Europos Sąjungos Taryba

Briuselis, 2023 m. balandžio 20 d.
(OR. en)

8512/23

Tarpinstitucinė byla:
2023/0109 (COD)

CYBER 92
TELECOM 108
CADREFIN 51
FIN 448
BUDGET 6
IND 181
JAI 471
MI 314
DATAPROTECT 110
RELEX 481
CODEC 662

PASIŪLYMAS

nuo:	Europos Komisijos generalinės sekretorės, kurios vardu pasirašo direktorė Martine DEPREZ
gavimo data:	2023 m. balandžio 19 d.
kam:	Europos Sąjungos Tarybos generalinei sekretorei Thérèse BLANCHET
Komisijos dok. Nr.:	COM(2023) 209 final
Dalykas:	Pasiūlymas dėl EUROPOS PARLAMENTO IR TARYBOS REGLAMENTO, kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės

Delegacijoms pridedamas dokumentas COM(2023) 209 final.

Pridedama: COM(2023) 209 final

EUROPOS
KOMISIJA

Strasbūras, 2023 04 18
COM(2023) 209 final

2023/0109 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės

AIŠKINAMASIS MEMORANDUMAS

1. PASIŪLYMO APLINKYBĖS

• Pasiūlymo pagrindimas ir tikslai

Šis aiškinamasis memorandumas pridedamas prie pasiūlymo dėl Kibernetinio solidarumo akto. Informacinių ir ryšių technologijų naudojimas ir priklausomumas nuo jų tapo visų ekonominės veiklos sektorių esminiais aspektais, nes mūsų viešojo administravimo institucijos, įmonės ir piliečiai skirtinguose sektoriuose ir skirtingose valstybėse labiau susieti tarpusavyje ir vieni nuo kitų priklausomi, nei bet kada anksčiau. Diegiant daugiau skaitmeninių technologijų didėja kibernetinio saugumo incidentų rizika ir jų galimas poveikis. Kartu valstybėse narėse didėja kibernetinio saugumo rizika ir apskritai yra sudėtingos grėsmės aplinkybės, taip pat aiški rizika, kad kibernetiniai incidentai sparčiai išplis iš vienos valstybės narės į kitą.

Be to, kibernetinės operacijos vis labiau integruojamos į hibridines ir karo strategijas ir daro didelį poveikį taikiniui. Visų pirma prieš Rusijos karinę agresiją prieš Ukrainą ir jos metu buvo įgyvendinama priešiškų kibernetinių operacijų strategija, kuri iš esmės keičia ES kolektyvinio kibernetinio saugumo krizių valdymo parengties suvokimą bei vertinimą ir skatina imtis skubių veiksmų. Dėl galimo didelio masto incidento, dėl kurio gali kilti didelių sutrikimų ir būti padaryta žala ypatingos svarbos infrastruktūros objektams, grėsmės reikia didinti parengtį visais ES kibernetinio saugumo ekosistemos lygmenimis. Ši grėsmė yra susijusi ne tik su Rusijos karine agresija prieš Ukrainą ir apima nuolatines kibernetines grėsmes, kurias kelia valstybiniai ir nevalstybiniai subjektai ir kurios, tikėtina, išliks, atsižvelgiant į tai, kad dabartinę geopolitinę įtampą lemia daugybė su valstybe susijusių subjektų, nusikaltėlių ir įsilaužėlių aktyvistų. Pastaraisiais metais kibernetinių išpuolių skaičius smarkiai išaugo, įskaitant tiekimo grandinės atakas, kurių tikslas – kibernetinis šnipinėjimas, išpirkos reikalavimo programinės įrangos įdiegimas ar trikdymas. 2020 m. „SolarWinds“ tiekimo grandinės ataka paveikė daugiau nei 18 000 organizacijų visame pasaulyje, įskaitant vyriausybines agentūras, dideles įmones. Reikšmingų kibernetinių incidentų trikdomasis poveikis gali būti pernelyg didelis, tad vienai ar kelioms paveiktoms valstybėms narėms, veikiant pavieniui, gali būti sunku su jais susidoroti. Dėl šios priežasties reikia stiprinti solidarumą Sąjungos lygmeniu, kad būtų galima geriau aptikti kibernetinio saugumo grėsmes ir incidentus, jiems pasirengti ir į juos reaguoti.

