

Laikinos nuostatos

1. Kol bus patvirtintos 6 straipsnio 2 dalyje nurodytos nuostatos ir sąlygos ar metodikos arba 6 straipsnio 3 dalyje nurodyti planai, ENTSO-E, bendradarbiaudamas su ES SSO subjektu, parengia neprivalomas gaires dėl:

a) preliminaraus kibernetinių incidentų poveikio elektros energijos srautams indekso (KIPEI) pagal šio straipsnio 2 dalį;

b) preliminaraus Sąjungos masto didelio poveikio ir ypatingos svarbos poveikio procesų sąrašo pagal šio straipsnio 4 dalį ir

c) preliminarus Europos ir tarptautinių standartų ir kontrolės priemonių, kurių reikalaujama pagal nacionalinės teisės aktus, aktualių tarpvalstybinių elektros energijos srautų kibernetinio saugumo aspektams, sąrašo pagal šio straipsnio 6 dalį.

2. Iki 2024 m. spalio 13 d. ENTSO-E, bendradarbiaudamas su ES SSO subjektu, parengia rekomendaciją dėl preliminaraus KIPEI. ENTSO-E, bendradarbiaudamas su ES SSO subjektu, rekomenduojamą preliminarų KIPEI praneša kompetentingoms institucijoms.

3. Po keturių mėnesių nuo rekomenduojamo preliminaraus KIPEI gavimo arba ne vėliau kaip 2025 m. vasario 13 d. kompetentingos institucijos, remdamosi rekomenduojamu KIPEI, nustato kandidatus į didelio poveikio ir ypatingos svarbos poveikio subjektus savo valstybėje narėje ir parengia preliminarų didelio poveikio ir ypatingos svarbos poveikio subjektų sąrašą. Preliminariame sąraše nurodyti didelio poveikio ir ypatingos svarbos poveikio subjektai gali savanoriškai vykdyti šiame reglamente nustatytas savo pareigas, remdamiesi atsargumo principu. Iki 2025 m. kovo 13 d. kompetentingos institucijos preliminariame sąraše nurodytiems subjektams praneša, kad jie identifikuoti kaip didelio poveikio arba ypatingos svarbos poveikio subjektai.

4. Iki 2024 m. gruodžio 13 d. ENTSO-E, bendradarbiaudamas su ES SSO subjektu, parengia preliminarų Sąjungos masto didelio poveikio ir ypatingos svarbos poveikio procesų sąrašą. Pagal 3 dalį informuoti subjektai, kurie, vadovaudamiesi atsargumo principu, nusprendžia savanoriškai vykdyti šiame reglamente nustatytas savo pareigas, naudojasi preliminariu didelio poveikio ir ypatingos svarbos poveikio procesų sąrašu, kad nustatytų preliminarius didelio poveikio ir ypatingos svarbos poveikio perimetrus ir turtą, kuris turi būti įtrauktas į pirmąjį subjekto lygmens kibernetinio saugumo rizikos vertinimą.

5. Iki 2024 m. rugsėjo 13 d. kiekviena kompetentinga institucija pagal 4 straipsnio 1 dalį ENTSO-E ir ES SSO subjektui pateikia savo nacionalinės teisės aktų, aktualių tarpvalstybinių elektros energijos srautų kibernetinio saugumo aspektams, sąrašą.

6. Iki 2025 m. birželio 13 d. ENTSO-E, bendradarbiaudamas su ES SSO subjektu, parengia preliminarų Europos ir tarptautinių standartų ir kontrolės priemonių, kurių reikalaujama pagal tarpvalstybinių elektros energijos srautų kibernetinio saugumo aspektams aktualius nacionalinės teisės aktus, sąrašą, atsižvelgdamas į kompetentingų institucijų pateiktą informaciją.

7. Į preliminarų Europos ir tarptautinių standartų ir kontrolės priemonių sąrašą įtraukiama:

a) Europos ir tarptautiniai standartai ir nacionalinės teisės aktai, kuriuose pateikiamos subjekto lygmens kibernetinio saugumo rizikos valdymo metodikos gairės, ir

b) kibernetinio saugumo kontrolės priemonės, lygiavertės kontrolės priemonėms, kurios, kaip tikimasi, bus įtrauktos į būtinąją ir sustiprintą kibernetinio saugumo kontrolę.

8. ENTSO-E ir ES SSO subjektas, baigdami rengti preliminarų standartų sąrašą, atsižvelgia į ENISA ir ACER pateiktas nuomones. ENTSO-E ir ES SSO subjektas pereinamojo laikotarpio Europos ir tarptautinių standartų ir kontrolės priemonių sąrašą skelbia savo interneto svetainėse.

9. ENTSO-E ir ES SSO subjektas konsultuojasi su ENISA ir ACER dėl pagal 1 dalį rengiamų neprivalomų gairių pasiūlymų.

10. Kol pagal 29 straipsnį bus parengtos ir pagal 8 straipsnį patvirtintos būtinosios ir sustiprintos kibernetinio saugumo kontrolės priemonės, visi 2 straipsnio 1 dalyje išvardyti subjektai stengiasi laipsniškai taikyti pagal 1 dalį parengtas neprivalomas gaires.

49 straipsnis

Įsigaliojimas

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2024 m. kovo 11 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN