Europos Sąjungos
oficialusis leidinys

LT
L serija

2025/38

2025 1 15

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS (ES) 2025/38

2024 m. gruodžio 19 d.

kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės ir iš dalies keičiamas Reglamentas (ES) 2021/694 (Kibernetinio solidarumo aktas)

EUROPOS PARLAMENTAS IR EUROPOS SĄJUNGOS TARYBA,

atsižvelgdami į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 173 straipsnio 3 dalį ir į 322 straipsnio 1 dalies a punktą,

atsižvelgdami į Europos Komisijos pasiūlymą,

teisėkūros procedūra priimamo akto projektą perdavus nacionaliniams parlamentams,

atsižvelgdami į Audito Rūmų nuomonę ([1]),

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę ([2]),

atsižvelgdami į Regionų komiteto nuomonę ([3]),

laikydamiesi įprastos teisėkūros procedūros ([4]),

kadangi:

(1) informacinių ir ryšių technologijų naudojimas ir priklausomumas nuo jų tapo esminiais visų ekonominės veiklos sektorių ir visuomenės aspektais, nes valstybių narių viešojo administravimo institucijos, įmonės ir piliečiai įvairiuose sektoriuose ir įvairiose valstybėse yra vis labiau susieti tarpusavyje ir vieni nuo kitų priklausomi, o dėl to kartu atsiranda ir pažeidžiamumo galimybių;

(2) kibernetinio saugumo incidentų, įskaitant tiekimo grandinės išpuolius kibernetinio šnipinėjimo vykdymo, išpirkos reikalavimo programinės įrangos arba veiklos sutrikdymo tikslais, mastas, dažnumas ir poveikis didėja Sąjungos ir pasaulio mastu. Tai kelia didelę grėsmę tinklų ir informacinių sistemų veikimui. Atsižvelgiant į sparčiai kintančias grėsmių aplinkybes, dėl galimų didelio masto kibernetinio saugumo incidentų, dėl kurių gali kilti didelių sutrikimų ar būti padaryta žala ypatingos svarbos infrastruktūros objektams, grėsmės reikia didinti Sąjungos kibernetinio saugumo sistemos parengtį. Ta grėsmė yra susijusi ne vien su Rusijos agresijos karu prieš Ukrainą ir ji, tikėtina, išliks, atsižvelgiant į tai, kad dabartinę geopolitinę įtampą lemia daugybė veikėjų. Tokie incidentai gali trukdyti teikti viešąsias paslaugas, nes kibernetiniai išpuoliai yra dažnai nukreipti į vietos, regionines ar nacionalines viešąsias paslaugas ir infrastruktūrą, o vietos valdžios institucijos yra ypač pažeidžiamos, be kita ko, dėl ribotų išteklių. Jie taip pat gali trukdyti vykdyti ekonominę veiklą, be kita ko, ypatingos svarbos ar kituose itin svarbiuose sektoriuose, sukelti didelių finansinių nuostolių, pakenkti naudotojų pasitikėjimui, padaryti didelės žalos Sąjungos ekonomikai ir demokratinėms sistemoms, o jų padariniai gali būti pavojingi net žmonių sveikatai ar gyvybei. Be to, kibernetinio saugumo incidentai yra nenuspėjami, nes dažnai kyla ir išsiplėtoja greitai, nėra susiję su jokia konkrečia geografine teritorija ir vyksta vienu metu arba akimirksniu išplinta daugelyje valstybių. Būtinas glaudus ir koordinuotas viešojo sektoriaus, privačiojo sektoriaus, akademinės bendruomenės, pilietinės visuomenės ir žiniasklaidos bendradarbiavimas;

(3) būtina stiprinti Sąjungos pramonės ir paslaugų sektorių konkurencinę padėtį skaitmeninėje ekonomikoje ir remti jų skaitmeninę transformaciją, didinant kibernetinio saugumo lygį bendrojoje skaitmeninėje rinkoje, kaip rekomenduojama trijuose skirtinguose Konferencijos dėl Europos ateities pasiūlymuose. Būtina didinti piliečių, įmonių, įskaitant labai mažas įmones, mažąsias ir vidutines įmones bei startuolius, ir subjektų, valdančių ypatingos svarbos infrastruktūros objektus, atsparumą didėjančioms kibernetinėms grėsmėms, kurios gali turėti pražūtingą poveikį visuomenei ir ekonomikai. Todėl reikia investuoti į infrastruktūrą ir paslaugas ir stiprinti pajėgumus, kad

([1]) 2023 m. balandžio 18 d. nuomonė (dar nepaskelbta Oficialiajame leidinyje).
([2]) OL C 349, 2023 9 29, p. 167.
([3]) OL C, C/2024/1049, 2024 2 9, ELI: http://data.europa.eu/eli/C/2024/1049/oj.
([4]) 2024 m. balandžio 24 d. Europos Parlamento pozicija (dar nepaskelbta Oficialiajame leidinyje) ir 2024 m. gruodžio 2 d. Tarybos sprendimas.

būtų ugdomi kibernetinio saugumo įgūdžiai, kurie padėtų greičiau aptikti kibernetinio saugumo grėsmes bei incidentus ir į juos greičiau reaguoti. Be to, valstybėms narėms reikia pagalbos geriau pasirengti reikšmingiems kibernetinio saugumo incidentams ir didelio masto kibernetinio saugumo incidentams bei į juos reaguoti, taip pat pagalbos užtikrinant pradinį veiklos atkūrimą tokiems incidentams įvykus. Naudodamasi esamomis struktūromis ir glaudžiai su jomis bendradarbiaudama, Sąjunga taip pat turėtų didinti savo pajėgumus tose srityse, visų pirma, susijusius su duomenų apie kibernetines grėsmes ir incidentus rinkimu ir analize;

(4) Sąjunga jau ėmėsi tam tikrų priemonių, kuriomis siekiama sumažinti ypatingos svarbos infrastruktūros objektų ir subjektų pažeidžiamumą ir padidinti jų atsparumą kibernetinio saugumo rizikai, visų pirma priėmė Europos Parlamento ir Tarybos reglamentą (ES) 2019/881 ([5]), Europos Parlamento ir Tarybos direktyvas 2013/40/ES ([6]) bei (ES) 2022/2555 ([7]) ir Komisijos rekomendaciją (ES) 2017/1584 ([8]). Be to, 2022 m. gruodžio 8 d. Tarybos rekomendacijoje dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą valstybės narės raginamos imtis priemonių ir veiksmingai, solidariai bei koordinuotai bendradarbiauti tarpusavyje, su Komisija ir kitomis atitinkamomis valdžios institucijomis bei atitinkamais subjektais, siekiant padidinti ypatingos svarbos infrastruktūros objektų, naudojamų esminėms paslaugoms vidaus rinkoje teikti, atsparumą;

(5) dėl didėjančios kibernetinio saugumo rizikos ir apskritai sudėtingos grėsmių aplinkos, kai yra aiški rizika, kad incidentai greitai išplis iš vienos valstybės narės į kitą ir iš trečiosios valstybės į Sąjungą, reikia stiprinti solidarumą Sąjungos lygmeniu, kad būtų galima geriau aptikti kibernetines grėsmes ir incidentus, jiems pasirengti, į juos reaguoti ir po jų atkurti veiklą, visų pirma stiprinant esamų struktūrų pajėgumus. Be to, 2022 m. gegužės 23 d. Tarybos išvadose dėl Europos Sąjungos pozicijos kibernetiniais klausimais paragino Komisiją pateikti pasiūlymą dėl naujo Reagavimo į kibernetinio saugumo krizes fondo;

(6) 2022 m. lapkričio 10 d. Komisijos ir Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai bendrame komunikate Europos Parlamentui ir Tarybai dėl ES kibernetinės gynybos politikos paskelbta ES kibernetinio solidarumo iniciatyva, kuria siekiama šių tikslų: stiprinti bendrus ES aptikimo, informuotumo apie padėtį ir reagavimo pajėgumus, skatinant diegti ES saugumo operacijų centrų (toliau – SOC) infrastruktūrą, remiant laipsnišką ES lygmens kibernetinių išteklių rezervo kūrimą, pasitelkiant patikimų privačių paslaugų teikėjų paslaugas, ir ypatingos svarbos subjektų galimo pažeidžiamumo testavimą ES rizikos vertinimų pagrindu;

(7) būtina stiprinti kibernetinių grėsmių ir incidentų aptikimą ir informuotumą apie padėtį visoje Sąjungoje, taip pat stiprinti solidarumą didinant valstybių narių ir Sąjungos parengtį bei pajėgumus užkirsti kelią reikšmingiems kibernetinio saugumo incidentams ir didelio masto kibernetinio saugumo incidentams ir į juos reaguoti. Todėl, siekiant plėtoti koordinuotus aptikimo ir informuotumo apie padėtį pajėgumus, turėtų būti sukurtas Europos masto kibernetinio saugumo centrų tinklas (toliau – Europos kibernetinio saugumo įspėjimų sistema), kuris sustiprintų Sąjungos grėsmių aptikimo ir dalijimosi informacija pajėgumus; turėtų būti sukurtas Reagavimo į kibernetinio saugumo krizes mechanizmas, siekiant padėti valstybėms narėms, joms paprašius, pasirengti reikšmingiems kibernetinio saugumo incidentams ir didelio masto kibernetinio saugumo incidentams, į juos reaguoti, sumažinti jų padarinius ir po jų inicijuoti veiklos atkūrimą, ir siekiant padėti kitiems naudotojams pasirengti reikšmingiems kibernetinio saugumo incidentams ir didelio masto incidentams lygiaverčiams kibernetinio saugumo incidentams; ir turėtų būti sukurtas Europos kibernetinio saugumo incidentų peržiūros mechanizmas, kad būtų galima peržiūrėti ir įvertinti konkrečius reikšmingus kibernetinio saugumo incidentus arba didelio masto kibernetinio saugumo incidentus. Veiksmai, kurių imtasi pagal šį reglamentą, turėtų būti vykdomi tinkamai atsižvelgiant į valstybių narių kompetenciją ir jais turėtų būti papildoma, o ne dubliuojama CSIRT tinklo, Europos ryšių palaikymo dėl kibernetinių krizių organizacinį tinklo (EU-CyCLONe) ar Bendradarbiavimo grupės (toliau – TIS Bendradarbiavimo grupė), kurie visi įsteigti pagal Direktyvą (ES) 2022/2555, vykdoma veikla. Tais veiksmais nedaromas poveikis Sutarties dėl Europos Sąjungos veikimo (SESV) 107 ir 108 straipsniams;

([5]) 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).

([6]) 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (OL L 218, 2013 8 14, p. 8).

([7]) 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).

([8]) 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).

(8) siekiant tų tikslų taip pat būtina tam tikrose srityse iš dalies pakeisti Europos Parlamento ir Tarybos reglamentą (ES) 2021/694 ([9]). Visų pirma šiuo reglamentu turėtų būti iš dalies pakeistas Reglamentas (ES) 2021/694, siekiant įtraukti naujus veiklos tikslus, susijusius su Europos kibernetinio saugumo įspėjimų sistema ir Reagavimo į kibernetinio saugumo krizes mechanizmu pagal Skaitmeninės Europos programos (SEP) 3-iąjį konkretų tikslą, kuriuo siekiama užtikrinti bendrosios skaitmeninės rinkos atsparumą, vientisumą ir patikimumą, stiprinti kibernetinių išpuolių ir kibernetinių grėsmių stebėsenos bei reagavimo į juos pajėgumus ir stiprinti tarpvalstybinį bendradarbiavimą ir koordinavimą kibernetinio saugumo srityje. Europos kibernetinio saugumo įspėjimų sistema galėtų atlikti svarbų vaidmenį padedant valstybėms narėms numatyti kibernetines grėsmes ir nuo jų apsisaugoti, o ES kibernetinio saugumo rezervas galėtų atlikti svarbų vaidmenį padedant valstybėms narėms, Sąjungos institucijoms, organams, įstaigoms ir agentūroms bei SEP asocijuotosioms trečiosioms valstybėms reaguoti į reikšmingus kibernetinio saugumo incidentus, didelio masto kibernetinio saugumo incidentus ir didelio masto incidentams lygiaverčius kibernetinio saugumo incidentus ir mažinti jų padarinius. Tie padariniai galėtų apimti didelę materialinę ar nematerialinę žalą ir didelį pavojų visuomenės saugumui ir saugai. Atsižvelgiant į konkrečius vaidmenis, kuriuos galėtų atlikti Europos kibernetinio saugumo įspėjimų sistema ir ES kibernetinio saugumo rezervas, šiuo reglamentu turėtų būti iš dalies pakeistos Reglamento (ES) 2021/694 nuostatos dėl Sąjungoje įsisteigusių, bet iš trečiųjų valstybių kontroliuojamų teisės subjektų dalyvavimo, kai esama realios rizikos, kad Sąjungoje nebus reikiamų ir pakankamų priemonių, infrastruktūros ir paslaugų arba technologijų, ekspertinių žinių ir pajėgumų, o tokių subjektų įtraukimo nauda nusveria saugumo riziką. Turėtų būti nustatytos konkrečios sąlygos, kuriomis veiksmams, kuriais įgyvendinama Europos kibernetinio saugumo įspėjimų sistema ir ES kibernetinio saugumo rezervas, gali būti teikiama finansinė parama ir turėtų būti apibrėžti numatytiems tikslams pasiekti būtini valdymo ir koordinavimo mechanizmai. Kiti Reglamento (ES) 2021/694 pakeitimai turėtų apimti siūlomų veiksmų pagal naujus veiklos tikslus aprašymus, taip pat išmatuojamus tų naujų veiklos tikslų įgyvendinimo stebėsenos rodiklius;

(9) siekiant sustiprinti Sąjungos atsaką į kibernetinio saugumo grėsmes, labai svarbus bendradarbiavimas su tarptautinėmis organizacijomis ir patikimais, panašiai mąstančiais tarptautiniais partneriais. Tomis aplinkybėmis patikimi, panašiai mąstantys tarptautiniai partneriai turėtų būti suprantami kaip valstybės, kurios laikosi principų, kuriais grindžiamas Sąjungos sukūrimas: demokratijos, teisinės valstybės, žmogaus teisių ir pagrindinių laisvių visuotinumo ir nedalomumo, pagarbos žmogaus orumui, lygybės ir solidarumo principų, taip pat kurios laikosi Jungtinių Tautų Chartijos ir tarptautinės teisės principų ir kurios nekenkia esminiams Sąjungos ar jos valstybių narių saugumo interesams. Toks bendradarbiavimas taip pat galėtų būti naudingas veiksmams, kurių imamasi pagal šį reglamentą, visų pirma Europos kibernetinio saugumo įspėjimų sistemai ir ES kibernetinio saugumo rezervui. Reglamente (ES) 2021/694 turėtų būti nustatyta, kad jei įvykdomos tam tikros prieinamumo ir saugumo sąlygos, konkursai dėl Europos kibernetinio saugumo įspėjimų sistemos ir ES kibernetinio saugumo rezervo turi būti atviri iš trečiųjų valstybių kontroliuojamiems juridiniams asmenims, jei laikomasi saugumo reikalavimų. Vertinant saugumo riziką, susijusią su tokiu viešųjų pirkimų atvėrimu, svarbu atsižvelgti į principus ir vertybes, kuriais vadovaujasi Sąjunga ir jos panašiai mąstantys tarptautiniai partneriai, kai tie principai ir vertybės yra susiję su esminiais Sąjungos saugumo interesais. Be to, kai tokie saugumo reikalavimai svarstomi pagal Reglamentą (ES) 2021/694, būtų galima atsižvelgti į kelis elementus, pavyzdžiui, subjekto organizacinę struktūrą ir sprendimų priėmimo procesą, duomenų ir įslaptintos arba neskelbtinos informacijos saugumą ir užtikrinimą, kad reikalavimų neatitinkančios trečiosios valstybės netikrintų veiksmo rezultatų ar jų neribotų;

(10) veiksmų finansavimas pagal šį reglamentą turėtų būti numatytas Reglamente (ES) 2021/694, kuris turėtų ir toliau būti svarbus pagrindinis teisės aktas dėl veiksmų, įtvirtintų SEP 3-iame konkrečiame tiksle. Konkrečios dalyvavimo kiekviename veiksme sąlygos turi būti numatytos atitinkamose darbo programose laikantis Reglamento (ES) 2021/694;

(11) šiam reglamentui taikomos Europos Parlamento ir Tarybos pagal SESV 322 straipsnį priimtos horizontaliosios finansinės taisyklės. Tos taisyklės išdėstytos Europos Parlamento ir Tarybos reglamente (ES, Euratomas) 2024/2509 ([10]) – visų pirma jomis nustatoma Sąjungos biudžeto sudarymo ir įgyvendinimo tvarka ir numatoma finansų pareigūnų atsakomybės kontrolė. Pagal SESV 322 straipsnį priimtos taisyklės taip pat apima

([9]) 2021 m. balandžio 29 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/694, kuriuo nustatoma Skaitmeninės Europos programa ir panaikinamas Sprendimas (ES) 2015/2240 (OL L 166, 2021 5 11, p. 1).

([10]) 2024 m. rugsėjo 23 d. Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) 2024/2509 dėl Sąjungos bendrajam biudžetui taikomų finansinių taisyklių (OL L, 2024/2509, 2024 9 26, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

bendrąją Sąjungos biudžeto apsaugos sąlygų sistemą, kaip nustatyta Europos Parlamento ir Tarybos reglamentu (ES, Euratomas) 2020/2092 ([11]);

(12) nors prevencijos ir pasirengimo priemonės yra būtinos siekiant padidinti Sąjungos atsparumą reaguojant į reikšmingus kibernetinio saugumo incidentus, didelio masto kibernetinio saugumo incidentus ir didelio masto incidentams lygiaverčius kibernetinio saugumo incidentus, tokių incidentų atsiradimas, laikas ir mastas dėl savo pobūdžio yra nenuspėjami. Finansiniai ištekliai, kurių reikia adekvačiam atsakui užtikrinti, gali įvairiais metais labai skirtis ir juos turėtų būti galima panaudoti nedelsiant. Todėl, derinant biudžeto nuspėjamumo principą su būtinumu greitai reaguoti į naujus poreikius, reikia koreguoti finansinį darbo programų įgyvendinimą. Todėl, papildant asignavimų perkėlimus, leidžiamus pagal Reglamento (ES, Euratomas) 2024/2509 12 straipsnio 4 dalį, tikslinga leisti nepanaudotus asignavimus perkelti tik į kitus metus ir juos skirti tik ES kibernetinio saugumo rezervui ir savitarpio pagalbos rėmimo veiksmams;

(13) siekiant veiksmingiau užkirsti kelią kibernetinėms grėsmėms ir incidentams, juos įvertinti, į juos reaguoti ir po jų atsigauti, būtina kaupti daugiau žinių apie Sąjungos teritorijoje esančiam ypatingos svarbos turtui ir infrastruktūros objektams kylančias grėsmes, įskaitant jų geografinį pasiskirstymą, sąsajas ir galimą poveikį kibernetinių išpuolių, darančių poveikį tiems infrastruktūros objektams, atveju. Proaktyvus požiūris į kibernetinių grėsmių nustatymą, mažinimą ir prevenciją apima didesnius pažangių aptikimo gebėjimų pajėgumus. Europos kibernetinio saugumo įspėjimų sistemą turėtų sudaryti keli tarpusavyje susiję tarpvalstybiniai kibernetinio saugumo centrai, iš kurių kiekvienas apjungia tris ar daugiau nacionalinių kibernetinio saugumo centrų. Ta infrastruktūra turėtų atitikti nacionalinius ir Sąjungos kibernetinio saugumo interesus ir poreikius, naudojant naujausias pažangaus svarbių ir, kai tinkama, anonimizuotų duomenų ir informacijos rinkimo bei analizės priemonių technologijas, stiprinant koordinuotus kibernetinio saugumo grėsmių aptikimo ir valdymo pajėgumus ir užtikrinant informuotumą apie padėtį tikruoju laiku. Ta infrastruktūra turėtų padėti gerinti kibernetinio saugumo padėtį, didinant duomenų ir informacijos aptikimą, kaupimą ir analizę, siekiant užkirsti kelią kibernetinio saugumo grėsmėms ir incidentams, ir taip papildyti ir remti už kibernetinių krizių valdymą Sąjungoje atsakingus Sąjungos subjektus ir tinklus, visų pirma EU-CyCLONe;

(14) valstybių narių dalyvavimas Europos kibernetinio saugumo įspėjimų sistemoje yra savanoriškas. Kiekviena valstybė narė nacionaliniu lygmeniu turėtų paskirti vieną subjektą, kuriam būtų pavesta koordinuoti kibernetinių grėsmių aptikimo veiklą toje valstybėje narėje. Tie nacionaliniai kibernetinio saugumo centrai turėtų veikti kaip nacionalinis atskaitos taškas, nuo kurio nacionaliniu lygmeniu atsiveria galimybė dalyvauti Europos kibernetinio saugumo įspėjimų sistemos veikloje, ir jie turėtų užtikrinti, kad iš viešųjų ir privačių subjektų gauta informacija apie kibernetines grėsmes būtų veiksmingai ir racionaliai dalijamasi ir ji būtų renkama nacionaliniu lygmeniu. Nacionaliniai kibernetinio saugumo centrai galėtų stiprinti viešųjų ir privačiųjų subjektų bendradarbiavimą ir dalijimąsi informacija, jie taip pat galėtų remti keitimąsi atitinkamais duomenimis ir informacija su atitinkamomis sektorių ir tarpsektorinėmis bendruomenėmis, įskaitant atitinkamų pramonės sektorių dalijimosi informacija ir jos analizės centrus (ISAC). Glaudus ir koordinuotas viešųjų ir privačių subjektų bendradarbiavimas yra labai svarbus stiprinant Sąjungos kibernetinį atsparumą. Toks bendradarbiavimas ypač vertingas dalijantis kibernetinių grėsmių žvalgybos informacija, siekiant pagerinti aktyvią kibernetinę apsaugą. Vykdydami tokį bendradarbiavimą ir keitimąsi informacija, nacionaliniai kibernetinio saugumo centrai galėtų prašyti konkrečios informacijos ir ją gauti. Tie nacionaliniai kibernetinio saugumo centrai nėra pagal šį reglamentą nei įpareigoti, nei įgalioti užtikrinti tokių prašymų vykdymą. Kai tinkama ir laikantis Sąjungos ir nacionalinės teisės, informacija, kurios prašoma arba kuri gaunama, galėtų apimti telemetrijos, jutiklių ir registravimo duomenis iš subjektų, pavyzdžiui, valdomų saugumo paslaugų teikėjų, vykdančių veiklą ypatingos svarbos sektoriuose arba kituose itin svarbiuose sektoriuose toje valstybėje narėje, kad būtų pagerintas spartus galimų kibernetinių grėsmių ir incidentų nustatymas ankstyvuoju etapu ir taip būtų didinamas informuotumas apie padėtį. Jei nacionalinis kibernetinio saugumo centras nėra kompetentinga institucija, kurią atitinkama valstybė narė paskyrė arba įsteigė pagal Direktyvos (ES) 2022/2555 8 straipsnio 1 dalį, labai svarbu, kad jis koordinuotų veiksmus su ta kompetentinga institucija dėl prašymų pateikti tokius duomenis ir jų gavimo;

(15) pagal Europos kibernetinio saugumo įspėjimų sistemą turėtų būti įsteigti keli tarpvalstybiniai kibernetinio saugumo centrai. Tie tarpvalstybiniai kibernetinio saugumo centrai turėtų suburti nacionalinius kibernetinio saugumo centrus iš bent trijų valstybių narių, kad būtų galima visapusiškai pasinaudoti tarpvalstybinio grėsmių aptikimo, dalijimosi informacija ir valdymo privalumais. Bendras tarpvalstybinių kibernetinio saugumo centrų tikslas turėtų būti stiprinti

([11]) 2020 m. gruodžio 16 d. Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) 2020/2092 dėl bendro Sąjungos biudžeto apsaugos sąlygų režimo (OL L 433 I, 2020 12 22, p. 1, ELI: https://eur-lex.europa.eu/eli/reg/2020/2092/oj).

gebėjimus analizuoti kibernetinio saugumo grėsmes, užkirsti joms kelią bei jas aptikti ir remti kokybiškos kibernetinių grėsmių žvalgybos informacijos rengimą, visų pirma patikimoje ir saugioje aplinkoje dalijantis svarbia ir, kai tinkama, anonimizuota informacija iš įvairių viešųjų ar privačių šaltinių, taip pat dalijantis naujausiomis priemonėmis ir jas bendrai naudojant, ir bendrai plėtojant aptikimo, analizės ir prevencijos pajėgumus patikimoje ir saugioje aplinkoje. Tarpvalstybiniai kibernetinio saugumo centrai turėtų suteikti naujų papildomų pajėgumų, kurie remsis esamų SOC ir CSIRT bei kitų atitinkamų subjektų, įskaitant CSIRT tinklą, veikla ir ją papildys;

(16) valstybė narė, kurią Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras (ECCC), įsteigtas Europos Parlamento ir Tarybos reglamentu (ES) 2021/887 ([12]), atrinko po kvietimo pareikšti susidomėjimą įsteigti nacionalinį kibernetinio saugumo centrą arba padidinti jo pajėgumus, turėtų kartu su ECCC pirkti atitinkamas priemones, infrastruktūrą arba paslaugas. Tokia valstybė narė turėtų turėti teisę gauti dotaciją priemonėms ir infrastruktūrai eksploatuoti ar paslaugoms teikti. Prieglobos konsorciumas, kurį sudaro bent trys valstybės narės ir kurį po kvietimo pareikšti susidomėjimą įsteigti tarpvalstybinį kibernetinio saugumo centrą arba padidinti jo pajėgumus atrenka ECCC, turėtų kartu su ECCC pirkti atitinkamas priemones, infrastruktūrą ar paslaugas. Prieglobos konsorciumas turėtų turėti teisę gauti dotaciją priemonėms ir infrastruktūrai eksploatuoti ar paslaugoms teikti. Atitinkamų priemonių, infrastruktūros ar paslaugų pirkimo procedūrą turėtų bendrai vykdyti ECCC ir po tokių kvietimų pareikšti susidomėjimą atrinktos atitinkamos valstybių narių perkančiosios organizacijos. Tokie viešieji pirkimai turėtų atitikti Reglamento (ES, Euratomas) 2024/2509 168 straipsnio 2 dalį ir ECCC finansines taisykles. Todėl privatūs subjektai neturėtų turėti teisės dalyvauti kvietimuose pareikšti susidomėjimą pirkti priemones, infrastruktūrą arba paslaugas kartu su ECCC arba gauti dotacijas toms priemonėms ir infrastruktūrai eksploatuoti arba paslaugoms teikti. Tačiau valstybės narės, laikydamosi Sąjungos ir nacionalinės teisės, turėtų galėti į savo nacionalinių kibernetinio saugumo centrų ir tarpvalstybinio kibernetinio saugumo centrų kūrimą, stiprinimą ir veikimą įtraukti privačius subjektus kitais būdais, kuriuos jos laiko tinkamais. Privatūs subjektai taip pat galėtų būti laikomi tinkamais gauti Sąjungos finansavimą pagal Reglamentą (ES) 2021/887, siekiant teikti paramą nacionaliniams kibernetinio saugumo centrams;

(17) siekiant padidinti kibernetinių grėsmių aptikimą ir informuotumą apie padėtį Sąjungoje, valstybė narė, kuri buvo atrinkta paskelbus kvietimą pareikšti susidomėjimą įsteigti nacionalinį kibernetinio saugumo centrą arba padidinti jo pajėgumus, turėtų įsipareigoti teikti paraišką dalyvauti tarpvalstybinio kibernetinio saugumo centro veikloje. Jei valstybė narė per dvejus metus nuo priemonių, infrastruktūros ar paslaugų įsigijimo arba dotacijos gavimo dienos, priklausomai nuo to, kas įvyko anksčiau, netampa tarpvalstybinio kibernetinio saugumo centro dalyve, ji neturėtų turėti teisės dalyvauti tolesniuose Sąjungos paramos veiksmuose pagal Europos kibernetinį saugumo įspėjimų sistemą, kad būtų didinami jos nacionalinio kibernetinio saugumo centro pajėgumai. Tokiais atvejais valstybių narių subjektai vis tiek galėtų dalyvauti kvietimuose teikti pasiūlymus kitomis temomis pagal SEP ar kitas Sąjungos finansavimo programas, įskaitant kvietimus teikti pasiūlymus dėl kibernetinių grėsmių aptikimo ir dalijimosi informacija pajėgumų, su sąlyga, kad tie subjektai atitinka tose programose nustatytus tinkamumo kriterijus;

(18) CSIRT tarnybos keičiasi informacija CSIRT tinkle pagal Direktyvą (ES) 2022/2555. Europos kibernetinio saugumo įspėjimų sistema turėtų tapti nauju pajėgumu, papildančiu CSIRT tinklą, padėdama didinti Sąjungos informuotumą apie padėtį ir taip sudarydama sąlygas stiprinti CSIRT tinklo pajėgumus. Tarpvalstybiniai kibernetinio saugumo centrai turėtų koordinuoti veiksmus ir glaudžiai bendradarbiauti su CSIRT tinklu. Jie turėtų veikti kaupdami duomenis ir dalydamiesi svarbia ir, kai tinkama, anonimizuota viešųjų ir privačių subjektų pateikta informacija apie kibernetines grėsmes, didindami tokių duomenų ir informacijos vertę pasitelkiant ekspertų analizę ir bendrai įsigytas infrastruktūras bei pažangiausias priemones ir prisidėdami prie Sąjungos technologinio suverenumo, jos atviro strateginio savarankiškumo, konkurencingumo bei atsparumo ir Sąjungos pajėgumų plėtojimo;

(19) tarpvalstybiniai kibernetinio saugumo centrai turėtų veikti kaip centriniai punktai, leidžiantys sutelkti daug svarbių duomenų ir kibernetinių grėsmių žvalgybos informaciją, ir sudaryti sąlygas skleisti informaciją apie grėsmes dideliam įvairių suinteresuotųjų subjektų ratui, pvz., kompiuterinių incidentų tyrimo tarnyboms (toliau – CERT), CSIRT, ISAC ir ypatingos svarbos infrastruktūros objektų operatoriams. Prieglobos konsorciumo nariai konsorciumo susitarime turėtų nurodyti atitinkamą informaciją, kuria turi dalytis atitinkamo tarpvalstybinio kibernetinio saugumo centro dalyviai. Informacija, kuria keičiasi tarpvalstybinio kibernetinio saugumo centro dalyviai, galėtų apimti, pavyzdžiui, tinklų ir jutiklių duomenis, grėsmių žvalgybos duomenų kanalus, užvaldymo rodiklius ir kontekstinę informaciją apie incidentus, kibernetines grėsmes, vos neįvykusius incidentus, pažeidžiamumus, metodus ir procedūras, priešišką

([12]) 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/887, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas (OL L 202, 2021 6 8, p. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

taktiką, konkrečią grėsmę keliančių subjektų informaciją, kibernetinio saugumo įspėjimus ir rekomendacijas dėl kibernetinio saugumo priemonių konfigūracijos siekiant aptikti kibernetinius išpuolius. Be to, tarpvalstybiniai kibernetinio saugumo centrai taip pat vieni su kitais turėtų sudaryti bendradarbiavimo susitarimus. Tuose bendradarbiavimo susitarimuose visų pirma turėtų būti nustatyti dalijimosi informacija principai ir sąveikumas. Jų sąlygos dėl sąveikumo, visų pirma dalijimosi informacija formatai ir protokolai, turėtų būti grindžiamos Europos Sąjungos kibernetinio saugumo agentūros, įsteigtos Reglamentu (ES) 2019/881, (toliau – ENISA) paskelbtomis gairėmis sąveikumo srityje, kurios turėtų būti laikomos atskaitos tašku. Tos gairės turėtų būti paskelbtos kuo greičiau siekiant užtikrinti, kad tarpvalstybiniai kibernetinio saugumo centrai galėtų į jas atsižvelgti ankstyvuoju etapu. Juose turėtų būti atsižvelgiama į tarptautinius standartus, geriausią praktiką ir visų įsteigtų tarpvalstybinių kibernetinio saugumo centrų veikimą;

(20) tarpvalstybiniai kibernetinio saugumo centrai ir CSIRT tinklas turėtų glaudžiai bendradarbiauti, kad būtų užtikrinta veiklos sinergija ir papildomumas. Tuo tikslu jie turėtų susitarti dėl procedūrinės bendradarbiavimo ir dalijimosi atitinkama informacija tvarkos. Tai galėtų apimti dalijimąsi atitinkama informacija apie kibernetines grėsmes ir reikšmingus kibernetinio saugumo incidentus ir užtikrinimą, kad su CSIRT tinklu būtų dalijamasi patirtimi, susijusia su pažangiausiomis priemonėmis, visų pirma dirbtiniu intelektu ir duomenų analizės technologijomis, naudojamomis tarpvalstybiniuose kibernetinio saugumo centruose;

(21) atitinkamų institucijų bendras informuotumas apie padėtį yra būtina Sąjungos masto parengties reikšmingiems kibernetinio saugumo incidentams ir didelio masto kibernetinio saugumo incidentams ir veiksmų koordinavimo sąlyga. Siekiant remti koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą operatyviniu lygmeniu ir užtikrinti reguliarų keitimąsi svarbia informacija tarp valstybių narių ir Sąjungos institucijų, organų, įstaigų ir agentūrų, Direktyva (ES) 2022/2555 buvo įsteigtas EU-CyCLONe. Direktyva (ES) 2022/2555 taip pat buvo įsteigtas CSIRT tinklas siekiant skatinti greitą ir veiksmingą operatyvinį visų valstybių narių bendradarbiavimą. Siekiant užtikrinti informuotumą apie padėtį ir sustiprinti solidarumą, tais atvejais, kai tarpvalstybiniai kibernetinio saugumo centrai gauna informacijos, susijusios su galimu arba vykstančiu didelio masto kibernetinio saugumo incidentu, jie turėtų teikti atitinkamą informaciją CSIRT tinklui ir pranešti EU-CyCLONe, pateikdami ankstyvąjį perspėjimą. Visų pirma, priklausomai nuo situacijos, informacija, kuria turi būti dalijamasi, galėtų apimti techninę informaciją, informaciją apie užpuoliko arba potencialaus užpuoliko pobūdį bei motyvus ir aukštesnio lygio netechninę informaciją apie galimą arba vykstantį didelio masto kibernetinio saugumo incidentą. Tomis aplinkybėmis reikėtų deramai atsižvelgti į būtinybės žinoti principą ir į galimai neskelbtiną informacijos, kuria dalijamasi, pobūdį. Direktyvoje (ES) 2022/2555 taip pat buvo pakartota Komisijos atsakomybė už Sąjungos civilinės saugos mechanizmą (toliau – SCSM), nustatytą Europos Parlamento ir Tarybos sprendimu Nr. 1313/2013/ES ([13]), taip pat jos atsakomybė už analitinių ataskaitų dėl integruoto politinio atsako į krizes mechanizmo (toliau – IPCR mechanizmas) teikimą pagal Tarybos įgyvendinimo sprendimą (ES) 2018/1993 ([14]). Kai tarpvalstybiniai kibernetinio saugumo centrai su EU-CyCLONe ir CSIRT tinklu dalijasi svarbia informacija ir ankstyvaisiais perspėjimais, susijusiais su galimu arba vykstančiu didelio masto kibernetinio saugumo incidentu, būtina, kad ta informacija tuose tinkluose būtų dalijamasi su valstybių narių institucijomis ir Komisija. Tuo atžvilgiu Direktyvoje (ES) 2022/2555 nustatyta, kad EU-CyCLONe tikslas yra remti koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą operatyviniu lygmeniu ir užtikrinti reguliarų keitimąsi svarbia informacija tarp valstybių narių ir Sąjungos institucijų, organų, įstaigų ir agentūrų. EU-CyCLONe užduotys apima tokių incidentų ir krizių atvejais didinti bendrą informuotumą apie padėtį. Labai svarbu, kad EU-CyCLONe, atsižvelgdamas į tą tikslą ir savo užduotis, užtikrintų, kad tokia informacija būtų nedelsiant perduodama atitinkamų valstybių narių atstovams ir Komisijai. Tuo tikslu labai svarbu, kad į EU-CyCLONe darbo tvarkos taisykles būtų įtrauktos atitinkamos nuostatos;

(22) Europos kibernetinio saugumo įspėjimų sistemoje dalyvaujantys subjektai turėtų užtikrinti aukšto lygio tarpusavio sąveikumą, be kita ko, kai tinkama, duomenų formatų, taksonomijos, duomenų tvarkymo ir duomenų analizės priemonių. Jie taip pat turėtų užtikrinti ir apsaugoti komunikacijos kanalus, minimalų taikomųjų programų saugumo lygį, informuotumo apie padėtį suvestinę ir rodiklius. Priimant bendrą taksonomiją ir rengiant padėties ataskaitų šabloną aptiktų kibernetinio saugumo grėsmių priežastims ir rizikai apibūdinti, turėtų būti atsižvelgiama į atliktą darbą įgyvendinant Direktyvą (ES) 2022/2555;

([13]) 2013 m. gruodžio 17 d. Europos Parlamento ir Tarybos sprendimas Nr. 1313/2013/ES dėl Sąjungos civilinės saugos mechanizmo (OL L 347, 2013 12 20, p. 924, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).

([14]) 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, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

(23) siekiant sudaryti sąlygas didele apimtimi ir patikimoje bei saugioje aplinkoje keistis atitinkamais duomenimis ir informacija apie kibernetinio saugumo grėsmes iš įvairių šaltinių, Europos kibernetinio saugumo įspėjimų sistemoje dalyvaujantys subjektai turėtų turėti naujausias, labai saugias priemones, įrangą ir infrastruktūros objektus ir kvalifikuotus darbuotojus. Tai turėtų sudaryti sąlygas pagerinti kolektyvinius nustatymo pajėgumus ir laiku įspėti institucijas ir atitinkamus subjektus, visų pirma naudojant naujausias dirbtinio intelekto ir duomenų analizės technologijas;

(24) renkant svarbius duomenis ir informaciją, juos analizuojant, jais dalijantis bei keičiantis, Europos kibernetinio saugumo įspėjimų sistema turėtų būti stiprinamas Sąjungos technologinis suverenumas ir atviras strateginis savarankiškumas kibernetinio saugumo, konkurencingumo ir atsparumo srityje. Kokybiškų patikrintų duomenų sutelkimas taip pat galėtų padėti plėtoti pažangias dirbtinio intelekto ir duomenų analizės technologijas. Norint veiksmingai kaupti kokybiškus duomenis labai svarbu išlaikyti žmogaus vykdomą priežiūrą, ir, siekiant to tikslo, kvalifikuotą darbo jėgą;

(25) nors Europos kibernetinio saugumo įspėjimų sistema yra civilinis projektas, kibernetinės gynybos bendruomenei galėtų būti naudingi stipresni civiliniai aptikimo ir informuotumo apie padėtį pajėgumai, parengti ypatingos svarbos infrastruktūrai apsaugoti;

(26) Europos kibernetinio saugumo įspėjimų sistemos dalyviai turėtų dalytis informacija laikydamiesi galiojančių teisinių reikalavimų, visų pirma Sąjungos ir nacionalinės duomenų apsaugos teisės, taip pat Sąjungos taisyklių konkurencijos srityje, kuriomis reglamentuojamas keitimasis informacija. Jei būtina tvarkyti asmens duomenis, informacijos gavėjas turėtų įgyvendinti technines ir organizacines priemones, kuriomis būtų apsaugotos duomenų subjektų teisės ir laisvės, ir sunaikinti duomenis, kai tik jie tampa nebereikalingi nurodytam tikslui, ir informuoti duomenis teikiantį subjektą, kad duomenys buvo sunaikinti;

(27) konfidencialumo ir informacijos saugumo užtikrinimas yra itin svarbus visiems trims šio reglamento ramsčiams: skatinant dalijimąsi arba keitimąsi informacija Europos kibernetinio saugumo įspėjimo sistemoje, išsaugant subjektų, prašančių paramos pagal Reagavimo į kibernetinio saugumo krizes mechanizmą, interesus, ar užtikrinant, kad teikiant pranešimus pagal Europos kibernetinio saugumo incidentų peržiūros mechanizmą būtų galima gauti naudingos patirties nedarant neigiamo poveikio nuo incidentų nukentėjusiems subjektams. Valstybių narių ir subjektų dalyvavimas tuose mechanizmuose priklauso nuo tarpusavio pasitikėjimu pagrįstų santykių tarp jų komponentų. Jei informacija pagal Sąjungos arba nacionalines taisykles yra konfidenciali, dalijimasis arba keitimasis ja pagal šį reglamentą turėtų būti apribotas, t. y. turėtų būti dalijamasi arba keičiamasi tik ta informacija, kuri yra svarbi ir proporcinga dalijimosi ar keitimosi tikslui. Tuo dalijimusi arba keitimusi taip pat turėtų būti išsaugomas tos informacijos konfidencialumas ir, be kita ko, apsaugomi atitinkamų subjektų saugumo ir komerciniai interesai. Pagal šį reglamentą informacija galėtų būti dalijamasi arba keičiamasi naudojantis informacijos neatskleidimo susitarimais arba informacijos platinimo gairėmis, pvz., srauto kontrolės protokolu (TLP). TLP turi būti suprantamas kaip būdas teikti informaciją apie bet kokius apribojimus, taikomus tolesnei informacijos sklaidai. Jis naudojamas beveik visose CSIRT ir kai kuriuose ISAC centruose. Be tų bendrųjų reikalavimų, kalbant apie Europos kibernetinio saugumo įspėjimų sistemą, prieglobos konsorciumų susitarimuose turėtų būti nustatytos konkrečios taisyklės dėl dalijimosi informacija atitinkamame tarpvalstybiniame kibernetinio saugumo centre sąlygų. Tuose susitarimuose visų pirma galėtų būti reikalaujama, kad informacija būtų dalijamasi tik pagal Sąjungos ir nacionalinę teisę;

(28) kalbant apie ES kibernetinio saugumo rezervo naudojimą, būtinos specialios konfidencialumo taisyklės. Paramos bus prašoma, ji bus vertinama ir teikiama kilus krizei ir jautriuose sektoriuose veiklą vykdantiems subjektams. Kad ES kibernetinio saugumo rezervas veiktų veiksmingai, labai svarbu, kad naudotojai ir subjektai galėtų nedelsdami dalytis visa informacija, kurios reikia, kad kiekvienas subjektas galėtų atlikti savo vaidmenį vertinant prašymus ir teikiant paramą, ir suteikti prieigą prie jos. Todėl šiame reglamente turėtų būti nustatyta, kad visa tokia informacija būtų naudojama arba ja dalijamasi tik tais atvejais, kai tai būtina ES kibernetinio saugumo rezervo veiklai, ir kad ta informacija, kuri yra konfidenciali arba įslaptinta pagal Sąjungos ir nacionalinę teisę, būtų naudojama ir ja dalijamasi tik laikantis tos teisės. Be to, naudotojams turėtų būti suteikta galimybė, kai tinkama, naudotis dalijimosi informacija protokolais, pavyzdžiui, TLP, norint nustatyti papildomus apribojimus. Nors naudotojai šiuo atžvilgiu gali veikti savo nuožiūra, svarbu, kad taikydami tokius apribojimus jie atsižvelgtų į galimas pasekmes, visų pirma susijusias su pavėluotu prašomų paslaugų vertinimu arba teikimu. Kad ES kibernetinio saugumo rezervas būtų veiksmingas, svarbu, kad perkančioji organizacija paaiškintų tas pasekmes naudotojui prieš jam pateikiant prašymą. Tos apsaugos

priemonės taikomos tik prašymui dėl ES kibernetinio saugumo rezervo paslaugų ir jų teikimui ir jomis nedaromas poveikis keitimuisi informacija kitomis aplinkybėmis, pavyzdžiui, vykdant ES kibernetinio saugumo rezervo viešuosius pirkimus;

(29) atsižvelgiant į didėjančią riziką ir poveikį valstybėms narėms darančių incidentų skaičių, būtina nustatyti paramos krizės atveju priemonę, t. y. Reagavimo į kibernetinio saugumo krizes mechanizmą, kuria būtų didinamas Sąjungos atsparumas reikšmingiems kibernetinio saugumo incidentams, didelio masto kibernetinio saugumo incidentams ir didelio masto incidentams lygiaverčiams incidentams ir papildomi valstybių narių veiksmai teikiant skubią pasirengimo, reagavimo į incidentus ir neatidėliojamo esminių paslaugų pradinio atkūrimo finansinę paramą. Kadangi visiškas veiklos atkūrimas po incidento yra kompleksinis procesas, kuriuo nuo incidento nukentėjusio subjekto veikla atkuriama ją sugrąžinant į iki incidento buvusią padėtį ir kuris gali ilgai užtrukti ir sudaryti didelių išlaidų, parama iš ES kibernetinio saugumo rezervo turėtų būti teikiama tik pradiniu atkūrimo proceso etapu, kad būtų atstatytos pagrindinės sistemų funkcijos. Reagavimo į kibernetinio saugumo krizes mechanizmas turėtų sudaryti sąlygas greitai ir veiksmingai suteikti pagalbą nustatytomis aplinkybėmis bei aiškiomis sąlygomis ir sudaryti sąlygas atidžiai stebėti ir vertinti, kaip naudojami ištekliai. Reagavimo į kibernetinio saugumo krizes mechanizmu skatinamas valstybių narių solidarumas pagal Europos Sąjungos sutarties (ES sutartis) 3 straipsnio 3 dalį, tačiau pirminė atsakomybė už incidentų ir krizių prevenciją, pasirengimą jiems ir reagavimą į juos pirmiausia tenka valstybėms narėms;

(30) Reagavimo į kibernetinio saugumo krizes mechanizmas turėtų padėti valstybėms narėms papildyti jų pačių priemones bei išteklius ir kitas esamas paramos galimybes reaguojant į reikšmingus kibernetinio saugumo ir didelio masto kibernetinio saugumo incidentus ir pradiniu etapu po tokių incidentų atkuriant veiklą, pavyzdžiui, ENISA jos kompetencijos srityje teikiamas paslaugas, koordinuotą reagavimą ir CSIRT tinklo pagalbą, EU-CyCLONe poveikio mažinimo paramą, taip pat valstybių narių savitarpio pagalbą, be kita ko, pagal ES sutarties 42 straipsnio 7 dalį ir greitojo reagavimo į kibernetinius incidentus komandas nuolatinio struktūrizuoto bendradarbiavimo (PESCO) kontekste, įsteigtas pagal Tarybos sprendimą (BUSP) 2017/2315 ([15]). Juo turėtų būti atsižvelgiama į poreikį užtikrinti, kad būtų specialių priemonių, kuriomis būtų remiamas pasirengimas tokiems incidentams, reagavimas į juos ir veiklos atkūrimas visoje Sąjungoje ir SEP asocijuotosiose trečiosiose valstybėse;

(31) šiuo reglamentu nedaromas poveikis Sąjungos lygmens reagavimo į krizes koordinavimo procedūroms ir sistemoms, visų pirma Direktyvai (ES) 2022/2555, Sąjungos civilinės saugos mechanizmui, nustatytam pagal Europos Parlamento ir Tarybos sprendimą Nr. 1313/2013/ES ([16]), IPCR mechanizmui ir Komisijos rekomendacijai (ES) 2017/1584 ([17]). Atsižvelgiant į civilinį Reagavimo į kibernetinio saugumo krizes mechanizmo pobūdį, parama pagal Reagavimo į kibernetinio saugumo krizes mechanizmą gali papildyti pagal bendrą užsienio ir saugumo politiką ir bendrą saugumo ir gynybos politiką teikiamą pagalbą, be kita ko, pasitelkiant greitojo reagavimo į kibernetines grėsmes grupes. Parama, teikiama pagal Reagavimo į kibernetinio saugumo krizes mechanizmą, gali papildyti veiksmus, įgyvendinamus pagal ES sutarties 42 straipsnio 7 dalį, įskaitant vienos valstybės narės kitai valstybei narei teikiamą pagalbą, būti Sąjungos ir valstybių narių bendro atsako dalis arba papildyti veiksmus, įgyvendinamus SESV 222 straipsnyje nurodytais atvejais. Be to, šio reglamento įgyvendinimas, kai tinkama, turėtų būti koordinuojamas su kibernetinio saugumo diplomatijos priemonių rinkinio priemonių įgyvendinimu;

(32) pagal šį reglamentą teikiama pagalba turėtų būti remiami ir papildomi veiksmai, kurių valstybės narės imasi nacionaliniu lygmeniu. Tuo tikslu turėtų būti užtikrintas glaudus Komisijos, ENISA, valstybių narių ir, kai tinkama, ECCC bendradarbiavimas ir konsultacijos. Prašydama paramos pagal Reagavimo į kibernetinio saugumo krizes mechanizmą, valstybė narė turėtų pateikti atitinkamą informaciją, pagrindžiančią paramos poreikį;

(33) Direktyvoje (ES) 2022/2555 reikalaujama, kad valstybės narės paskirtų arba įsteigtų vieną ar daugiau kibernetinio saugumo krizių valdymo institucijų ir užtikrintų, kad jos turėtų tinkamų išteklių veiksmingai ir efektyviai vykdyti joms pavestas užduotis. Joje taip pat reikalaujama, kad valstybės narės nustatytų, kokius pajėgumus, objektus ir procedūras galima panaudoti krizės atveju, taip pat priimtų nacionalinį reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planą, kuriame išdėstomi didelio masto kibernetinio saugumo incidentų ir krizių valdymo tikslai ir tvarka. Taip pat reikalaujama, kad valstybės narės įsteigtų vieną ar daugiau CSIRT, kurioms būtų pavesta atsakomybė už incidentų valdymą pagal aiškiai apibrėžtą procesą, apimant bent sektorius, subsektorius ir

([15]) 2017 m. gruodžio 11 d. Tarybos sprendimas (BUSP) 2017/2315, kuriuo nustatomas nuolatinis struktūrizuotas bendradarbiavimas (PESCO) ir nustatomas dalyvaujančių valstybių narių sąrašas (OL L 331, 2017 12 14, p. 57, ELI: http://data.europa.eu/eli/dec/2017/2315/oj).

([16]) 2013 m. gruodžio 17 d. Europos Parlamento ir Tarybos sprendimas Nr. 1313/2013/ES dėl Sąjungos civilinės saugos mechanizmo (OL L 347, 2013 12 20, p. 924).

([17]) 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).

subjekto rūšis, patenkančius į tos direktyvos taikymo sritį, ir užtikrintų, kad jos turėtų tinkamų išteklių savo užduotims veiksmingai vykdyti. Šiuo reglamentu nedaromas poveikis Komisijos vaidmeniui užtikrinti, kad valstybės narės laikytųsi Direktyvoje (ES) 2022/2555 nustatytų pareigų. Pagal Reagavimo į kibernetinio saugumo krizes mechanizmą turėtų būti teikiama pagalba veiksmams, kuriais siekiama stiprinti parengtį, taip pat reagavimo į incidentus veiksmams, kuriais siekiama sumažinti reikšmingų kibernetinio saugumo incidentų ir didelio masto kibernetinio saugumo incidentų poveikį ir remti pradinį atsigavimą arba atkurti bazines paslaugų, kurias teikia subjektai, vykdantys veiklą ypatingos svarbos sektoriuose arba subjektai, vykdantys veiklą kituose itin svarbiuose sektoriuose, funkcijas;

(34) vykdant pasirengimo veiksmus, siekiant skatinti nuoseklų požiūrį ir stiprinti saugumą visoje Sąjungoje ir jos vidaus rinkoje, parama turėtų būti teikiama pagal Direktyvą (ES) 2022/2555 nustatytuose ypatingos svarbos sektoriuose veiklą vykdančių subjektų kibernetinio saugumo koordinuotam testavimui ir vertinimui, be kita ko, pasitelkiant pratybas ir mokymus. Tuo tikslu Komisija, pasikonsultavusi su ENISA, TIS bendradarbiavimo grupe ir EU-CyCLONe, turėtų reguliariai nustatyti, kurie atitinkami sektoriai ar subsektoriai turėtų būti tinkami gauti finansinę paramą koordinuotam Sąjungos lygmens parengties testavimui. Sektoriai arba subsektoriai turėtų būti atrinkti iš Direktyvos (ES) 2022/2555 I priede išvardytų ypatingos svarbos sektorių. Koordinuotas parengties testavimas turėtų būti grindžiamas bendrais rizikos scenarijais ir metodikomis. Atrenkant sektorius ir rengiant rizikos scenarijus turėtų būti atsižvelgiama į atitinkamus Sąjungos masto rizikos vertinimus ir rizikos scenarijus, įskaitant poreikį vengti dubliavimosi, kaip antai rizikos vertinimą ir rizikos scenarijus, kuriuos, kaip Taryba ragino savo išvadose dėl Europos Sąjungos kibernetinio saugumo būklės raidos, parengė Komisija, Sąjungos vyriausiasis įgaliotinis užsienio reikalams ir saugumo politikai (toliau – vyriausiasis įgaliotinis) ir TIS bendradarbiavimo grupė, derindami veiksmus su atitinkamomis civilinėmis ir karinėmis įstaigomis bei agentūromis ir sukurtais tinklais, įskaitant EU-CyCLONe, taip pat ryšių tinklų ir infrastruktūrų rizikos vertinimą, kurio buvo paprašyta Nevere paskelbtame bendrame ministrų raginime ir kurį atlieka TIS bendradarbiavimo grupė, padedant Komisijai bei ENISA ir bendradarbiaujant su Europos elektroninių ryšių reguliuotojų institucija, įsteigta Europos Parlamento ir Tarybos reglamentu (ES) 2018/1971 ([18]), Sąjungos lygmeniu koordinuojamus ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimus, kurie turi būti atliekami pagal Direktyvos (ES) 2022/2555 22 straipsnį, ir skaitmeninės veiklos atsparumo testavimą, kaip numatyta Europos Parlamento ir Tarybos reglamente (ES) 2022/2554 ([19]). Atrenkant sektorius taip pat reikėtų atsižvelgti į Tarybos rekomendaciją dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą;

(35) be to, pagal Reagavimo į kibernetinio saugumo krizes mechanizmą turėtų būti teikiama parama kitiems pasirengimo veiksmams ir parama parengčiai kituose sektoriuose, kuriems netaikomas koordinuotas subjektų, vykdančių veiklą ypatingos svarbos sektoriuose arba subjektų, vykdančių veiklą kituose itin svarbiuose sektoriuose, parengties testavimas. Tie veiksmai galėtų apimti įvairių rūšių nacionalinę pasirengimo veiklą;

(36) kai valstybės narės gauna dotacijas pasirengimo veiksmams remti, veiklą ypatingos svarbos sektoriuose vykdantys subjektai gali dalyvauti tuose veiksmuose savanoriškai. Gera praktika yra tai, kad tokiems veiksmams pasibaigus dalyvaujantys subjektai parengia žalos ištaisymo planą, kad įgyvendintų visas parengtas rekomendacijas dėl konkrečių priemonių ir kad iš šių parengiamųjų veiksmų gautų kuo daugiau naudos. Nors svarbu, kad valstybės narės prašytų, kad šiuose veiksmuose dalyvaujantys subjektai parengtų ir įgyvendintų tokius žalos ištaisymo planus, šiuo reglamentu valstybės narės nėra nei įpareigotos, nei įgaliotos užtikrinti tokių prašymų vykdymą. Tokiais prašymais nedaromas poveikis subjektams taikomiems reikalavimams ir kompetentingų institucijų priežiūros įgaliojimams laikantis Direktyvos (ES) 2022/2555;

(37) pagal Reagavimo į kibernetinio saugumo krizes mechanizmą parama taip pat turėtų būti teikiama reagavimo į incidentus veiksmams, kuriais siekiama sumažinti reikšmingų kibernetinio saugumo incidentų, didelio masto kibernetinio saugumo incidentų ir didelio masto incidentams lygiaverčių kibernetinio saugumo incidentų poveikį, remti pradinį veiklos arba esminių paslaugų veikimo atkūrimą. Kai tinkama, jis turėtų papildyti SCSM, kad būtų užtikrintas visapusiškas požiūris į reagavimą į kibernetinių incidentų poveikį piliečiams;

([18]) 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1971, kuriuo įsteigiama Europos elektroninių ryšių reguliuotojų institucija (BEREC) ir BEREC paramos agentūra (BEREC biuras), iš dalies keičiamas Reglamentas (ES) 2015/2120 ir panaikinamas Reglamentas (EB) Nr. 1211/2009 (OL L 321, 2018 12 17, p. 1).

([19]) 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).

(38) pagal Reagavimo į kibernetinio saugumo krizes mechanizmą turėtų būti remiama techninė pagalba, kurią viena valstybė narė teikia kitai valstybei narei, nukentėjusiai nuo reikšmingo kibernetinio saugumo incidento arba didelio masto kibernetinio saugumo incidento, įskaitant CSIRT, kaip nurodyta Direktyvos (ES) 2022/2555 11 straipsnio 3 dalies f punkte. Tokią pagalbą teikiančioms valstybėms narėms turėtų būti leidžiama teikti prašymus padengti išlaidas, susijusias su ekspertų grupių siuntimu teikiant savitarpio pagalbą. Tinkamos finansuoti išlaidos galėtų apimti kibernetinio saugumo ekspertų kelionės, apgyvendinimo ir dienpinigių išlaidas;

(39) atsižvelgiant į esminį privačių įmonių vaidmenį nustatant didelio masto kibernetinio saugumo incidentus ir didelio masto incidentams lygiaverčius kibernetinio saugumo incidentus, joms rengiantis jiems ir į juos reaguojant, svarbu pripažinti savanoriško *pro bono* bendradarbiavimo su tokiomis įmonėmis vertę, jei jos siūlo paslaugas be atlygio didelio masto kibernetinio saugumo incidentų ir krizių bei didelio masto incidentams lygiaverčių kibernetinio saugumo incidentų ir krizių atvejais. ENISA, bendradarbiaudama su EU-CyCLONe, galėtų stebėti tokių *pro bono* iniciatyvų raidą ir skatinti jų atitiktį kriterijams, kurie taikomi patikimiems valdomų saugumo paslaugų teikėjams pagal šį reglamentą, be kita ko, kiek tai susiję su privačių įmonių patikimumu, jų patirtimi ir gebėjimu saugiai tvarkyti neskelbtiną informaciją;

(40) pagal Reagavimo į kibernetinio saugumo krizes mechanizmą palaipsniui turėtų būti sukurtas ES kibernetinio saugumo rezervas, kurį sudarytų patikimų valdomų saugumo paslaugų teikėjų paslaugos, kuriomis būtų remiami reagavimo veiksmai ir inicijuojami veiklos atkūrimo veiksmai reikšmingų kibernetinio saugumo incidentų, didelio masto kibernetinio saugumo incidentų arba didelio masto incidentams lygiaverčių kibernetinio saugumo incidentų, darančių poveikį valstybėms narėms, Sąjungos institucijoms, organams, įstaigoms ar agentūroms arba SEP asocijuotosioms trečiosioms valstybėms, atvejais. ES kibernetinio saugumo rezervas turėtų užtikrinti paslaugų prieinamumą ir parengtį. Todėl jis turėtų apimti paslaugas, dėl kurių įsipareigota iš anksto, įskaitant, pavyzdžiui, pajėgumus, kurie yra parengties būsenoje ir kuriuos galima dislokuoti per trumpą laiką. ES kibernetinio saugumo rezervo paslaugos turėtų padėti nacionalinėms institucijoms teikti pagalbą paveiktiems subjektams, vykdantiems veiklą ypatingos svarbos ar paveiktiems subjektams, vykdantiems veiklą kituose itin svarbiuose sektoriuose, papildant jų pačių veiksmus nacionaliniu lygmeniu. ES kibernetinio saugumo rezervo paslaugomis taip pat turėtų būti galima naudotis panašiomis sąlygomis teikiant paramą Sąjungos institucijoms, organams, įstaigoms ir agentūroms. ES kibernetinio saugumo rezervas taip pat galėtų padėti stiprinti Sąjungos pramonės ir paslaugų sektorius, įskaitant labai mažas įmones ir mažąsias bei vidutines įmones, taip pat startuolius, konkurencinę padėtį visoje skaitmeninėje ekonomikoje, be kita ko, teikiant paskatas investuoti į mokslinius tyrimus ir inovacijas. Perkant paslaugas ES kibernetinio saugumo rezervui svarbu atsižvelgti į ENISA Europos kibernetinio saugumo įgūdžių sistemą. Prašydami paramos iš ES kibernetinio saugumo rezervo, naudotojai į savo paraišką turėtų įtraukti tinkamą informaciją apie paveiktą subjektą ir galimus padarinius, informaciją apie iš ES kibernetinio saugumo rezervo prašomą paslaugą, ir paveiktam subjektui nacionaliniu lygmeniu suteiktą paramą: į tai reikėtų atsižvelgti vertinant pareiškėjo prašymą. Siekiant užtikrinti papildomumą su kitomis paveiktam subjektui prieinamomis paramos formomis, prašyme taip pat turėtų būti nurodyta informacija apie sutartimis įformintus susitarimus dėl reagavimo į incidentą ir pradinio veiklos atkūrimo paslaugų, taip pat apie draudimo sutartis, kurios gali apimti tokio pobūdžio incidentus;

(41) siekiant užtikrinti veiksmingą Sąjungos finansavimo panaudojimą, iš anksto įsipareigotas teikti paslaugas ES kibernetinio saugumo rezervo sistemoje pagal atitinkamą sutartį turėtų būti galima paversti parengties paslaugomis, susijusiomis su incidentų prevencija ir reagavimu į juos, jei tos iš anksto įsipareigotos teikti paslaugos nenaudojamos reagavimui į incidentus tuo laikotarpiu, kuriam jos yra iš anksto įsipareigotos. Tos paslaugos turėtų papildyti pasirengimo veiksmus, kuriuos turi valdyti ECCC, ir neturėtų jų nedubliuoti;

(42) valstybių narių kibernetinių krizių valdymo institucijų ir CSIRT prašymus arba CERT-EU prašymus, pateiktus Sąjungos institucijų, organų, įstaigų ir agentūrų vardu, suteikti paramą iš ES kibernetinio saugumo rezervo turėtų vertinti perkančioji organizacija. Kai ENISA pavesta administruoti ir eksploatuoti ES kibernetinio saugumo rezervą, ta perkančioji organizacija yra ENISA. SEP asocijuotųjų trečiųjų valstybių paramos prašymus turėtų įvertinti Komisija. Siekdama palengvinti paramos prašymų pateikimą ir vertinimą, ENISA galėtų sukurti saugią platformą;

(43) kai vienu metu gaunama daug prašymų, tie prašymai išdėstomi prioritetine tvarka laikantis šiame reglamente nustatytų kriterijų. Atsižvelgiant į bendruosius šio reglamento tikslus, tie kriterijai turėtų apimti incidento sunkumą, paveikto subjekto rūšį, galimą incidento poveikį paveiktai valstybei narei ir naudotojams, galimą incidento tarpvalstybinį platesnio poveikio pobūdį ir išplitimo į kitas valstybes nares riziką, taip pat priemones, kurių naudotojas jau ėmėsi, kad padėtų reaguoti ir atkurti veiklą pradiniu etapu. Atsižvelgiant į tuos tikslus ir į tai, kad

valstybių narių naudotojų prašymais išimtinai siekiama remti subjektus, vykdančius veiklą ypatingos svarbos sektoriuose arba subjektus, vykdančius veiklą kituose itin svarbiuose sektoriuose visoje Sąjungoje, tikslinga didesnį prioritetą teikti valstybių narių naudotojų prašymams, jei dėl tų kriterijų du ar daugiau prašymų vertinami kaip vienodi. Tai nedaro poveikio jokioms pareigoms, kurias valstybės narės gali turėti pagal prieglobos susitarimus, imtis priemonių siekiant apsaugoti Sąjungos institucijas, organus, įstaigas ir agentūras bei jiems padėti;

(44) Komisija turėtų prisiimti bendrą atsakomybę už ES kibernetinio saugumo rezervo įgyvendinimą. Atsižvelgiant į didelę ENISA patirtį, įgytą vykdant paramos kibernetiniam saugumui veiksmus, ENISA yra tinkamiausia agentūra ES kibernetinio saugumo rezervui įgyvendinti. Todėl Komisija turėtų pavesti ENISA dalį arba, jei Komisija mano, kad tai tikslinga, visus ES kibernetinio saugumo rezervo valdymo ir administravimo įgaliojimus. Šie įgaliojimai turėtų būti suteikiami laikantis pagal Reglamentą (ES, Euratomas) 2024/2509 taikytinų taisyklių ir visų pirma turėtų būti įvykdytos atitinkamos susitarimo dėl įnašo pasirašymo sąlygos. Bet kokius ES kibernetinio saugumo rezervo valdymo ir administravimo aspektus, kurie nėra pavesti ENISA, turėtų tiesiogiai valdyti Komisija, be kita ko, prieš pasirašant susitarimą dėl įnašo;

(45) valstybės narės turėtų atlikti pagrindinį vaidmenį kuriant ES kibernetinio saugumo rezervą, jį diegiant bei vykdant veiklą pasibaigus jo diegimui. Kadangi Reglamentas (ES) 2021/694 yra svarbus pagrindinis aktas, skirtas veiksmams, kuriais įgyvendinamas ES kibernetinio saugumo rezervas, veiksmai pagal ES kibernetinio saugumo rezervą turėtų būti numatyti darbo programose, nurodytose Reglamento (ES) 2021/694 24 straipsnyje. Pagal to straipsnio 6 dalį tas darbo programas Komisija turi priimti įgyvendinimo aktais, laikydamasi nagrinėjimo procedūros. Be to, Komisija, koordinuodama veiksmus su TIS bendradarbiavimo grupe, turėtų nustatyti ES kibernetinio saugumo rezervo prioritetus ir raidą;

(46) sutartimis, sudarytomis naudojant ES kibernetinio saugumo rezervą, neturėtų būti daromas poveikis įmonių tarpusavio santykiams ir esamoms paveikto subjekto arba naudotojų ir paslaugų teikėjo pareigoms;

(47) siekiant atrinkti privačius paslaugų teikėjus, kurie teiktų paslaugas pagal ES kibernetinio saugumo rezervą, būtina nustatyti minimaliuosius kriterijus ir reikalavimus, kurie turėtų būti įtraukti į kvietimą teikti pasiūlymus tiems paslaugų teikėjams atrinkti, siekiant užtikrinti, kad būtų tenkinami valstybių narių institucijų, subjektų, vykdančius veiklą ypatingos svarbos sektoriuose ir subjektų, vykdančius veiklą kituose itin svarbiuose sektoriuose, poreikiai. Siekdama patenkinti konkrečius valstybių narių poreikius, perkančioji organizacija, pirkdama ES kibernetinio saugumo rezervui skirtas paslaugas, prireikus, be šiame reglamente nustatytų kriterijų, turėtų parengti atrankos kriterijus ir reikalavimus. Svarbu skatinti mažesnių paslaugų teikėjų, veikiančių regionų ir vietos lygmeniu, dalyvavimą;

(48) atrinkdama į ES kibernetinio saugumo rezervą įtrauktinus paslaugų teikėjus, perkančioji organizacija turėtų siekti užtikrinti, kad į ES kibernetinio saugumo rezervą, kaip visumą, būtų įtraukti paslaugų teikėjai, galintys patenkinti naudotojų kalbos reikalavimus. Tuo tikslu perkančioji organizacija turėtų, prieš rengdama konkurso specifikacijas, pasiteirauti, ar potencialūs ES kibernetinio saugumo rezervo naudotojai turi konkrečių kalbinių reikalavimų, kad ES kibernetinio saugumo rezervo paramos paslaugas būtų galima teikti viena iš Sąjungos institucijų arba valstybių narių oficialiųjų kalbų, kurią, tikėtina, supranta atitinkamas naudotojas ar paveiktas subjektas. Jei ES kibernetinio saugumo rezervo paramos paslaugų naudotojui reikalinga daugiau nei viena kalba ir tam naudotojui skirtos tos paslaugos buvo įsigytos tomis kalbomis, jis turėtų turėti galimybę prašyme dėl ES kibernetinio saugumo rezervo paramos nurodyti, kuria iš tų kalbų paslaugos turėtų būti teikiamos konkretaus incidento, dėl kurio buvo pateiktas prašymas, atveju;

(49) siekiant paremti ES kibernetinio saugumo rezervo sukūrimą, svarbu, kad Komisija prašytų ENISA pagal Reglamentą (ES) 2019/881 parengti potencialią kibernetinio saugumo sertifikavimo schemą, skirtą valdomoms saugumo paslaugoms, tose srityse, kurioms taikomas Reagavimo į kibernetinio saugumo krizes mechanizmas;

(50) siekiant remti šio reglamento tikslus skatinti bendrą informuotumą apie padėtį, didinti Sąjungos atsparumą ir sudaryti sąlygas veiksmingai reaguoti į reikšmingus kibernetinio saugumo incidentus ir didelio masto kibernetinio saugumo incidentus, Komisija arba EU-CyCLONe turėtų turėti galimybę prašyti ENISA, padedant CSIRT tinklui ir pritarus atitinkamoms valstybėms narėms, peržiūrėti ir įvertinti kibernetines grėsmes, žinomus išnaudojamus pažeidžiamumo aspektus ir poveikio mažinimo veiksmus, susijusius su konkrečiu reikšmingu kibernetinio saugumo incidentu ar didelio masto kibernetinio saugumo incidentu. Užbaigusi incidento peržiūrą ir vertinimą, ENISA, bendradarbiaudama su atitinkama valstybe nare, atitinkamais suinteresuotaisiais subjektais, įskaitant privačiojo

sektoriaus subjektus, Komisija ir kitomis atitinkamomis Sąjungos institucijomis, organais, įstaigomis ir agentūromis, turėtų parengti incidento peržiūros ataskaitą. Remiantis bendradarbiavimu su suinteresuotaisiais subjektais, įskaitant privačiojo sektoriaus subjektus, konkrečių incidentų peržiūros ataskaitoje turėtų būti siekiama įvertinti incidento priežastis, poveikį ir padarinių mažinimą po incidento. Ypač daug dėmesio turėtų būti skiriama informacijai ir patirčiai, kuria dalijasi valdomų saugumo paslaugų teikėjai, atitinkantys aukščiausio profesinio sąžiningumo, nešališkumo ir reikiamos techninės kompetencijos sąlygas, kaip to reikalaujama šiuo reglamentu. Ataskaita turėtų būti teikiama EU-CyCLONe, CSIRT tinklui ir Komisijai ir ji turėtų būti naudojama siekiant informuoti apie jų ir ENISA darbą. Kai incidentas susijęs su SEP asocijuotąja trečiąja valstybe, Komisija turėtų ja pasidalyti ir su vyriausiuoju įgaliotiniu;

(51) atsižvelgiant į nenuspėjamą kibernetinio saugumo išpuolių pobūdį ir į tai, kad jie dažnai nėra susiję su konkrečia geografine vietove ir kelia didelę šalutinio poveikio riziką, kaimyninių valstybių atsparumo didinimas ir gebėjimo veiksmingai reaguoti į reikšmingus kibernetinio saugumo incidentus ir didelio masto incidentams lygiaverčių kibernetinio saugumo incidentus stiprinimas padeda užtikrinti visos Sąjungos, ypač jos vidaus rinkos ir pramonės, apsaugą. Tokia veikla galėtų dar labiau prisidėti prie Sąjungos kibernetinės diplomatijos. Todėl SEP asocijuotosios trečiosios valstybės turėtų turėti galimybę prašyti paramos iš ES kibernetinio saugumo rezervo visoje jų teritorijoje arba jos dalyje, jei tai numatyta susitarime, pagal kurį trečioji valstybė yra SEP asocijuotoji šalis. Sąjunga turėtų remti SEP asocijuotųjų trečiųjų valstybių finansavimą pagal toms valstybėms skirtas atitinkamas partnerystes ir finansavimo priemones. Parama turėtų būti skiriama paslaugoms, susijusioms su reagavimu į reikšmingus kibernetinio saugumo incidentus arba didelio masto incidentams lygiaverčius kibernetinio saugumo incidentus ir pradiniu veiklos atkūrimu po tokių incidentų;

(52) šiame reglamente ES kibernetinio saugumo rezervui ir patikimiems valdomų saugumo paslaugų teikėjams nustatytos sąlygos turėtų būti taikomos teikiant paramą SEP asocijuotosioms trečiosioms valstybėms. SEP asocijuotosios trečiosios valstybės turėtų turėti galimybę prašyti paramos iš ES kibernetinio saugumo rezervo, jeigu subjektai, į kuriuos nusitaikyta ir kuriems jos prašo paramos iš ES kibernetinio saugumo rezervo, yra subjektai, vykdantys veiklą ypatingos svarbos sektoriuose arba subjektai, vykdantys veiklą kituose itin svarbiuose sektoriuose, ir jeigu nustatyti incidentai sukelia didelių veiklos sutrikimų arba gali turėti šalutinį poveikį Sąjungoje. SEP asocijuotosios trečiosios valstybės turėtų būti laikomos atitinkančiomis reikalavimus paramai gauti tik tuo atveju, jei susitarime, pagal kurį jos yra prisijungusios prie SEP, konkrečiai numatyta tokia parama. Be to, tokios trečiosios valstybės turėtų būti laikomos atitinkančiomis reikalavimus tik tol, kol tenkinami trys kriterijai. Pirma, trečioji valstybė turėtų visiškai laikytis atitinkamų to susitarimo sąlygų. Antra, atsižvelgiant į ES kibernetinio saugumo rezervo papildomumą, trečioji valstybė turi būti ėmusis tinkamų veiksmų, kad pasirengtų reikšmingiems kibernetinio saugumo incidentams arba didelio masto incidentams lygiaverčiams kibernetinio saugumo incidentams. Trečia, paramos iš ES kibernetinio saugumo rezervo teikimas turėtų derėti su Sąjungos politika tos valstybės atžvilgiu ir bendrais santykiais su ja bei su kitomis Sąjungos politikos sritimis saugumo srityje. Vertindama atitiktį tam trečiajam kriterijui, Komisija turėtų konsultuotis su vyriausiuoju įgaliotiniu dėl tokios paramos teikimo suderinimo su bendra užsienio ir saugumo politika;

(53) SEP asocijuotosioms trečiosioms valstybėms teikiama parama gali daryti poveikį santykiams su trečiosiomis valstybėmis ir Sąjungos saugumo politikai, be kita ko, bendros užsienio ir saugumo politikos bei bendros saugumo ir gynybos politikos srityje. Todėl tikslinga Tarybai suteikti įgyvendinimo įgaliojimus duoti leidimą ir nustatyti laikotarpį, per kurį tokia parama gali būti teikiama. Taryba turėtų veikti remdamasi Komisijos pasiūlymu, deramai atsižvelgdama į Komisijos atliktą trijų kriterijų įvertinimą. Tas pats turėtų būti taikoma galiojimo pratęsimams ir pasiūlymams iš dalies pakeisti arba panaikinti tokius aktus. Išimtiniais atvejais, kai Taryba mano, kad pagal trečiąjį kriterijų iš esmės pasikeitė aplinkybės, Taryba turėtų galėti veikti savo iniciatyva ir iš dalies pakeisti arba panaikinti įgyvendinimo aktą, nelaukdama Komisijos pasiūlymo. Tikėtina, kad dėl tokių reikšmingų pokyčių reikės imtis skubių veiksmų, kurie turės ypač didelį poveikį santykiams su trečiosiomis valstybėmis, o išsamaus Komisijos išankstinio vertinimo nereikės. Be to, dėl SEP asocijuotųjų trečiųjų valstybių prašymų ir tokioms trečiosioms valstybėms suteiktos paramos įgyvendinimo Komisija turėtų bendradarbiauti su vyriausiuoju įgaliotiniu. Komisija taip pat turėtų atsižvelgti į visas ENISA pateiktas nuomones dėl tokių prašymų ir paramos. Komisija turėtų informuoti Tarybą apie prašymų vertinimo rezultatus, įskaitant atitinkamus su tuo susijusius svarstymus, ir apie teikiamas paslaugas;

(54) 2023 m. balandžio 18 d. Komisijos komunikate dėl Kibernetinio saugumo įgūdžių akademijos pabrėžtas kvalifikuotų specialistų trūkumas. Tokie įgūdžiai yra reikalingi šio reglamento tikslams pasiekti. Sąjungai skubiai reikia įgūdžių ir kompetenciją turinčių specialistų, kad būtų galima užkirsti kelią kibernetiniams išpuoliams, juos nustatyti ir nuo jų atgrasyti ir ginti Sąjungą, įskaitant jos svarbiausią infrastruktūrą, nuo tokių išpuolių ir užtikrinti jos atsparumą. Tuo tikslu svarbu skatinti suinteresuotųjų subjektų, įskaitant privataus sektoriaus, pilietinės visuomenės ir akademinės bendruomenės subjektus, bendradarbiavimą. Taip pat svarbu kurti sinergiją visose Sąjungos teritorijose, kad investicijos į švietimą ir mokymą skatintų kurti apsaugos priemones, kuriomis būtų užkirstas kelias protų nutekėjimui ar kad kai kuriuose regionuose įgūdžių spragos nedidėtų daugiau nei kituose. Būtina skubiai užpildyti kibernetinio saugumo įgūdžių spragas, ypatingą dėmesį skiriant lyčių atotrūkio kibernetinio saugumo darbo rinkoje mažinimui, kad būtų skatinamas moterų dalyvavimas kuriant skaitmeninio valdymo struktūrą;

(55) siekiant skatinti inovacijas bendrojoje skaitmeninėje rinkoje, svarbu stiprinti mokslinius tyrimus ir inovacijas kibernetinio saugumo srityje, kad būtų didinamas valstybių narių atsparumas ir Sąjungos atviras strateginis savarankiškumas – abu šie tikslai yra šio reglamento tikslai. Sinergija yra labai svarbi siekiant stiprinti įvairių suinteresuotųjų subjektų, įskaitant privataus sektoriaus, pilietinės visuomenės ir akademinės bendruomenės subjektus, bendradarbiavimą ir jų veiksmų koordinavimą;

(56) šiuo reglamentu turėtų būti atsižvelgiama į 2022 m. sausio 26 d. Europos Parlamento, Tarybos ir Komisijos bendroje deklaracijoje „Europos deklaracija dėl skaitmeninio dešimtmečio skaitmeninių teisių ir principų parengimo“ nustatytą įsipareigojimą apsaugoti Sąjungos demokratijos, žmonių, įmonių ir viešųjų institucijų interesus nuo kibernetinio saugumo pavojų ir kibernetinių nusikaltimų, įskaitant duomenų saugumo pažeidimus ir tapatybės vagystes ar manipuliavimą tapatybe;

(57) siekiant papildyti tikrus neesminius šio reglamento elementus, Komisijai pagal SESV 290 straipsnį turėtų būti deleguoti įgaliojimai priimti aktus, kuriuose būtų nustatyti ES kibernetinio saugumo rezervui reikalingų reagavimo paslaugų rūšys ir skaičius. Ypač svarbu, kad atlikdama parengiamąjį darbą Komisija tinkamai konsultuotųsi, taip pat ir su ekspertais, ir kad tos konsultacijos būtų vykdomos vadovaujantis 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros ([20]) nustatytais principais. Visų pirma, siekiant užtikrinti vienodas galimybes dalyvauti rengiant deleguotuosius aktus, Europos Parlamentas ir Taryba visus dokumentus gauna tuo pačiu metu kaip ir valstybių narių ekspertai, o jų ekspertams sistemingai suteikiama galimybė dalyvauti Komisijos ekspertų grupių, kurios atlieka su deleguotaisiais aktais susijusį parengiamąjį darbą, posėdžiuose;

(58) siekiant užtikrinti vienodas šio reglamento įgyvendinimo sąlygas, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai išsamiau išdėstyti ES kibernetinio saugumo rezervo paramos paslaugų skyrimo procedūrinę tvarką. Tais įgaliojimais turėtų būti naudojamasi laikantis Europos Parlamento ir Tarybos reglamento (ES) Nr. 182/2011 ([21]);

(59) nedarant poveikio taisyklėms, susijusioms su Sąjungos metiniu biudžetu pagal Sutartis, Komisija, vertindama ENISA biudžeto sudarymo ir personalo poreikius, turėtų atsižvelgti į iš šio reglamento kylančias pareigas;

(60) Komisija turėtų reguliariai atlikti šiame reglamente nustatytų priemonių vertinimą. Pirmasis toks vertinimas turėtų būti atliekamas per pirmuosius 2 metus po šio reglamento įsigaliojimo dienos, o vėliau – bent kas 4 metus, atsižvelgiant į daugiametės finansinės programos, įsteigtos pagal SESV 312 straipsnį, peržiūros terminą. Komisija turėtų pateikti padarytos pažangos ataskaitą Europos Parlamentui ir Tarybai. Siekdama įvertinti įvairius reikiamus elementus, įskaitant informacijos, kuria dalijamasi Europos kibernetinio saugumo įspėjimų sistemoje, mastą, Komisija turėtų remtis tik lengvai prieinama arba savanoriškai pateikta informacija. Atsižvelgiant į geopolitinius pokyčius ir siekiant užtikrinti šiame reglamente nustatytų priemonių tęstinumą ir tolesnį plėtojimą po 2027 m., svarbu užtikrinti, kad Komisija įvertintų būtinybę skirti atitinkamą biudžetą 2028–2034 m. daugiametėje finansinėje programoje;

([20]) OL L 123, 2016 5 12, p. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

([21]) 2011 m. vasario 16 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 182/2011, kuriuo nustatomos valstybių narių vykdomos Komisijos naudojimosi įgyvendinimo įgaliojimais kontrolės mechanizmų taisyklės ir bendrieji principai (OL L 55, 2011 2 28, p. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(61) kadangi šio reglamento tikslų, t. y. stiprinti Sąjungos pramonės ir paslaugų sektorių konkurencinę padėtį visoje skaitmeninėje ekonomikoje ir prisidėti prie Sąjungos technologinio suverenumo ir atviro strateginio savarankiškumo kibernetinio saugumo srityje, valstybės narės negali deramai pasiekti, o dėl veiksmo masto arba poveikio tų tikslų būtų geriau siekti Sąjungos lygmeniu, laikydamasi ES sutarties 5 straipsnyje nustatyto subsidiarumo principo Sąjunga gali patvirtinti priemones. Pagal tame straipsnyje nustatytą proporcingumo principą šiuo reglamentu neviršijama to, kas būtina nurodytiems tikslams pasiekti,

PRIĖMĖ ŠĮ REGLAMENTĄ:

I SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas ir tikslai

1. Šiuo reglamentu nustatomos priemonės, kuriomis Sąjungoje stiprinami pajėgumai aptikti kibernetines grėsmes ir incidentus, jiems pasirengti ir į juos reaguoti, sukuriant:

a) visos Europos kibernetinio saugumo centrų tinklą (toliau – Europos kibernetinio saugumo įspėjimų sistema), siekiant plėtoti ir stiprinti koordinuotus aptikimo ir bendro informuotumo apie padėtį pajėgumus;

b) Reagavimo į kibernetinio saugumo krizes mechanizmą, skirtą padėti valstybėms narėms pasirengti reikšmingiems kibernetinio saugumo incidentams ir didelio masto kibernetinio saugumo incidentams, į juos reaguoti, sumažinti jų poveikį ir po tokių incidentų inicijuoti veiklos atkūrimą bei padėti kitiems naudotojams pasirengti reikšmingiems kibernetinio saugumo incidentams ir didelio masto incidentams lygiaverčiams kibernetinio saugumo incidentams;

c) Europos kibernetinio saugumo incidentų peržiūros mechanizmą reikšmingiems kibernetinio saugumo incidentams arba didelio masto kibernetinio saugumo incidentams peržiūrėti ir įvertinti.

2. Šiuo reglamentu siekiama bendrųjų tikslų – stiprinti Sąjungos pramonės ir paslaugų sektorių, įskaitant labai mažas įmones ir mažąsias bei vidutines įmones, taip pat startuolius, konkurencinę padėtį visoje skaitmeninėje ekonomikoje ir prisidėti prie Sąjungos technologinio suverenumo ir atviro strateginio savarankiškumo kibernetinio saugumo srityje, be kita ko, skatinant inovacijas bendrojoje skaitmeninėje rinkoje. Juo tų tikslų siekiama stiprinant solidarumą Sąjungos lygmeniu ir kibernetinio saugumo ekosistemą, didinant valstybių narių kibernetinį atsparumą ir ugdant darbuotojų įgūdžius, praktinę patirtį, gebėjimus ir kompetenciją kibernetinio saugumo srityje.

3. 2 dalyje nurodytų bendrųjų tikslų turi būti siekiama įgyvendinant šiuos konkrečius tikslus:

a) stiprinti bendrus koordinuotus Sąjungos kibernetinių grėsmių ir incidentų aptikimo pajėgumus ir gerinti bendrą informuotumą apie padėtį;

b) stiprinti subjektų, vykdančių veiklą ypatingos svarbos sektoriuose, arba subjektų, vykdančių veiklą kituose itin svarbiuose sektoriuose, visoje Sąjungoje parengtį ir solidarumą plėtojant koordinuotą parengties testavimą ir sustiprintus reagavimo ir atkūrimo pajėgumus, kad būtų galima valdyti reikšmingus kibernetinio saugumo incidentus, didelio masto kibernetinio saugumo incidentus arba didelio masto incidentams lygiaverčius kibernetinio saugumo incidentus, įskaitant galimybę teikti Sąjungos reagavimo į kibernetinio saugumo incidentus paramą SEP asocijuotosioms trečiosioms valstybėms;

c) didinti Sąjungos atsparumą ir prisidėti prie veiksmingo reagavimo į incidentus peržiūrint ir vertinant reikšmingus kibernetinio saugumo incidentus arba didelio masto kibernetinio saugumo incidentus, be kita ko, apibendrinant įgytą patirtį ir, kai tinkama, rengiant rekomendacijas.

4. Veiksmai pagal šį reglamentą vykdomi tinkamai atsižvelgiant į valstybių narių kompetenciją ir jais turėtų būti papildoma CSIRT tinklo, EU-CyCLONe ir TIS bendradarbiavimo grupės vykdoma veikla.

5. Šiuo reglamentu nedaromas poveikis valstybių narių esminėms valstybinėms funkcijoms, įskaitant valstybės teritorinio vientisumo užtikrinimą, viešosios tvarkos palaikymą ir nacionalinio saugumo užtikrinimą. Visų pirma, kiekviena valstybė narė išlieka išimtinai atsakinga už savo nacionalinį saugumą.

6. Dalijimasis arba keitimasis informacija pagal šį reglamentą, kuri yra konfidenciali pagal Sąjungos arba nacionalines taisykles turėtų apsiriboti tik tuo, kas yra aktualu ir proporcinga to dalijimosi ar keitimosi tikslais. Dalijantis ar keičiantis tokia informacija išsaugomas informacijos konfidencialumas ir apsaugomi atitinkamų subjektų saugumo ir komerciniai interesai. Tai neapima informacijos, kurios atskleidimas prieštarauja esminiams valstybių narių nacionalinio saugumo, visuomenės saugumo ar gynybos interesams, teikimo.

2 straipsnis

Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1) tarpvalstybinis kibernetinio saugumo centras – pagal rašytinį konsorciumo susitarimą įsteigta daugiašalė platforma, kuri į koordinuojamą tinklo struktūrą sujungia bent trijų valstybių narių nacionalinius kibernetinio saugumo centrus ir kurios paskirtis – gerinti kibernetinių grėsmių stebėseną, aptikimą ir analizę siekiant užkirsti kelią incidentams ir padėti rengti kibernetinių grėsmių žvalgybos informaciją, visų pirma keičiantis svarbiais ir, kai tinkama, anonimizuotais duomenimis ir informacija, taip pat dalijantis naujausiomis priemonėmis ir bendrai plėtojant kibernetinio saugumo srityje aptikimo, analizės ir prevencijos bei apsaugos pajėgumus patikimoje aplinkoje;

2) prieglobos konsorciumas – konsorciumas, sudarytas iš dalyvaujančių valstybių narių, kurios sutiko įsteigti tarpvalstybinį kibernetinio saugumo centrą ir prisidėti prie jam skirtų priemonių, infrastruktūros arba paslaugų įsigijimo ir prie jo veikimo;

3) CSIRT – CSIRT, paskirtas arba įsteigtas pagal Direktyvos (ES) 2022/2555 10 straipsnį;

4) subjektas – subjektas, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 38 punkte;

5) subjektai, vykdantys veiklą ypatingos svarbos sektoriuose – Direktyvos (ES) 2022/2555 I priede išvardytų rūšių subjektai;

6) subjektai, vykdantys veiklą kituose itin svarbiuose sektoriuose – Direktyvos (ES) 2022/2555 II priede išvardytų rūšių subjektai;

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

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

9) incidentas – incidentas, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 6 punkte;

10) reikšmingas kibernetinio saugumo incidentas – incidentas, atitinkantis Direktyvos (ES) 2022/2555 23 straipsnio 3 dalyje nustatytus kriterijus;

11) didelis incidentas – didelis incidentas, kaip apibrėžta Europos Parlamento ir Tarybos reglamento (ES, Euratomas) 2023/2841 ([22]) 3 straipsnio 8 punkte;

12) didelio masto kibernetinio saugumo incidentas – didelio masto kibernetinio saugumo incidentas, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 7 punkte;

([22]) 2023 m. gruodžio 13 d. Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) 2023/2841, kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti (OL L, 2023/2841, 2023 12 18, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

13) didelio masto incidentui lygiavertis kibernetinio saugumo incidentas – Sąjungos institucijų, organų, įstaigų ir agentūrų atveju – didelis incidentas, o SEP asocijuotųjų trečiųjų valstybių atveju – incidentas, kurio sukelto sutrikdymo mastas viršija SEP atitinkamos asocijuotosios trečiosios valstybės pajėgumą į jį reaguoti;

14) SEP asocijuotoji trečioji valstybė – trečioji valstybė, kuri yra susitarimo su Sąjunga, pagal kurį jai leidžiama dalyvauti Skaitmeninės Europos programoje pagal Reglamento (ES) 2021/694 10 straipsnį, šalis;

15) perkančioji organizacija – Komisija arba, jei ES kibernetinio saugumo rezervo veikimas ir administravimas pagal 14 straipsnio 5 dalį buvo patikėtas ENISA, – ENISA;

16) valdomų saugumo paslaugų teikėjas – valdomų saugumo paslaugų teikėjas, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 40 punkte;

17) patikimi valdomų saugumo paslaugų teikėjai – valdomų saugumo paslaugų teikėjai, atrinkti, kad būtų įtraukti į ES kibernetinio saugumo rezervą pagal 17 straipsnį.

II SKYRIUS

EUROPOS KIBERNETINIO SAUGUMO ĮSPĖJIMŲ SISTEMA

3 straipsnis

Europos kibernetinio saugumo įspėjimų sistemos sukūrimas

1. Europos kibernetinio saugumo įspėjimų sistema – visos Europos infrastruktūros tinklas, kurį sudaro savanoriškai prisijungiantys nacionaliniai kibernetinio saugumo centrai ir tarpvalstybiniai kibernetinio saugumo centrai – turi būti sukurta, kad būtų remiamas pažangių Sąjungos pajėgumų plėtojimas, siekiant stiprinti kibernetinių grėsmių aptikimo, analizės ir duomenų tvarkymo pajėgumus ir incidentų prevenciją Sąjungoje.

2. Europos kibernetinio saugumo įspėjimų sistema:

a) padeda geriau apsisaugoti nuo kibernetinių grėsmių ir į jas reaguoti remdama atitinkamus subjektus, visų pirma CSIRT, CSIRT tinklą, EU-CyCLONe ir kompetentingas institucijas, paskirtas arba įsteigtas pagal Direktyvos (ES) 2022/2555 8 straipsnio 1 dalį, ir su jais bendradarbiaudama bei stiprindama jų pajėgumus;

b) telkia atitinkamus duomenis ir informaciją apie kibernetines grėsmes ir incidentus iš įvairių tarpvalstybinių kibernetinio saugumo centrų šaltinių ir dalijasi analizuota arba apibendrinta informacija per tarpvalstybinius kibernetinio saugumo centrus, kai aktualu, su CSIRT tinklu;

c) renka aukštos kokybės informaciją, kuria remiantis galima imtis veiksmų, ir kibernetinių grėsmių žvalgybos informaciją, naudojant pažangiausias priemones ir pažangiąsias technologijas, ir remia tokios informacijos rengimą bei dalijasi ta informacija ir kibernetinių grėsmių žvalgybos informacija;

d) padeda stiprinti koordinuotą kibernetinių grėsmių aptikimą ir didinti bendrą informuotumą apie padėtį visoje Sąjungoje, taip pat teikia įspėjimus, be kita ko, kai aktualu, teikdama konkrečias rekomendacijas subjektams;

e) teikia paslaugas ir vykdo veiklą, skirtas kibernetinio saugumo bendruomenei Sąjungoje, be kita ko, padėdama kurti pažangias priemones ir technologijas, pavyzdžiui, dirbtinio intelekto ir duomenų analizės priemones.

3. Veiksmai, kuriais įgyvendinama Europos kibernetinio saugumo įspėjimų sistema, remiami Skaitmeninės Europos programos (SEP) lėšomis ir įgyvendinami pagal Reglamentą (ES) 2021/694, visų pirma jo 3 konkretų tikslą.

4 straipsnis

Nacionaliniai kibernetinio saugumo centrai

1. Jei valstybė narė nusprendžia dalyvauti Europos kibernetinio saugumo įspėjimų sistemoje, ji šio reglamento tikslais paskiria arba, kai taikytina, įsteigia nacionalinį kibernetinio saugumo centrą.

2. Nacionalinis kibernetinio saugumo centras yra vienas subjektas, veikiantis pagal valstybės narės įgaliojimus. Tai gali būti CSIRT arba, kai taikytina, nacionalinė kibernetinių krizių valdymo institucija ar kita kompetentinga institucija, paskirta arba įsteigta pagal Direktyvos (ES) 2022/2555 8 straipsnio 1 dalį, arba kitas subjektas. Nacionalinis kibernetinio saugumo centras:

a) turi būti pajėgus veikti kaip atskaitos taškas ir kreiptis į kitas viešąsias ir privačias nacionalinio lygmens organizacijas, kad rinktų ir analizuotų informaciją apie kibernetines grėsmes ir incidentus ir prisidėtų prie 5 straipsnyje nurodytos tarpvalstybinio kibernetinio saugumo centro veiklos, ir

b) geba aptikti, agreguoti ir analizuoti su kibernetinėmis grėsmėmis ir incidentais susijusius duomenis ir informaciją, pavyzdžiui, kibernetinių grėsmių žvalgybos informaciją, visų pirma naudojant naujausias technologijas, siekiant užkirsti kelią incidentams.

3. Vykdydami šio straipsnio 2 dalyje nurodytas funkcijas, nacionaliniai kibernetinio saugumo centrai gali bendradarbiauti su privačiojo sektoriaus subjektais, kad keistųsi atitinkamais duomenimis ir informacija kibernetinių grėsmių ir incidentų nustatymo ir prevencijos tikslais, be kita ko, su esminių ir svarbių subjektų, nurodytų Direktyvos (ES) 2022/2555 3 straipsnyje, sektorinėmis ir tarpsektorinėmis bendruomenėmis. Kai tinkama ir laikantis Sąjungos ir nacionalinės teisės, nacionalinių kibernetinio saugumo centrų prašoma arba gauta informacija gali apimti telemetrijos, jutiklių ir registravimo duomenis.

4. Pagal 9 straipsnio 1 dalį atrinkta valstybė narė įsipareigoja pateikti paraišką dėl savo nacionalinio kibernetinio saugumo centro dalyvavimo tarpvalstybinio kibernetinio saugumo centro veikloje.

5 straipsnis

Tarpvalstybiniai kibernetinio saugumo centrai

1. Jei bent trys valstybės narės yra įsipareigojusios užtikrinti, kad jų nacionaliniai kibernetinio saugumo centrai bendradarbiautų koordinuojant savo kibernetinių grėsmių aptikimo ir stebėsenos veiklą, tos valstybės narės šio reglamento tikslais gali įsteigti prieglobos konsorciumą.

2. Prieglobos konsorciumą sudaro bent trys dalyvaujančios valstybės narės, kurios sutiko įsteigti tarpvalstybinį kibernetinio saugumo centrą ir prisidėti prie jam skirtų priemonių, infrastruktūros arba paslaugų įsigijimo ir prie jo veikimo pagal 4 dalį.

3. Jei prieglobos konsorciumas atrenkamas pagal 9 straipsnio 3 dalį, jo nariai sudaro rašytinį konsorciumo susitarimą, kuriuo:

a) nustatoma vidaus tvarka dėl 9 straipsnio 3 dalyje nurodyto prieglobos ir naudojimo susitarimo įgyvendinimo;

b) įsteigiamas prieglobos konsorciumo tarpvalstybinis kibernetinio saugumo centras, ir

c) įtraukiamos konkrečios sąlygos, kurių reikalaujama pagal 6 straipsnio 1 ir 2 dalis.

4. Tarpvalstybinis kibernetinio saugumo centras yra pagal 3 dalyje nurodytą rašytinį konsorciumo susitarimą įsteigta daugiašalė platforma. Ji į koordinuojamą tinklo struktūrą sujungia prieglobos konsorciumo valstybių narių nacionalinius kibernetinio saugumo centrus. Ji skirta kibernetinių grėsmių stebėsenai, aptikimui ir analizei gerinti, siekiant užkirsti kelią incidentams ir padėti rengti kibernetinių grėsmių žvalgybos informaciją, visų pirma keičiantis svarbiais ir, kai tinkama, anonimizuotais duomenimis ir informacija, taip pat dalijantis naujausiomis priemonėmis ir bendrai plėtojant kibernetinio saugumo srityje aptikimo, analizės ir prevencijos bei apsaugos pajėgumus patikimoje aplinkoje.

5. Tarpvalstybiniam kibernetinio saugumo centrui teisiškai atstovauja atitinkamo prieglobos konsorciumo narys, veikiantis kaip koordinatorius, arba prieglobos konsorciumas, jei jis turi juridinio asmens statusą. Atsakomybė už tarpvalstybinio kibernetinio saugumo centro atitiktį šiam reglamentui ir prieglobos ir naudojimo susitarimui nurodoma 3 dalyje nurodytame rašytiniame konsorciumo susitarime.

6. Valstybė narė gali prisijungti prie jau veikiančio prieglobos konsorciumo gavusi prieglobos konsorciumo narių sutikimą. 3 dalyje nurodytas rašytinis konsorciumo susitarimas ir prieglobos ir naudojimo susitarimas atitinkamai pakeičiami. Tai nedaro poveikio Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro (toliau – ECCC) nuosavybės teisėms į priemones, infrastruktūrą ar paslaugas, kurios jau buvo bendrai įsigytos su tuo prieglobos konsorciumu.

6 straipsnis

Bendradarbiavimas ir dalijimasis informacija tarpvalstybiniuose kibernetinio saugumo centruose ir tarp jų

1. Prieglobos konsorciumo nariai užtikrina, kad jų nacionaliniai kibernetinio saugumo centrai pagal 5 straipsnio 3 dalyje nurodytą konsorciumo susitarimą tarpusavyje tarpvalstybiniame kibernetinio saugumo centre dalintųsi svarbia ir, kai tinkama, anonimizuota informacija, pavyzdžiui, informacija, susijusia su kibernetinėmis grėsmėmis, vos neįvykusiais incidentais, pažeidžiamumais, metodais ir procedūromis, užvaldymo rodikliais, priešiška taktika, konkrečių grėsmių ir dalyvių informacija, kibernetinio saugumo įspėjimais ir rekomendacijomis dėl kibernetinio saugumo priemonių konfigūracijos siekiant aptikti kibernetines atakas, kai tokiu dalijimusi informacija:

a) skatinamas ir stiprinamas kibernetinių grėsmių aptikimas ir stiprinamas CSIRT tinklo pajėgumas užkirsti kelią incidentams ir į juos reaguoti arba sumažinti jų poveikį;

b) didinamas kibernetinio saugumo lygis, pavyzdžiui, didinant informuotumą apie kibernetines grėsmes, ribojant arba sustabdant tokių grėsmių plitimo galimybes, remiant įvairius gynybos pajėgumus, pažeidžiamumų ištaisymą ir atskleidimą, grėsmių aptikimo, sustabdymo ir prevencijos metodus, poveikio mažinimo strategijas, reagavimo ir veiklos atkūrimo etapus arba skatinant bendradarbiavimu grindžiamus viešųjų ir privačių subjektų atliekamus kibernetinių grėsmių mokslinius tyrimus.

2. 5 straipsnio 3 dalyje nurodytame rašytiniame konsorciumo susitarime nustatoma:

a) įsipareigojimas su prieglobos konsorciumo nariais dalytis 1 dalyje nurodyta informacija, ir sąlygos, kuriomis turi būti dalijamasi ta informacija;

b) valdymo sistema, kuria patikslinamas ir skatinamas visų dalyvių dalijimasis 1 dalyje nurodyta svarbia ir, kai tinkama, anonimizuota informacija;

c) prisidėjimo prie pažangių priemonių ir technologijų, pavyzdžiui, dirbtinio intelekto ir duomenų analizės priemonių, kūrimo tikslai.

Rašytiniame konsorciumo susitarime gali būti nurodyta, kad 1 dalyje nurodyta informacija turi būti dalijamasi pagal Sąjungos ir nacionalinę teisę.

3. Tarpvalstybiniai kibernetinio saugumo centrai sudaro tarpusavio bendradarbiavimo susitarimus, kuriuose nustatomi tarpvalstybinių kibernetinio saugumo centrų sąveikos ir dalijimosi informacija principai. Tarpvalstybiniai kibernetinio saugumo centrai informuoja Komisiją apie sudarytus bendradarbiavimo susitarimus.

4. 1 dalyje nurodytas dalijimasis informacija tarp tarpvalstybinių kibernetinio saugumo centrų užtikrinamas užtikrinant aukštą sąveikos lygį. Siekdama remti tokią sąveiką, ENISA, glaudžiai konsultuodamasi su Komisija, nepagrįstai nedelsdama ir bet kuriuo atveju ne vėliau kaip 2026 m. vasario 5 d. paskelbia gaires dėl sąveikos, kuriose, visų pirma, nurodomi dalijimosi informacija formatai ir protokolai, atsižvelgiant į tarptautinius standartus ir geriausią praktiką, taip pat visų įsteigtų tarpvalstybinių kibernetinio saugumo centrų veikimas. Tarpvalstybinių kibernetinio saugumo centrų bendradarbiavimo susitarimuose nustatyti sąveikos reikalavimai grindžiami ENISA paskelbtomis gairėmis.

7 straipsnis

Bendradarbiavimas ir dalijimasis informacija su Sąjungos lygmens tinklais

1. Tarpvalstybiniai kibernetinio saugumo centrai ir CSIRT tinklas glaudžiai bendradarbiauja, visų pirma dalijimosi informacija tikslais. Tuo tikslu jie susitaria dėl procedūrinės bendradarbiavimo ir dalijimosi svarbia informacija tvarkos ir, nedarant poveikio 2 daliai, dėl informacijos, kuria dalijamasi, rūšių.

2. Jei tarpvalstybiniai kibernetinio saugumo centrai gauna informacijos, susijusios su galimu arba tebesitęsiančiu didelio masto kibernetinio saugumo incidentu, jie, siekdami bendro informuotumo apie padėtį, užtikrina, kad per EU-CyCLONe ir CSIRT tinklą valstybių narių institucijoms ir Komisijai būtų nepagrįstai nedelsiant teikiama svarbi informacija ir išankstiniai įspėjimai.

8 straipsnis

Saugumas

1. Europos kibernetinio saugumo įspėjimų sistemos veikloje dalyvaujančios valstybės narės užtikrina aukštą Europos kibernetinio saugumo įspėjimų sistemos tinklo kibernetinio saugumo, įskaitant konfidencialumą ir duomenų saugumą, taip pat fizinio saugumo lygį ir užtikrina, kad tinklas būtų tinkamai valdomas ir kontroliuojamas taip, kad jis būtų apsaugotas nuo grėsmių ir būtų užtikrintas jo ir sistemų saugumas, įskaitant duomenų ir informacijos, kuria dalijamasi per tinklą, saugumą.

2. Europos kibernetinio saugumo įspėjimų sistemoje dalyvaujančios valstybės narės užtikrina, kad dalijimasis 6 straipsnio 1 dalyje nurodyta informacija Europos kibernetinio saugumo įspėjimų sistemoje su bet kuriuo subjektu, kuris nėra valstybės narės valdžios institucija ar įstaiga, nedarytų neigiamo poveikio Sąjungos ar valstybių narių saugumo interesams.

9 straipsnis

Europos kibernetinio saugumo įspėjimų sistemos finansavimas

1. Paskelbus kvietimą valstybėms narėms, ketinančioms dalyvauti Europos kibernetinio saugumo įspėjimų sistemoje, pareikšti susidomėjimą, ECCC atrenka valstybes nares, kad jos kartu su ECCC dalyvautų bendruose priemonių, infrastruktūros ar paslaugų viešuosiuose pirkimuose, siekiant įsteigti pagal 4 straipsnio 1 dalį paskirtus arba įsteigtus nacionalinius kibernetinio saugumo centrus arba padidinti jų pajėgumus. ECCC atrinktoms valstybėms narėms gali skirti dotacijas tokių priemonių, infrastruktūros ar paslaugų veikimui finansuoti. Sąjungos finansiniu įnašu padengiama iki 50 % priemonių, infrastruktūros ar paslaugų įsigijimo išlaidų ir iki 50 % veiklos išlaidų. Atrinktos valstybės narės padengia likusias išlaidas. Prieš pradėdami priemonių, infrastruktūros ar paslaugų įsigijimo procedūrą, ECCC ir atrinktos valstybės narės sudaro prieglobos ir naudojimo susitarimą, kuriuo reglamentuojamas priemonių, infrastruktūros ar paslaugų naudojimas.

2. Jei valstybės narės nacionalinis kibernetinio saugumo centras per 2 metus nuo priemonių, infrastruktūros ar paslaugų įsigijimo arba dotacijos gavimo dienos, priklausomai nuo to, kas įvyko anksčiau, netampa tarpvalstybinio kibernetinio saugumo centro dalyviu, valstybė narė negali gauti papildomos Sąjungos paramos pagal šį skyrių tol, kol jis neprisijungs prie tarpvalstybinio kibernetinio saugumo centro.

3. Paskelbus kvietimą pareikšti susidomėjimą, ECCC atrenka prieglobos konsorciumą dalyvauti bendruose viešuosiuose priemonių, infrastruktūros ar paslaugų pirkimuose su ECCC. ECCC atrinktam prieglobos konsorciumui gali skirti dotaciją priemonių, infrastruktūros ar paslaugų veikimui finansuoti. Sąjungos finansiniu įnašu padengiama iki 75 % priemonių, infrastruktūros ir paslaugų įsigijimo išlaidų ir iki 50 % veiklos išlaidų. Prieglobos konsorciumas padengia likusias išlaidas. Prieš pradėdami priemonių, infrastruktūros ar paslaugų įsigijimo procedūrą, ECCC ir prieglobos konsorciumas sudaro prieglobos ir naudojimo susitarimą, kuriuo reglamentuojamas priemonių, infrastruktūros ar paslaugų naudojimas.

4. ECCC ne rečiau kaip kas 2 metus parengia priemonių, infrastruktūros ar paslaugų, būtinų ir tinkamos kokybės nacionaliniams kibernetinio saugumo centrams ir tarpvalstybiniams kibernetinio saugumo centrams steigti ar stiprinti jų pajėgumus, ir jų prieinamumo, be kita ko, iš valstybėse narėse įsisteigusių arba laikomų įsisteigusiais ir valstybių narių arba valstybių narių piliečių kontroliuojamų teisės subjektų, aprašą. Rengdamas aprašą ECCC konsultuojasi su CSIRT tinklu, visais esamais tarpvalstybiniais kibernetinio saugumo centrais, ENISA ir Komisija.

III SKYRIUS

REAGAVIMO Į KIBERNETINIO SAUGUMO KRIZES MECHANIZMAS

10 straipsnis

Reagavimo į kibernetinio saugumo krizes mechanizmo sukūrimas

1. Siekiant padėti didinti Sąjungos atsparumą kibernetinėms grėsmėms ir solidariai pasirengti trumpalaikiam reikšmingų kibernetinio saugumo incidentų, didelio masto kibernetinio saugumo incidentų ir didelio masto incidentams lygiaverčių kibernetinio saugumo incidentų poveikiui ir jį sumažinti, sukuriamas Reagavimo į kibernetinio saugumo krizes mechanizmas.

2. Valstybių narių atveju pagal Reagavimo į kibernetinio saugumo krizes mechanizmą numatyti veiksmai vykdomi gavus prašymą ir jie papildo valstybių narių pastangas ir veiksmus, kuriais siekiama pasirengti kibernetinio saugumo incidentams, į juos reaguoti ir atkurti veiklą po jų.

3. Veiksmai, kuriais įgyvendinamas Reagavimo į kibernetinio saugumo krizes mechanizmas, remiami SEP lėšomis ir įgyvendinami pagal Reglamentą (ES) 2021/694, visų pirma jo 3 konkretų tikslą.

4. Veiksmai pagal Reagavimo į kibernetinio saugumo krizes mechanizmą įgyvendinami visų pirma per ECCC pagal Reglamentą (ES) 2021/887. Tačiau šio reglamento 11 straipsnio b punkte nurodytus veiksmus, kuriais įgyvendinamas ES kibernetinio saugumo rezervas, įgyvendina Komisija ir ENISA.

11 straipsnis

Veiksmų rūšys

Reagavimo į kibernetinio saugumo krizes mechanizmu remiami šių rūšių veiksmai:

a) parengties veiksmai, t. y.:

   i) 12 straipsnyje nurodytas koordinuotas subjektų, vykdančių veiklą ypatingos svarbos sektoriuose visoje Sąjungoje, parengties testavimas;

   ii) 13 straipsnyje nurodyti kiti parengties veiksmai, skirti subjektams, vykdantiems veiklą ypatingos svarbos sektoriuose arba subjektams, vykdantiems veiklą kituose itin svarbiuose sektoriuose;

b) veiksmai, kuriais remiamas reagavimas į reikšmingus kibernetinio saugumo incidentus, didelio masto kibernetinio saugumo incidentus ir didelio masto incidentams lygiaverčius kibernetinio saugumo incidentus ir inicijuojamas veiklos atkūrimas po tokių incidentų, ir kuriuos turi vykdyti patikimi valdomų saugumo paslaugų teikėjai, dalyvaujantys ES kibernetinio saugumo rezerve, sukurtame pagal 14 straipsnį;

c) 18 straipsnyje nurodytos savitarpio pagalbos veiksmai.

12 straipsnis

Koordinuotas subjektų parengties testavimas

1. Reagavimo į kibernetinio saugumo krizes mechanizmu remiamas savanoriškas koordinuotas ypatingos svarbos sektoriuose veikiančių subjektų parengties testavimas.

2. Koordinuotą parengties testavimą gali sudaryti parengties veikla, pavyzdžiui, skverbimosi testavimas, ir grėsmių vertinimas.

3. Parama parengties veiksmams pagal šį straipsnį valstybėms narėms teikiama visų pirma dotacijų forma ir laikantis Reglamento (ES) 2021/694 24 straipsnyje nurodytose atitinkamose darbo programose nustatytų sąlygų.

4. Siekdama remti koordinuotą šio reglamento 11 straipsnio a punkto i papunktyje nurodytą subjektų parengties testavimą visoje Sąjungoje, Komisija, pasikonsultavusi su TIS bendradarbiavimo grupe, EU-CyCLONe ir ENISA, iš Direktyvos (ES) 2022/2555 I priede išvardytų ypatingos svarbos sektorių nustato sektorius arba subsektorius, kuriems gali

būti paskelbtas kvietimas teikti paraiškas dėl dotacijų skyrimo. Valstybės narės tuose kvietimuose teikti paraiškas dalyvauja savanoriškai.

5. Nustatydama 4 dalyje nurodytus sektorius ar subsektorius, Komisija atsižvelgia į koordinuotus rizikos vertinimus ir atsparumo testavimą Sąjungos lygmeniu bei jų rezultatus.

6. TIS bendradarbiavimo grupė, bendradarbiaudama su Komisija, Sąjungos vyriausiuoju įgaliotiniu užsienio reikalams ir saugumo politikai (toliau – vyriausiasis įgaliotinis) ir ENISA bei, pagal savo įgaliojimus, su EU-CyCLONe, parengia bendrus rizikos scenarijus ir metodikas 11 straipsnio 1 dalies a punkto i papunktyje nurodytam koordinuotam parengties testavimui ir, kai tinkama, to straipsnio a punkto ii papunktyje nurodytus kitus pasirengimo veiksmus.

7. Kai subjektas, vykdantis veiklą ypatingos svarbos sektoriuje, savanoriškai dalyvauja koordinuotame parengties testavime ir po to testavimo pateikiamos rekomendacijos dėl konkrečių priemonių, kurias dalyvaujantis subjektas galėtų įtraukti į koregavimo planą, už koordinuotą parengties testavimą atsakinga valstybės narės institucija, kai tinkama, peržiūri dalyvaujančių subjektų tolesnius veiksmus, susijusius su tomis priemonėmis, siekdama sustiprinti parengtį.

13 straipsnis

Kiti parengties veiksmai

1. Reagavimo į kibernetinio saugumo krizes mechanizmu remiami parengties veiksmai, kuriems netaikomas 12 straipsnis. Tokie veiksmai apima parengties veiksmus, skirtus subjektams, vykdantiems veiklą sektoriuose, kuriems nenurodyta atlikti koordinuotą parengties testavimą pagal 12 straipsnį. Tokiais veiksmais gali būti remiama pažeidžiamumo stebėsena, rizikos stebėsena, pratybos ir mokymai.

2. Parama parengties veiksmams pagal šį straipsnį teikiama valstybėms narėms jų prašymu, visų pirma dotacijų forma ir laikantis Reglamento (ES) 2021/694 24 straipsnyje nurodytose atitinkamose darbo programose nustatytų sąlygų.

14 straipsnis

ES kibernetinio saugumo rezervo sukūrimas

1. Siekiant 3 dalyje nurodytiems naudotojams jų prašymu padėti reaguoti į reikšmingus kibernetinio saugumo incidentus, didelio masto kibernetinio saugumo incidentus arba didelio masto kibernetinio saugumo incidentams lygiaverčius kibernetinio saugumo incidentus arba teikti reagavimo į tokius incidentus paramą ir inicijuoti veiklos atkūrimą po tokių incidentų, sukuriamas ES kibernetinio saugumo rezervas.

2. ES kibernetinio saugumo rezervą sudaro reagavimo paslaugos, kurias teikia patikimi valdomų saugumo paslaugų teikėjai, atrinkti pagal 17 straipsnio 2 dalyje nustatytus kriterijus. ES kibernetinio saugumo rezervas gali apimti iš anksto įsipareigotas teikti paslaugas. Patikimo valdomų saugumo paslaugų teikėjo iš anksto įsipareigotas teikti paslaugas galima paversti parengties paslaugomis, susijusiomis su incidentų prevencija ir reagavimu į juos, tais atvejais, kai tos iš anksto įsipareigotas teikti paslaugos nenaudojamos reagavimui į incidentus tuo laikotarpiu, kuriuo iš anksto įsipareigota teikti tas paslaugas. Pateikus prašymą, ES kibernetinio saugumo rezervą galima naudoti visose valstybėse narėse, Sąjungos institucijose, organuose, įstaigose ir agentūrose ir SEP asocijuotosiose trečiosiose valstybėse, nurodytose 19 straipsnio 1 dalyje.

3. ES kibernetinio saugumo rezervo paslaugų naudotojai yra:

a) valstybių narių kibernetinio saugumo krizių valdymo institucijos ir CSIRT, nurodyti atitinkamai Direktyvos (ES) 2022/2555 9 straipsnio 1 ir 2 dalyse ir 10 straipsnyje;

b) CERT-EU pagal Reglamento (ES, Euratomas) 2023/2841 13 straipsnį;

c) kompetentingos institucijos, pavyzdžiui, SEP asocijuotųjų trečiųjų valstybių reagavimo į kompiuterinius saugumo incidentus tarnybos ir kibernetinių krizių valdymo institucijos pagal 19 straipsnio 8 dalį.

4. Komisijai tenka bendra atsakomybė už ES kibernetinio saugumo rezervo įgyvendinimą. Komisija, koordinuodama veiksmus su TIS bendradarbiavimo grupe ir atsižvelgdama į 3 dalyje nurodytų naudotojų reikalavimus, nustato ES kibernetinio saugumo rezervo prioritetus ir raidą, prižiūri jo įgyvendinimą ir užtikrina papildomumą, nuoseklumą, sinergiją ir sąsajas su kitais paramos veiksmais pagal šį reglamentą, taip pat su kitais Sąjungos veiksmais ir programomis. Tie

prioritetai peržiūrimi ir, prireikus, patikslinami kas 2 metus. Komisija informuoja Europos Parlamentą ir Tarybą apie tuos prioritetus ir bet kokius jų patikslinimus.

5. Nedarant poveikio bendrai šio straipsnio 4 dalyje nurodytai Komisijos atsakomybei už ES kibernetinio saugumo rezervo įgyvendinimą ir laikantis susitarimo dėl įnašo, kaip apibrėžta Reglamento (ES, Euratomas) 2024/2509 2 straipsnio 19 punkte, Komisija visiškai arba iš dalies paveda ES kibernetinio saugumo rezervo veikimą ir administravimą ENISA. ENISA nepavestus aspektus ir toliau tiesiogiai valdo Komisija.

6. ENISA ne rečiau kaip kas 2 metus parengia šio straipsnio 3 dalies a ir b punktuose nurodytiems naudotojams reikalingų paslaugų aprašą. Į aprašą taip pat įtraukiama informacija apie tokių paslaugų prieinamumą, įskaitant paslaugas, kurias teikia valstybėse narėse įsisteigę arba laikomi jose įsisteigusiais teisės subjektai, kuriuos kontroliuoja valstybės narės arba valstybių narių piliečiai. Įtraukdama į aprašą informaciją apie tą prieinamumą, ENISA įvertina Sąjungos kibernetinio saugumo srities darbuotojų įgūdžius ir pajėgumus, susijusius su ES kibernetinio saugumo rezervo tikslais. Rengdama aprašą ENISA konsultuojasi su TIS bendradarbiavimo grupe, EU-CyCLONe, Komisija ir, kai taikytina, Tarpinstitucine kibernetinio saugumo taryba, įsteigta pagal Reglamento (ES, Euratomas) 2023/2841 10 straipsnį (toliau – TKST). Įtraukdama į aprašą informaciją apie paslaugų prieinamumą, ENISA taip pat konsultuojasi su atitinkamais kibernetinio saugumo pramonės suinteresuotaisiais subjektais, įskaitant valdomų saugumo paslaugų teikėjus. ENISA, informavusi Tarybą ir pasikonsultavusi su EU-CyCLONe, Komisija ir, kai aktualu, vyriausiuoju įgaliotiniu, parengia panašų aprašą, siekdama nustatyti šio straipsnio 3 dalies c punkte nurodytų naudotojų poreikius.

7. Komisijai pagal 23 straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, siekiant papildyti šį reglamentą, nustatant ES kibernetinio saugumo rezervui reikalingų reagavimo paslaugų rūšis ir skaičių. Rengdama tuos deleguotuosius aktus Komisija atsižvelgia į šio straipsnio 6 dalyje nurodytą aprašą ir gali keistis patarimais ir bendradarbiauti su TIS bendradarbiavimo grupe ir ENISA.

15 straipsnis

Prašymai suteikti paramą iš ES kibernetinio saugumo rezervo

1. 14 straipsnio 3 dalyje nurodyti naudotojai gali prašyti ES kibernetinio saugumo rezervo paslaugų, kad padėtų reaguoti į reikšmingus kibernetinio saugumo incidentus, didelio masto kibernetinio saugumo incidentus arba didelio masto incidentams lygiaverčius kibernetinio saugumo incidentus ir inicijuoti veiklos atkūrimą po tokių incidentų.

2. Kad gautų paramą iš ES kibernetinio saugumo rezervo, 12 straipsnio 3 dalyje nurodyti naudotojai imasi visų tinkamų priemonių incidento, dėl kurio prašoma paramos, poveikiui sumažinti, įskaitant, atitinkamais atvejais, tiesioginės techninės pagalbos ir kitų išteklių, skirtų padėti reaguoti į incidentą, teikimą ir pastangas atkurti veiklą po incidento.

3. Prašymai suteikti paramą perkančiajai organizacijai perduodami taip:

a) šio reglamento 14 straipsnio 3 dalies a punkte nurodytų naudotojų atveju tokie prašymai perduodami per valstybės narės pagal Direktyvos (ES) 2022/2555 8 straipsnio 3 dalį paskirtą arba įsteigtą bendrąjį kontaktinį punktą;

b) 14 straipsnio 3 dalies b punkte nurodyto naudotojo atveju tokius prašymus perduoda tas naudotojas;

c) 14 straipsnio 3 dalies c punkte nurodyto naudotojo atveju tokie prašymai perduodami per 19 straipsnio 9 dalyje nurodytą bendrąjį kontaktinį punktą.

4. Jei gaunami šio reglamento 14 straipsnio 3 dalies a punkte nurodytų naudotojų prašymai, valstybės narės informuoja CSIRT tinklą ir, kai tinkama, EU-CyCLONe apie savo naudotojų prašymus suteikti su reagavimu į incidentus ir pradiniu veiklos atkūrimu po jų susijusią paramą pagal šį straipsnį.

5. Prašyme suteikti reagavimo į incidentus ir pradinio veiklos atkūrimo po jų paramą pateikiama:

a) tinkama informacija apie paveiktą subjektą ir galimą incidento poveikį:

   i) 14 straipsnio 3 dalies a punkte nurodytų naudotojų atveju – paveiktoms valstybėms narėms ir naudotojams, įskaitant išplitimo į kitą valstybę narę riziką;

ii) 14 straipsnio 3 dalies b punkte nurodyto naudotojo atveju – paveiktoms Sąjungos institucijoms, organams, įstaigoms ar agentūroms;

iii) 14 straipsnio 3 dalies c punkte nurodyto naudotojo atveju – paveiktoms SEP asocijuotosioms šalims;

b) informacija apie prašomą paslaugą, kartu su planuojamu prašomos paramos panaudojimu, įskaitant numatomų poreikių nurodymą;

c) tinkama informacija apie priemones, kurių imtasi incidento, dėl kurio prašoma paramos poveikiui sumažinti, nurodytos 2 dalyje;

d) kai aktualu, turima informacija apie kitų formų paramą, kurią gali gauti paveiktas subjektas.

6. ENISA, bendradarbiaudama su Komisija ir EU-CyCLONe, parengia šabloną, kad būtų lengviau teikti prašymus suteikti paramą iš ES kibernetinio saugumo rezervo.

7. Komisija gali priimti įgyvendinimo aktus, kuriais išsamiau nustatoma išsami procedūrinė tvarka, pagal kurią prašoma ES kibernetinio saugumo rezervo paramos paslaugų ir pagal kurią turi būti atsakoma į tuos prašymus pagal šį straipsnį, 16 straipsnio 1 dalį ir 19 straipsnio 10 dalį, įskaitant tokių prašymų pateikimo ir atsakymų pateikimo tvarką bei 16 straipsnio 9 dalyje nurodytų ataskaitų šablonus. Tie įgyvendinimo aktai priimami laikantis 24 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

16 straipsnis

ES kibernetinio saugumo rezervo paramos įgyvendinimas

1. 14 straipsnio 3 dalies a ir b punktuose nurodytų naudotojų prašymų atveju prašymus suteikti paramą iš ES kibernetinio saugumo rezervo vertina perkančioji organizacija. Siekiant užtikrinti paramos veiksmingumą, atsakymas 14 straipsnio 3 dalies a ir b punktuose nurodytiems naudotojams perduodamas nedelsiant ir bet kuriuo atveju ne vėliau kaip per 48 valandas nuo prašymo pateikimo. Perkančioji organizacija informuoja Tarybą ir Komisiją apie proceso rezultatus.

2. Kiek tai susiję su informacija, kuria dalijamasi prašant ES kibernetinio saugumo rezervo paslaugų ir jas teikiant, visos šalys, dalyvaujančios taikant šį reglamentą:

a) užtikrina, kad ta informacija būtų naudojama ir ja būtų dalijamasi tik tiek, kiek tai būtina jų pareigoms ar funkcijoms pagal šį reglamentą vykdyti;

b) naudoja konfidencialią arba pagal Sąjungos ir nacionalinę teisę įslaptintą informaciją ir ja dalijasi tik pagal tą teisę, ir

c) užtikrina veiksmingą, efektyvų ir saugų keitimąsi informacija, kai tinkama, naudojant atitinkamus dalijimosi informacija protokolus, įskaitant Srauto kontrolės protokolą, ir jų laikantis.

3. Vertindama atskirus prašymus pagal 16 straipsnio 1 dalį ir 19 straipsnio 10 dalį, perkančioji organizacija arba, kai taikytina, Komisija pirmiausia įvertina, ar tenkinami 15 straipsnio 1 ir 2 dalyse nurodyti kriterijai. Jei taip yra, jos įvertina, kokia paramos trukmė ir pobūdis yra tinkami, atsižvelgdamos į 1 straipsnio 3 dalies b punkte nurodytą tikslą ir, kai aktualu, į šiuos kriterijus:

a) incidento mastą ir sunkumą;

b) paveikto subjekto rūšį, didesnę pirmenybę teikiant incidentams, darantiems poveikį esminiams subjektams, nurodytiems Direktyvos (ES) 2022/2555 3 straipsnio 1 dalyje;

c) galimą poveikį paveiktoms valstybėms narėms, Sąjungos institucijoms, organams, įstaigoms ar agentūroms, arba SEP asocijuotosioms trečiosioms valstybėms;

d) galimą incidento tarpvalstybinį pobūdį ir išplitimo į kitas valstybes nares, Sąjungos institucijas, organus, įstaigas ar agentūras arba SEP asocijuotąsias trečiąsias valstybes riziką;

e) priemones, kurių naudotojas ėmėsi siekdamas padėti reaguoti, ir pradinio veiklos atkūrimo pastangas, nurodytas 15 straipsnio 2 dalyje.

4. Kai vienu metu pateikiami keli 14 straipsnio 3 dalyje nurodytų naudotojų prašymai, siekiant nustatyti jų pirmenybę, kai aktualu, atsižvelgiama į šio straipsnio 3 dalyje nurodytus kriterijus, nedarant poveikio lojalaus valstybių narių ir Sąjungos institucijų, organų, įstaigų ir agentūrų bendradarbiavimo principui. Kai du ar daugiau prašymų vertinami kaip lygiaverčiai pagal tuos kriterijus, pirmenybė teikiama valstybių narių naudotojų prašymams. Kai pagal 14 straipsnio 5 dalį ENISA visiškai arba iš dalies patikėtas ES kibernetinio saugumo rezervo veikimas ir administravimas, ENISA ir Komisija glaudžiai bendradarbiauja, kad pagal šią dalį nustatytų prašymų pirmenybę.

5. ES kibernetinio saugumo rezervo paslaugos teikiamos pagal konkrečius patikimo valdomų saugumo paslaugų teikėjo ir naudotojo, kuriam teikiama parama iš ES kibernetinio saugumo rezervo, susitarimus. Tos paslaugos gali būti teikiamos pagal konkrečius patikimo valdomų saugumo paslaugų teikėjo, naudotojo ir paveikto subjekto susitarimus. Į visus šioje dalyje nurodytus susitarimus įtraukiamos, be kita ko, atsakomybės sąlygos.

6. 5 dalyje nurodyti susitarimai grindžiami šablonais, kuriuos rengia ENISA, pasikonsultavusi su valstybėmis narėmis ir, prireikus, su kitais ES kibernetinio saugumo rezervo naudotojais.

7. Komisija, ENISA ir ES kibernetinio saugumo rezervo naudotojai neprisiima sutartinės atsakomybės už žalą, sukeltą trečiosioms valstybėms dėl paslaugų, teikiamų įgyvendinant ES kibernetinio saugumo rezervą.

8. Naudotojai gali naudotis ES kibernetinio saugumo rezervo paslaugomis, teikiamomis atsakant į prašymą pagal 15 straipsnio 1 dalį, tik tam, kad padėtų reaguoti į reikšmingus kibernetinio saugumo incidentus, didelio masto kibernetinio saugumo incidentus arba didelio masto incidentams lygiaverčius kibernetinio saugumo incidentus ir inicijuoti veiklos atkūrimą po tokių incidentų. Tomis paslaugomis jie gali naudotis tik jeigu tai susiję su:

a) 14 straipsnio 3 dalies a punkte nurodytų naudotojų atveju – subjektais, vykdančiais veiklą ypatingos svarbos sektoriuose, arba subjektais, vykdančiais veiklą kituose itin svarbiuose sektoriuose, o 14 straipsnio 3 dalies c punkte nurodytų naudotojų atveju – lygiaverčiais subjektais, ir

b) 14 straipsnio 3 dalies b punkte nurodyto naudotojo atveju – Sąjungos institucijomis, organais, įstaigomis ir agentūromis.

9. Per du mėnesius nuo paramos pabaigos visi paramą gavę naudotojai pateikia apibendrinamąją suteiktos paslaugos, pasiektų rezultatų ir įgytos patirties ataskaitą:

a) 14 straipsnio 3 dalies a punkte nurodytų naudotojų atveju – Komisijai, ENISA, CSIRT tinklui ir EU-CyCLONe;

b) 14 straipsnio 3 dalies b punkte nurodyto naudotojo atveju – Komisijai, ENISA ir TKST;

c) 14 straipsnio 3 dalies c punkte nurodytų naudotojų atveju – Komisijai.

Visas apibendrinamąsias ataskaitas, gautas iš 14 straipsnio 3 dalyje nurodytų naudotojų pagal šios dalies pirmos pastraipos c punktą, Komisija perduoda Tarybai ir vyriausiajam įgaliotiniui.

10. Jei pagal šio reglamento 14 straipsnio 5 dalį ENISA visiškai arba iš dalies pavestas ES kibernetinio saugumo rezervo veikimas ir administravimas, ENISA tuo klausimu reguliariai teikia ataskaitas Komisijai ir su ja konsultuojasi. Tomis aplinkybėmis ENISA nedelsdama siunčia Komisijai visus prašymus, kuriuos ji gauna iš šio reglamento 14 straipsnio 3 dalies c punkte nurodytų naudotojų, ir, kai to reikia prioritetų nustatymo pagal šį straipsnį tikslais, visus prašymus, kuriuos ji gavo iš šio reglamento 14 straipsnio 3 dalies a arba b punkte nurodytų naudotojų. Šioje dalyje nustatytomis pareigomis nedaromas poveikis Reglamento (ES) 2019/881 14 straipsniui.

11. 14 straipsnio 3 dalies a ir b punktuose nurodytų naudotojų atveju perkančioji organizacija reguliariai ir bent du kartus per metus teikia ataskaitas TIS bendradarbiavimo grupei apie paramos naudojimą ir rezultatus.

12. 14 straipsnio 3 dalies c punkte nurodytų naudotojų atveju Komisija reguliariai, bent du kartus per metus, teikia ataskaitas Tarybai ir informuoja vyriausiąjį įgaliotinį apie paramos naudojimą ir rezultatus.

17 straipsnis

Patikimi valdomų saugumo paslaugų teikėjai

1. Viešojo pirkimo procedūrose, vykdomose siekiant sukurti ES kibernetinio saugumo rezervą, perkančioji organizacija veikia laikydamasi Reglamente (ES, Euratomas) 2024/2509 nustatytų principų ir šių principų:

a) užtikrinti, kad į ES kibernetinio saugumo rezervą įtrauktos paslaugos kaip visuma būtų tokios, kad ES kibernetinio saugumo rezervas apimtų paslaugas, kurios gali būti diegiamos visose valstybėse narėse, visų pirma atsižvelgiant į nacionalinius tokių paslaugų teikimo reikalavimus, įskaitant kalbų, sertifikavimo ar akreditavimo reikalavimus;

b) užtikrinti esminių Sąjungos ir jos valstybių narių saugumo interesų apsaugą;

c) užtikrinti, kad ES kibernetinio saugumo rezervas duotų Sąjungos pridėtinę vertę – padėtų siekti Reglamento (ES) 2021/694 3 straipsnyje nustatytų tikslų, be kita ko, skatinant kibernetinio saugumo įgūdžių ugdymą Sąjungoje.

2. Pirkdama ES kibernetinio saugumo rezervui skirtas paslaugas, perkančioji organizacija į pirkimo dokumentus įtraukia šiuos kriterijus ir reikalavimus:

a) paslaugų teikėjas turi įrodyti, kad jo darbuotojams būdingas aukščiausio lygio profesinis sąžiningumas, nepriklausomumas, atsakomybė ir reikiama techninė kompetencija, kad galėtų vykdyti veiklą savo konkrečioje srityje, ir užtikrina ekspertinių žinių pastovumą ir tęstinumą, taip pat reikiamus techninius išteklius;

b) paslaugų teikėjas ir visos atitinkamos patronuojamosios įmonės bei subrangovai turi laikytis taikytinų įslaptintos informacijos apsaugos taisyklių ir taikyti tinkamas priemones, įskaitant, kai aktualu, tarpusavio susitarimus, kad apsaugotų su paslauga susijusią konfidencialią informaciją, visų pirma įrodymus, išvadas ir ataskaitas;

c) paslaugų teikėjas turi tinkamai įrodyti, kad jo valdymo struktūra yra skaidri, dėl jos nekyla pavojus jo nešališkumui ir paslaugų kokybei ir negali kilti interesų konfliktų;

d) paslaugų teikėjas turi būti atlikęs tinkamą patikimumo patikrinimą, bent jau personalo, kurį ketina priskirti paslaugoms teikti, kai to reikalauja valstybė narė;

e) paslaugų teikėjas turi užtikrinti tinkamą savo IT sistemų saugumo lygį;

f) paslaugų teikėjas turi turėti aparatinę ir programinę įrangą, kurios reikia prašomai paslaugai teikti ir kuri neturi žinomų išnaudojamų pažeidžiamumų, apima naujausius saugumo naujinius ir bet kuriuo atveju atitinka visas taikytinas Europos Parlamento ir Tarybos reglamento (ES) 2024/2847 ([23]) nuostatas; nuostatas;

g) paslaugų teikėjas turi gebėti įrodyti, kad turi panašių paslaugų teikimo atitinkamoms nacionalinėms institucijoms, subjektams, vykdantiems veiklą ypatingos svarbos sektoriuose, arba subjektams, vykdantiems veiklą kituose itin svarbiuose sektoriuose, patirties;

h) paslaugų teikėjas turi gebėti suteikti paslaugą per trumpą laikotarpį valstybėse narėse, kuriose jis gali teikti paslaugą;

i) paslaugų teikėjas turi galėti teikti paslaugą viena ar daugiau Sąjungos institucijų arba valstybės narės oficialiųjų kalbų, jei to reikalauja valstybės narės arba 14 straipsnio 3 dalies b ir c punktuose nurodyti naudotojai, jei paslaugų teikėjas gali suteikti tokią paslaugą;

j) kai pagal Reglamentą (ES) 2019/881 bus įdiegta valdomų saugumo paslaugų Europos kibernetinio saugumo sertifikavimo sistema, paslaugų teikėjas turės būti sertifikuotas pagal tą sistemą per 2 metus nuo tos sistemos taikymo pradžios;

([23]) 2024 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/2847 dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828 (Kibernetinio atsparumo aktas) (OL L, 2024/2847, 2024 11 20, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

k) paslaugų teikėjas į pasiūlymą turi įtraukti bet kokios nepanaudotos reagavimo į incidentus paslaugos, kuri galėtų būti paversta parengties paslaugomis, glaudžiai susijusiomis su reagavimu į incidentus, pavyzdžiui, pratybomis ar mokymais, konvertavimo sąlygas.

3. Paslaugų pirkimo ES kibernetinio saugumo rezervui tikslu perkančioji organizacija, glaudžiai bendradarbiaudama su valstybėmis narėmis, prireikus, gali parengti kriterijus ir reikalavimus, papildančius 2 dalyje nurodytus kriterijus.

18 straipsnis

Veiksmai, kuriais remiama savitarpio pagalba

1. Reagavimo į kibernetinio saugumo krizes mechanizmu remiama vienos valstybės narės teikiama techninė pagalba kitai valstybei narei, nukentėjusiai nuo reikšmingo kibernetinio saugumo incidento arba didelio masto kibernetinio saugumo incidento, be kita ko, teikiama Direktyvos (ES) 2022/2555 11 straipsnio 3 dalies f punkte nurodytais atvejais.

2. Šio straipsnio 1 dalyje nurodyta parama techninei savitarpio pagalbai teikiama dotacijų forma ir laikantis Reglamento (ES) 2021/694 24 straipsnyje nurodytose atitinkamose darbo programose nustatytų sąlygų.

19 straipsnis

Parama SEP asocijuotosioms trečiosioms valstybėms

1. SEP asocijuotoji trečioji valstybė gali prašyti paramos iš ES kibernetinio saugumo rezervo, jei susitarime, pagal kurį ji yra asocijuota su SEP, numatytas dalyvavimas ES kibernetinio saugumo rezervo veikloje. Į tą susitarimą įtraukiamos nuostatos, kuriomis reikalaujama, kad atitinkama SEP asocijuotoji trečioji valstybė laikytųsi šio straipsnio 2 ir 9 dalyse nustatytų pareigų. Trečiosios valstybės dalyvavimo ES kibernetinio saugumo rezerve tikslais dalinė trečiosios valstybės asociacija su SEP gali apimti asociaciją, kuri apsiriboja Reglamento (ES) 2021/694 6 straipsnio 1 dalies g punkte nurodytu veiklos tikslu.

2. Per 3 mėnesius nuo 1 dalyje nurodyto susitarimo sudarymo ir bet kuriuo atveju prieš gaudamos paramą iš ES kibernetinio saugumo rezervo, SEP asocijuotosios trečiosios valstybės pateikia Komisijai informaciją apie savo kibernetinį atsparumą ir rizikos valdymo pajėgumus, įskaitant bent informaciją apie nacionalines priemones, kurių imtasi siekiant pasirengti reikšmingiems kibernetinio saugumo incidentams ar didelio masto incidentams lygiaverčiams kibernetinio saugumo incidentams, taip pat informaciją apie atsakingus nacionalinius subjektus, įskaitant reagavimo į kompiuterinius saugumo incidentus tarnybas arba lygiaverčius subjektus, jų pajėgumus ir jiems skirtus išteklius. SEP asocijuotoji trečioji valstybė reguliariai, bent kartą per metus, teikia tą atnaujintą informaciją. Komisija tą informaciją teikia vyriausiajam įgaliotiniui ir ENISA, kad būtų lengviau taikyti 11 dalį.

3. Komisija reguliariai ir bent kartą per metus kiekvienos 1 dalyje nurodytos SEP asocijuotosios trečiosios valstybės atžvilgiu įvertina šiuos kriterijus:

a) ar ta valstybė laikosi 1 dalyje nurodyto susitarimo sąlygų, kiek tos sąlygos susijusios su dalyvavimu ES kibernetinio saugumo rezervo veikloje;

b) ar ta valstybė, remdamasi 2 dalyje nurodyta informacija, ėmėsi tinkamų veiksmų, kad pasirengtų reikšmingiems kibernetinio saugumo incidentams arba didelio masto incidentams lygiaverčiams kibernetinio saugumo incidentams, ir

c) ar paramos teikimas dera su Sąjungos politika tos valstybės atžvilgiu ir bendrais santykiais su ja ir ar ji suderinama su kitomis Sąjungos politikos kryptimis saugumo srityje.

Atlikdama pirmoje pastraipoje nurodytą vertinimą dėl tos pastraipos c punkte nurodyto kriterijaus Komisija konsultuojasi su vyriausiuoju įgaliotiniu.

Jei Komisija padaro išvadą, kad SEP asocijuotoji trečioji valstybė atitinka visas pirmoje pastraipoje nurodytas sąlygas, ji pateikia Tarybai pasiūlymą priimti įgyvendinimo aktą pagal 4 dalį, kuriuo leidžiama tai valstybei teikti paramą iš ES kibernetinio saugumo rezervo.

4. Taryba gali priimti 3 dalyje nurodytus įgyvendinimo aktus. Tie įgyvendinimo aktai taikomi ne ilgiau kaip vienus metus. Jie gali būti atnaujinti. Juose gali būti nustatytas dienų, už kurias gali būti teikiama parama atsakant į vieną prašymą, skaičiaus apribojimas, kuris negali būti trumpesnis kaip 75 dienos.

Šio straipsnio tikslais Taryba imasi veiksmų nedelsdama ir paprastai priima šioje dalyje nurodytus įgyvendinimo aktus per aštuonias savaites nuo atitinkamo Komisijos pasiūlymo priėmimo pagal 3 dalies trečią pastraipą.

5. Taryba, remdamasi Komisijos pasiūlymu, gali bet kuriuo metu iš dalies pakeisti arba panaikinti pagal 4 dalį priimtą įgyvendinimo aktą.

Jei Taryba mano, kad padaryta reikšmingų pokyčių, susijusių su 3 dalies pirmos pastraipos c punkte nurodytu kriterijumi, Taryba gali iš dalies pakeisti arba panaikinti pagal 4 dalį priimtą įgyvendinimo aktą, remdamasi vienos ar daugiau valstybių narių tinkamai pagrįsta iniciatyva.

6. Naudodamasi savo įgyvendinimo įgaliojimais pagal šį straipsnį, Taryba taiko 3 dalies pirmoje pastraipoje nurodytus kriterijus ir paaiškina, kaip ji vertina tuos kriterijus. Visų pirma, kai Taryba veikia savo iniciatyva pagal 5 dalies antrą pastraipą, ji paaiškina toje pastraipoje nurodytą reikšmingą pokytį.

7. Parama iš ES kibernetinio saugumo rezervo SEP asocijuotajai trečiajai valstybei teikiama pagal šį reglamentą ir visas 1 dalyje nurodytame susitarime nustatytas specialiąsias sąlygas.

8. Naudotojai iš SEP asocijuotųjų trečiųjų valstybių, turintys teisę gauti paslaugas iš ES kibernetinio saugumo rezervo, apima kompetentingas institucijas, tokias kaip reagavimo į kompiuterinius saugumo incidentus tarnybas arba lygiaverčius subjektus ir kibernetinių krizių valdymo institucijas.

9. Kiekviena SEP asocijuotoji trečioji valstybė, atitinkanti paramos iš ES kibernetinio saugumo rezervo reikalavimus, paskiria instituciją, kuri šio reglamento tikslais veikia kaip vienas bendras kontaktinis punktas.

10. Paramos iš ES kibernetinio saugumo rezervo prašymus pagal šį straipsnį vertina Komisija. Perkančioji institucija gali teikti paramą trečiajai valstybei tik tuo atveju ir tik tol, kol galioja pagal šio straipsnio 4 dalį priimtas Tarybos įgyvendinimo aktas, kuriuo leidžiama teikti tokią paramą tos valstybės atžvilgiu. Atsakymas 14 straipsnio 3 dalies c punkte nurodytiems naudotojams perduodamas nepagrįstai nedelsiant.

11. Gavusi paramos prašymą pagal šį straipsnį, Komisija nedelsdama informuoja Tarybą. Komisija nuolat informuoja Tarybą apie prašymo vertinimą. Komisija taip pat bendradarbiauja su vyriausiuoju įgaliotiniu gautų SEP asocijuotųjų trečiųjų valstybių prašymų ir joms iš ES kibernetinio saugumo rezervo skirtos paramos įgyvendinimo klausimais. Be to, Komisija taip pat atsižvelgia į visas ENISA pateiktas nuomones dėl tų prašymų.

20 straipsnis

Koordinavimas su Sąjungos krizių valdymo mechanizmais

1. Kai reikšmingo kibernetinio saugumo incidento, didelio masto kibernetinio saugumo incidento arba didelio masto incidentui lygiaverčio kibernetinio saugumo incidento priežastis arba pasekmė yra nelaimė, kaip apibrėžta Sprendimo Nr. 1313/2013/ES 4 straipsnio 1 punkte, reagavimo į tokį incidentą parama pagal šį reglamentą papildo pagal tą sprendimą vykdomus veiksmus ir nedaro poveikio to sprendimo taikymui.

2. Didelio masto kibernetinio saugumo incidentui arba didelio masto incidentui lygiaverčio kibernetinio saugumo incidento atveju, kai aktyvuojamas ES integruotas politinio atsako į krizes mechanizmas pagal Įgyvendinimo sprendimą (ES) 2018/1993 (toliau – IPCR mechanizmas), pagal šį reglamentą teikiama reagavimo į tokį incidentą parama valdoma pagal atitinkamas IPCR mechanizmo procedūras.

IV SKYRIUS

EUROPOS KIBERNETINIO SAUGUMO INCIDENTŲ PERŽIŪROS MECHANIZMAS

21 straipsnis

Europos kibernetinio saugumo incidentų peržiūros mechanizmas

1. Komisijos arba EU-CyCLONe prašymu ENISA, padedama CSIRT tinklo ir gavusi atitinkamų valstybių narių pritarimą, peržiūri ir įvertina su konkrečiu reikšmingu kibernetinio saugumo incidentu arba didelio masto kibernetinio saugumo incidentu susijusias kibernetines grėsmes, žinomus pažeidžiamumus, kuriuos galima išnaudoti, ir poveikio mažinimo veiksmus. Užbaigusi incidento peržiūrą ir vertinimą ir siekdama, kad įgyta patirtis padėtų išvengti incidentų ateityje ar sumažinti jų padarinius, ENISA pateikia incidento peržiūros ataskaitą EU-CyCLONe, CSIRT tinklui, atitinkamoms valstybėms narėms ir Komisijai, kad padėtų joms atlikti savo užduotis, visų pirma Direktyvos (ES) 2022/2555 15 ir 16 straipsniuose nustatytas užduotis. Kai incidentas daro poveikį SEP asocijuotajai trečiajai valstybei, ENISA šią ataskaitą pateikia Tarybai. Tokiais atvejais Komisija tą ataskaitą pateikia vyriausiajam įgaliotiniui.

2. Rengdama šio straipsnio 1 dalyje nurodytą incidento peržiūros ataskaitą, ENISA bendradarbiauja su visais atitinkamais suinteresuotaisiais subjektais, įskaitant valstybių narių atstovus, Komisiją, kitas atitinkamas Sąjungos institucijas, organus, įstaigas ir agentūras, pramonę, įskaitant valdomų saugumo paslaugų teikėjus, ir kibernetinio saugumo paslaugų naudotojus, ir renka iš jų grįžtamąją informaciją. Kai tinkama, ENISA, bendradarbiaudama su CSIRT ir, kai tinkama, kompetentingomis institucijomis paskirtomis arba įsteigtomis pagal Direktyvos (ES) 2022/2555 8 straipsnio 1 dalį, taip pat bendradarbiauja su subjektais, paveiktais reikšmingų kibernetinio saugumo incidentų arba didelio masto kibernetinio saugumo incidentų. Atstovai, su kuriais konsultuojamasi, turi atskleisti informaciją apie bet kokį galimą interesų konfliktą.

3. Šio straipsnio 1 dalyje nurodytoje incidento peržiūros ataskaitoje pateikiama konkretaus reikšmingo kibernetinio saugumo incidento arba didelio masto kibernetinio saugumo incidento apžvalga ir analizė, apimanti pagrindines priežastis, žinomus pažeidžiamumus, kuriuos galima išnaudoti, ir įgytą patirtį. ENISA užtikrina, kad ataskaita atitiktų Sąjungos ar nacionalinę teisę dėl neskelbtinos ar įslaptintos informacijos apsaugos. Jei to prašo atitinkamos valstybės narės arba kiti 14 straipsnio 3 dalyje nurodyti naudotojai, kuriuos paveikė incidentas, ataskaitoje pateikiami duomenys ir informacija turi būti anonimizuoti. Joje nepateikiama jokios informacijos apie aktyviai išnaudotus pažeidžiamumus, kurie dar nepašalinti.

4. Kai tinkama, incidento peržiūros ataskaitoje pateikiamos rekomendacijos, kaip pagerinti Sąjungos kibernetinio saugumo būklę, ir joje gali būti pateikta geriausios praktikos pavyzdžių ir patirties, įgytos iš atitinkamų suinteresuotųjų subjektų.

5. ENISA gali paskelbti viešai prieinamą incidento peržiūros ataskaitos versiją. Toje ataskaitos versijoje pateikiama tik patikima vieša informacija arba kita patikima informacija gavus atitinkamų valstybių narių sutikimą, o informacijos, susijusios su 14 straipsnio 3 dalies b arba c punkte nurodytu naudotoju, atveju – gavus to naudotojo sutikimą.

V SKYRIUS

BAIGIAMOSIOS NUOSTATOS

22 straipsnis

Reglamento (ES) 2021/694 daliniai pakeitimai

Reglamentas (ES) 2021/694 iš dalies keičiamas taip:

1) 6 straipsnis iš dalies keičiamas taip:

a) 1 dalis iš dalies keičiama taip:

i) įterpiamas šis punktas:

„aa) remti Europos kibernetinio saugumo įspėjimų sistemos, sukurtos Europos Parlamento ir Tarybos reglamento (ES) 2025/38 (*) 3 straipsniu, (toliau – Europos kibernetinio saugumo įspėjimų sistema), plėtojimą, įskaitant nacionalinių kibernetinio saugumo centrų ir tarpvalstybinių kibernetinio saugumo centrų, kurie padeda didinti informuotumą apie padėtį Sąjungoje ir stiprinti Sąjungos kibernetinių grėsmių žvalgybos pajėgumus, kūrimą, diegimą ir veikimą;

(*) 2024 m. gruodžio 19 d. Europos Parlamento ir Tarybos reglamentas (ES) 2025/38, kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės ir iš dalies keičiamas Reglamentas (ES) 2021/694 (Kibernetinio solidarumo aktas) (OL L, 2025/38, 2025 1 15, ELI: http://data.europa.eu/eli/reg/2025/38/oj).“;

ii) papildoma šiuo punktu:

„g) sukurti ir valdyti Reagavimo į kibernetinio saugumo krizes mechanizmą, sukurtą Reglamento (ES) 2025/38 10 straipsniu, įskaitant ES kibernetinio saugumo rezervą, sukurtą to reglamento 14 straipsniu, (toliau – ES kibernetinio saugumo rezervas), skirtą padėti valstybėms narėms pasirengti reikšmingiems kibernetinio saugumo incidentams ir didelio masto kibernetinio saugumo incidentus bei į juos reaguoti, papildant nacionalinius išteklius bei pajėgumus ir kitų formų Sąjungos lygmeniu teikiamą paramą, taip pat padėti kitiems naudotojams reaguoti į reikšmingus kibernetinio saugumo incidentus ir didelio masto lygiaverčius kibernetinio saugumo incidentus;“;

b) 2 dalis pakeičiama taip:

„2. Veiksmai pagal 3 konkretų tikslą įgyvendinami pirmiausia pasitelkiant Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrą ir Nacionalinių koordinavimo centrų tinklą, vadovaujantis Europos Parlamento ir Tarybos reglamentu (ES) 2021/887 (*). Tačiau ES kibernetinio saugumo rezervą įgyvendina Komisija, o pagal Reglamento (ES) 2025/38 14 straipsnio 6 dalį – ENISA.

(*) 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/887, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas (OL L 202, 2021 6 8, p. 1).“;

2) 9 straipsnis iš dalies keičiamas taip:

a) 2 dalies b, c ir d punktai pakeičiami taip:

„b) 1 760 806 000 EUR skiriama 2 konkrečiam tikslui „Dirbtinis intelektas“;

c) 1 372 020 000 EUR skiriama 3 konkrečiam tikslui „Kibernetinis saugumas ir pasitikėjimas“;

d) 482 640 000 EUR skiriama 4 konkrečiam tikslui „Aukšto lygio skaitmeniniai įgūdžiai“;“;

b) papildoma šia dalimi:

„8. Nukrypstant nuo Finansinio reglamento 12 straipsnio 1 dalies, nepanaudoti įsipareigojimų ir mokėjimų asignavimai, skirti su ES kibernetinio saugumo rezervo įgyvendinimu susijusiems veiksmams ir savitarpio pagalbos rėmimo veiksmams pagal Reglamentą (ES) 2025/38, kuriais siekiama šio reglamento 6 straipsnio 1 dalies g punkte nustatytų tikslų, perkeliami automatiškai ir gali būti paskirti ir išmokėti iki kitų finansinių metų gruodžio 31 d. Europos Parlamentas ir Taryba informuojami apie asignavimus, perkeltus pagal Finansinio reglamento 12 straipsnio 6 dalį.“;

3) 12 straipsnis iš dalies keičiamas taip:

a) įterpiamos šios dalys:

„5a. 5 dalis netaikoma, kiek tai susiję su Sąjungoje įsisteigusiais, tačiau iš trečiųjų valstybių kontroliuojamais teisės subjektais, jokiems veiksmams, kuriais įgyvendinama Europos kibernetinio saugumo įspėjimų sistema, jeigu atitinkamo veiksmo atžvilgiu tenkinamos abi šios sąlygos:

a) atsižvelgiant į aprašo, atlikto pagal Reglamento (ES) 2025/38 9 straipsnio 4 dalį, rezultatus, esama realios rizikos, kad iš valstybėse narėse įsisteigusių arba laikomų įsteigusiais ir valstybių narių ar valstybių narių piliečių kontroliuojamų teisės subjektų nebus teikiamos priemonės, infrastruktūra arba paslaugos, kurios yra būtinos ir pakankamos, kad tuo veiksmu būtų tinkamai prisidedama prie Europos kibernetinio saugumo įspėjimų sistemos tikslo;

b) viešųjų pirkimų iš tokių teisės subjektų Europos kibernetinio saugumo įspėjimų sistemoje saugumo rizika yra proporcinga naudai ir nekenkia esminiams Sąjungos ir jos valstybių narių saugumo interesams.

5b. 5 dalis netaikoma, kiek tai susiję su Sąjungoje įsisteigusiais, tačiau iš trečiųjų valstybių kontroliuojamais teisės subjektais, jokiems veiksmams, kuriais įgyvendinamas ES kibernetinio saugumo rezervas, jeigu atitinkamo veiksmo atžvilgiu tenkinamos abi šios sąlygos:

a) atsižvelgiant į aprašo, atlikto pagal Reglamento (ES) 2025/38 14 straipsnio 6 dalį, rezultatus, esama realios rizikos, kad iš valstybėse narėse įsisteigusių arba laikomų įsteigusiais ir valstybių narių ar valstybių narių piliečių kontroliuojamų teisės subjektų nebus teikiamos technologijos, ekspertinės žinios ar pajėgumai, būtini ir pakankami, kad ES kibernetinio saugumo rezervas galėtų tinkamai vykdyti savo funkcijas;

b) tokių teisės subjektų įtraukimo į ES kibernetinio saugumo rezervą saugumo rizika yra proporcinga naudai ir nekenkia esminiams Sąjungos ir jos valstybių narių saugumo interesams.“;

b) 6 dalis pakeičiama taip:

„6. Jeigu pateisinama tinkamai pagrįstomis saugumo priežastimis, darbo programoje taip pat gali būti nurodyta, kad asocijuotosiose valstybėse įsisteigę teisės subjektai ir Sąjungoje įsisteigę, tačiau iš trečiųjų valstybių kontroliuojami teisės subjektai gali atitikti dalyvavimo visuose arba kai kuriuose veiksmuose pagal 1 ir 2 konkrečius tikslus reikalavimus tik tuo atveju, jei jie tenkina reikalavimus, kuriuos turi įvykdyti tie teisės subjektai, kad užtikrintų Sąjungos ir valstybių narių esminių saugumo interesų ir įslaptintų dokumentų informacijos apsaugą. Tie reikalavimai nustatomi darbo programoje.

Pirma pastraipa, kiek tai susiję su Sąjungoje įsisteigusiais, bet iš trečiųjų valstybių kontroliuojamais teisės subjektais, taip pat taikoma veiksmams pagal 3 konkretų tikslą:

a) siekiant įgyvendinti Europos kibernetinio saugumo įspėjimų sistemą, kai taikoma 5a dalis, ir

b) siekiant įgyvendinti ES kibernetinio saugumo rezervą, kai taikoma 5b dalis.“;

4) 14 straipsnio 2 dalis pakeičiama taip:

„2. Pagal Programą gali būti teikiamas bet kurios Finansiniame reglamente nustatytos formos finansavimas, visų pirma įskaitant viešuosius pirkimus kaip pagrindinę formą arba dotacijas ir apdovanojimus.

Kai veiksmo tikslui pasiekti reikalingi novatoriškų prekių ir paslaugų viešieji pirkimai, dotacijos skiriamos tik tiems naudos gavėjams, kurie yra perkančiosios organizacijos arba perkantieji subjektai, kaip apibrėžta Europos Parlamento ir Tarybos direktyvose 2014/24/ES (*) ir 2014/25/ES (**).

Kai veiksmo tikslams pasiekti būtinas novatoriškų dideliu mastu komercinėmis sąlygomis dar neprieinamų prekių tiekimas ar paslaugų teikimas, perkančioji organizacija arba perkantysis subjektas gali leisti skirti kelias sutartis tos pačios viešųjų pirkimų procedūros metu.

Perkančioji organizacija arba perkantysis subjektas dėl tinkamai pagrįstų saugumo priežasčių gali reikalauti, kad sutarties vykdymo vieta būtų Sąjungos teritorijoje.

Įgyvendindamos viešųjų pirkimų procedūras, skirtas ES kibernetinio saugumo rezervui, Komisija ir ENISA gali veikti kaip centrinė perkančioji organizacija, perkanti Programos asocijuotosioms trečiosioms valstybėms arba jų vardu pagal šio reglamento 10 straipsnį. Komisija ir ENISA gali veikti ir kaip didmenininkės, perkančios, sandėliuojančios ir perparduodančios arba dovanojančios prekes ir paslaugas, taip pat jas nuomojančios toms trečiosioms valstybėms.

Nukrypstant nuo Europos Parlamento ir Tarybos reglamento (ES, Euratomas) 2024/2509 (***) 168 straipsnio 3 dalies, pavienės trečiosios valstybės prašymo pakanka, kad Komisija arba ENISA būtų įgaliota imtis veiksmų.

Įgyvendindamos viešųjų pirkimų procedūras, skirtas ES kibernetinio saugumo rezervui, Komisija ir ENISA gali veikti kaip centrinė perkančioji organizacija, perkanti Sąjungos institucijoms, organams, įstaigoms ar agentūroms arba jų vardu. Komisija ir ENISA gali veikti ir kaip didmenininkės, perkančios, sandėliuojančios ir perparduodančios arba dovanojančios prekes ir paslaugas, taip pat jas nuomojančios Sąjungos institucijoms, organams, įstaigoms ar agentūroms. Nukrypstant nuo Reglamento (ES, Euratomas) 2024/2509 168 straipsnio 3 dalies, vienos Sąjungos institucijos, organo, įstaigos ar agentūros prašymo pakanka, kad Komisija arba ENISA būtų įgaliota imtis veiksmų.

Finansavimas pagal Programą taip pat gali būti teikiamas finansinėmis priemonėmis, naudojant derinimo operacijas.

(*) 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).
(**) 2014 m. vasario 26 d. Europos Parlamento ir Tarybos direktyva 2014/25/ES dėl subjektų, vykdančių veiklą vandens, energetikos, transporto ir pašto paslaugų sektoriuose, vykdomų pirkimų, kuria panaikinama Direktyva 2004/17/EB (OL L 94, 2014 3 28, p. 243).
(***) 2024 m. rugsėjo 23 d. Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) 2024/2509 dėl Sąjungos bendrajam biudžetui taikomų finansinių taisyklių (OL L, 2024/2509, 2024 9 26, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).“;

5) įterpiamas šis straipsnis:

„*16a straipsnis*

Prieštaravimai tarp taisyklių

Veiksmų, kuriais įgyvendinama Europos kibernetinio saugumo įspėjimų sistema, atveju taikomos Reglamento (ES) 2025/38 4, 5 ir 9 straipsniuose nustatytos taisyklės. Jei šio reglamento nuostatos prieštarauja Reglamento (ES) 2025/38 4, 5 ir 9 straipsniams, pirmenybė teikiama pastarajam reglamentui ir jis taikomas tiems konkretiems veiksmams.

ES kibernetinio saugumo rezervo atveju, konkrečios Programos asocijuotųjų trečiųjų valstybių dalyvavimo taisyklės yra nustatytos Reglamento (ES) 2025/38 19 straipsnyje. Jei šio reglamento nuostatos prieštarauja Reglamento (ES) 2025/38 19 straipsniui, pirmenybė teikiama pastarajam reglamentui ir jis taikomas tiems konkretiems veiksmams.“;

6) 19 straipsnis pakeičiamas taip:

„*19 straipsnis*

Dotacijos

„Programos dotacijos skiriamos ir valdomos pagal Finansinio reglamento VIII antraštinę dalį ir jomis galima padengti iki 100 proc. tinkamų finansuoti išlaidų, nedarant poveikio bendro finansavimo principui, nustatytam Finansinio reglamento 190 straipsnyje. Tokios dotacijos skiriamos ir valdomos kaip nurodyta kiekvieno konkretaus tikslo atveju.

Pagal Finansinio reglamento 195 straipsnio 1 dalies d punktą paramą dotacijų forma ECCC gali tiesiogiai skirti Reglamento (ES) 2025/38 9 straipsnyje nurodytoms atrinktoms valstybėms narėms ir Reglamento (ES) 2025/38 5 straipsnyje nurodytam prieglobos konsorciumui, neskelbdamas kvietimo teikti pasiūlymus.

Pagal Finansinio reglamento 195 straipsnio 1 dalies d punktą ECCC valstybėms narėms gali tiesiogiai skirti Reagavimo į kibernetinio saugumo krizes mechanizmo paramą dotacijų forma, neskelbdamas kvietimo teikti pasiūlymus.

Veiksmų, kuriais remiamas savitarpio pagalbos teikimas, atveju, kaip numatyta Reglamento (ES) 2025/38 18 straipsnyje, ECCC informuoja Komisiją ir ENISA apie valstybių narių prašymus skirti tiesiogines dotacijas neskelbiant kvietimo teikti pasiūlymus. 18 straipsnyje, ECCC informuoja Komisiją ir ENISA apie valstybių narių prašymus skirti tiesiogines dotacijas neskelbiant kvietimo teikti pasiūlymus.

Veiksmų, kuriais remiamas savitarpio pagalbos teikimas, atveju, kaip numatyta Reglamento (ES) 2025/38 18 straipsnyje, ir laikantis Finansinio reglamento 193 straipsnio 2 dalies antros pastraipos a punkto, išlaidos tinkamai pagrįstais atvejais gali būti laikomos tinkamomis finansuoti, net jei jos buvo patirtos prieš pateikiant dotacijos paraišką.“;

7) I ir II priedai iš dalies keičiami pagal šio reglamento priedą.

23 straipsnis

Įgaliojimų delegavimas

1. Įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami šiame straipsnyje nustatytomis sąlygomis.

2. Įgaliojimai priimti 14 straipsnio 7 dalyje nurodytus deleguotuosius aktus Komisijai suteikiami 5 metų laikotarpiui nuo 2025 m. vasario 5 d. Likus ne mažiau kaip 9 mėnesiams iki 5 metų laikotarpio pabaigos Komisija parengia naudojimosi deleguotaisiais įgaliojimais ataskaitą. Deleguotieji įgaliojimai savaime pratęsiami tokios pačios trukmės laikotarpiams, išskyrus atvejus, kai Europos Parlamentas arba Taryba pareiškia prieštaravimų dėl tokio pratęsimo likus ne mažiau kaip 3 mėnesiams iki kiekvieno laikotarpio pabaigos.

3. Europos Parlamentas arba Taryba gali bet kada atšaukti 14 straipsnio 7 dalyje nurodytus deleguotuosius įgaliojimus. Sprendimu dėl įgaliojimų atšaukimo nutraukiami tame sprendime nurodyti įgaliojimai priimti deleguotuosius aktus. Sprendimas įsigalioja kitą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje* arba vėlesnę jame nurodytą dieną. Jis nedaro poveikio jau galiojančių deleguotųjų aktų galiojimui.

4. Prieš priimdama deleguotąjį aktą Komisija konsultuojasi su kiekvienos valstybės narės paskirtais ekspertais vadovaudamasi 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros nustatytais principais.

5. Apie priimtą deleguotąjį aktą Komisija nedelsdama vienu metu praneša Europos Parlamentui ir Tarybai.

6. Pagal 14 straipsnio 7 dalį priimtas deleguotasis aktas įsigalioja tik tuo atveju, jeigu per 2 mėnesius nuo pranešimo Europos Parlamentui ir Tarybai apie šį aktą dienos nei Europos Parlamentas, nei Taryba nepareiškia prieštaravimų arba jeigu dar nepasibaigus šiam laikotarpiui ir Europos Parlamentas, ir Taryba praneša Komisijai, kad prieštaravimų nereikš. Europos Parlamento arba Tarybos iniciatyva šis laikotarpis pratęsiamas 2 mėnesiais.

24 straipsnis

Komiteto procedūra

1. Komisijai padeda Skaitmeninės Europos programos koordinavimo komitetas, nurodytas Reglamento (ES) 2021/694 31 straipsnio 1 dalyje. Tas komitetas – tai komitetas, kaip tai suprantama Reglamente (ES) Nr. 182/2011.

2. Kai daroma nuoroda į šią dalį, taikomas Reglamento (ES) Nr. 182/2011 5 straipsnis.

25 straipsnis

Vertinimas ir peržiūra

1. Ne vėliau kaip 2027 m. vasario 5 d., o vėliau – bent kas 4 metus Komisija įvertina šiame reglamente numatytų priemonių veikimą ir pateikia Europos Parlamentui ir Tarybai ataskaitą.

2. 1 dalyje nurodytu vertinimu visų pirma įvertinama:

a) įsteigtų nacionalinių kibernetinio saugumo centrų ir tarpvalstybinių kibernetinio saugumo centrų skaičius, dalijimosi informacija mastas, įskaitant, jei įmanoma, poveikį CSIRT tinklo darbui, ir tai, kokiu mastu tie centrai padėjo stiprinti bendrą Sąjungos kibernetinių grėsmių ir incidentų aptikimą bei informuotumą apie padėtį ir plėtoti pažangiausias technologijas; SEP finansavimo naudojimas bendrai įsigytoms kibernetinio saugumo priemonėms, infrastruktūrai ar

paslaugoms; ir, jei turima tokia informacija, nacionalinių kibernetinio saugumo centrų ir Direktyvos (ES) 2022/2555 3 straipsnyje nurodytų sektorinių bei tarpsektorinių esminių ir svarbių subjektų bendruomenių bendradarbiavimo lygis;

b) veiksmų pagal Reagavimo į kibernetinio saugumo krizes mechanizmą, kuriais remiama parengtis, įskaitant mokymus, reagavimą į reikšmingus kibernetinio saugumo incidentus, didelio masto kibernetinio saugumo incidentus ir didelio masto incidentams lygiaverčius kibernetinio saugumo incidentus bei pradinį veiklos atkūrimą po tų incidentų, naudojimas ir veiksmingumas, įskaitant SEP finansavimo naudojimas, ir įgyvendinant Reagavimo į kibernetinio saugumo krizes mechanizmą įgyta patirtis bei rekomendacijos;

c) ES kibernetinio saugumo rezervo naudojimas ir veiksmingumas atsižvelgiant į naudotojų tipus, įskaitant SEP finansavimo naudojimą, paslaugų naudojimas, įskaitant jų rūšį, vidutinis atsakymo į prašymus ir ES kibernetinio saugumo rezervo panaudojimo laikas, paslaugų, paverstų parengties paslaugomis, susijusiomis su incidentų prevencija ir reagavimu į juos, procentinė dalis, taip pat įgyvendinant ES kibernetinio saugumo rezervą įgyta patirtis ir rekomendacijos;

d) šio reglamento indėlis stiprinant Sąjungos pramonės ir paslaugų sektorių, įskaitant labai mažas, mažąsias ir vidutines įmones bei startuolius, konkurencinę padėtį visoje skaitmeninėje ekonomikoje, taip pat indėlis siekiant bendro tikslo stiprinti darbo jėgos kibernetinio saugumo įgūdžius ir gebėjimus.

3. Remdamasi 1 dalyje nurodytomis ataskaitomis, Komisija, kai tikslinga, pateikia Europos Parlamentui ir Tarybai pasiūlymą dėl teisėkūros procedūra priimamo akto dėl šio reglamento dalinio keitimo.

26 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. gruodžio 19 d.

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkė	*Pirmininkas*
R. METSOLA	BÓKA J.

PRIEDAS

Reglamentas (ES) 2021/694 iš dalies keičiamas taip:

1) I priedo skirsnis „3 konkretus tikslas: Kibernetinis saugumas ir pasitikėjimas“ pakeičiamas taip:

„3 konkretus tikslas: Kibernetinis saugumas ir pasitikėjimas

Programa skatinamas pagrindinių pajėgumų apsaugoti Sąjungos skaitmeninę ekonomiką, visuomenę ir demokratiją stiprinimas, kūrimas ir įgijimas, stiprinant Sąjungos kibernetinio saugumo sektoriaus potencialą ir konkurencingumą, taip pat didinant tiek privačiojo, tiek viešojo sektorių pajėgumą apsaugoti piliečius ir įmones nuo kibernetinių grėsmių, įskaitant Direktyvos (ES) 2016/1148 įgyvendinimo rėmimą.

Pagal šį tikslą pradiniai ir prireikus tolesni veiksmai apima:

1. Bendrą investavimą su valstybėmis narėmis į pažangią kibernetinio saugumo įrangą, infrastruktūrą ir praktinę patirtį, kurios yra būtinos siekiant apsaugoti ypatingos svarbos infrastruktūros objektus ir bendrąją skaitmeninę rinką apskritai. Toks bendras investavimas galėtų apimti investicijas į kvantinės infrastruktūros objektus ir kibernetinio saugumo duomenų išteklius, informuotumą apie padėtį kibernetinėje erdvėje, įskaitant nacionalinius kibernetinio saugumo centrus ir tarpvalstybinius kibernetinio saugumo centrus, sudarančius Europos kibernetinio saugumo įspėjimų sistemą, taip pat kitas priemones, kurios turi tapti prieinamos viešajam ir privačiajam sektoriams visoje Europoje.

2. Esamo technologinio pajėgumo išplėtimą ir kompetencijos centrų valstybėse narėse sujungimą į tinklą, taip pat užtikrinimą, kad tie pajėgumai atitiktų viešojo sektoriaus ir pramonės poreikius, be kita ko, pasitelkiant produktus ir paslaugas, kuriais stiprinamas kibernetinis saugumas ir pasitikėjimas bendrojoje skaitmeninėje rinkoje.

3. Užtikrinimą, kad visose valstybėse narėse būtų plačiai diegiami veiksmingi pažangiausi kibernetinio saugumo ir pasitikėjimo sprendimai. Toks diegimas apima produktų saugumo ir saugos stiprinimą nuo jų kūrimo iki jų komercializacijos.

4. Paramą kibernetinio saugumo įgūdžių spragoms šalinti, atsižvelgiant į lyčių pusiausvyrą, pavyzdžiui, suderinant kibernetinio saugumo įgūdžių programas, pritaikant jas prie konkrečių sektorių poreikių ir palengvinant galimybes dalyvauti tiksliniuose specializuotuose mokymuose.

5. Valstybių narių solidarumo rengiantis reikšmingiems kibernetinio saugumo incidentams ir didelio masto kibernetinio saugumo incidentus ir į juos reaguojant skatinimą, tarpvalstybiniu mastu diegiant kibernetinio saugumo paslaugas, įskaitant paramą valdžios institucijų savitarpio pagalbai ir patikimų valdomų saugumo paslaugų teikėjų rezervo sukūrimą Sąjungos lygmeniu.“;

2) II priedo skirsnis „3 konkretus tikslas: Kibernetinis saugumas ir pasitikėjimas“ pakeičiamas taip:

„3 konkretus tikslas: Kibernetinis saugumas ir pasitikėjimas

3.1. Bendrai įsigytų, be kita ko, Europos kibernetinio saugumo įspėjimų sistemos kontekste, kibernetinės infrastruktūros objektų arba priemonių ar tiek objektų, tiek priemonių skaičius

3.2. Naudotojų ir naudotojų bendruomenių, kurie gauna prieigą prie Europos kibernetinio saugumo įrenginių, skaičius

3.3. Pagal Reagavimo į kibernetinio saugumo krizes mechanizmą vykdomų veiksmų, kuriais remiamas pasirengimas kibernetinio saugumo incidentams ir reagavimas į juos, skaičius“.

Dėl šio akto buvo padarytas pareiškimas; jį galima rasti OL C, C/2025/308, 2025 1 15, ELI: http://data.europa.eu/eli/C/2025/308/oj.