Kalbant apie kibernetinių grėsmių ir incidentų aptikimą, reikia skubiai intensyvinti keitimąsi informacija ir didinti mūsų kolektyvinius pajėgumus, kad būtų drastiškai sumažintas laikas, reikalingas kibernetinėms grėsmėms aptikti iki joms galint sukelti žalą ir išlaidas dideliu mastu[1]. Nors dėl skaitmeninės infrastruktūros objektų sujungimo daugelis kibernetinio saugumo grėsmių ir incidentų gali būti tarpvalstybinio pobūdžio, valstybių narių keitimasis

[1] Remiantis „Ponemon Institute“ ir „IBM Security“ pranešimu, 2022 m. vidutinis laikas, per kurį aptinkamas pažeidimas, buvo 207 dienos, o jam suvaldyti prireikdavo vidutiniškai dar 70 dienų. Be to, 2022 m. duomenų saugumo pažeidimai, kurių gyvavimo ciklas ilgesnis nei 200 dienų, vidutiniškai kainavo 4,86 mln. EUR, palyginti su 3,74 mln. EUR, kai ciklas yra trumpesnis nei 200 dienų. („Cost of a data breach 2022“, https://www.ibm.com/reports/data-breach).

atitinkama informacija tebėra ribotas. Padėti spręsti šią problemą siekiama kuriant tarpvalstybinių saugumo operacijų centrų (SOC) tinklą, kad būtų sustiprinti aptikimo ir reagavimo pajėgumai.

Kalbant apie parengtį kibernetinio saugumo incidentams ir reagavimą į juos, šiuo metu Sąjungos lygmeniu teikiama parama ir valstybių narių solidarumas yra riboti. 2021 m. spalio mėn. Tarybos išvadose pabrėžiama, kad šias spragas reikia šalinti, ir Komisija raginama pateikti pasiūlymą dėl naujo Reagavimo į kibernetinio saugumo krizes fondo[2].

Šiuo reglamentu taip pat įgyvendinama 2020 m. gruodžio mėn. priimta ES kibernetinio saugumo strategija[3], kurioje paskelbta apie Europos kibernetinio saugumo skydo sukūrimą, taip stiprinant kibernetinių grėsmių aptikimo ir keitimosi informacija pajėgumus Europos Sąjungoje, sujungiant nacionalinius ir tarpvalstybinius SOC.

Šis reglamentas grindžiamas pirmaisiais veiksmais, kurių jau imtasi glaudžiai bendradarbiaujant su pagrindiniais suinteresuotaisiais subjektais ir kurie remiami pagal Skaitmeninės Europos programą. Visų pirma, pagal 2021–2022 m. Skaitmeninės Europos programos kibernetinio saugumo darbo programą dėl SOC parengtas kvietimas pareikšti susidomėjimą bendrai pirkti priemones ir infrastruktūros objektus tarpvalstybiniams SOC steigti ir kvietimas dėl dotacijų viešąsias ir privačiąsias organizacijas aptarnaujančių SOC pajėgumams stiprinti. Parengties ir reagavimo į incidentus srityje Komisija parengė trumpojo laikotarpio paramos valstybėms narėms programą, skirdama papildomą finansavimą Europos Sąjungos kibernetinio saugumo agentūrai (ENISA), kad būtų nedelsiant sustiprinta parengtis ir pajėgumai reaguoti į didelius kibernetinius incidentus. Abu veiksmai parengti glaudžiai bendradarbiaujant su valstybėmis narėmis. Šiuo reglamentu šalinami trūkumai ir integruojamos iš tų veiksmų gautos įžvalgos.

Galiausiai šiuo pasiūlymu įgyvendinamas lapkričio 10 d. priimtame bendrame komunikate dėl kibernetinės gynybos[4] nustatytas įsipareigojimas parengti ES kibernetinio solidarumo iniciatyvos pasiūlymą siekiant šių tikslų: stiprinti bendrus ES aptikimo, informuotumo apie padėtį ir reagavimo pajėgumus, palaipsniui sukurti ES lygmens kibernetinių išteklių rezervą, grindžiamą patikimų privačių paslaugų teikėjų paslaugomis, ir remti ypatingos svarbos subjektų testavimą.

Atsižvelgdama į tai, Komisija siūlo šį Kibernetinio solidarumo aktą, kuriuo siekiama stiprinti Sąjungos lygmens solidarumą, kad būtų galima geriau aptikti kibernetinio saugumo grėsmes ir incidentus, jiems pasirengti ir į juos reaguoti siekiant šių konkrečių tikslų:

---

[2] Tarybos išvados dėl Europos Sąjungos kibernetinio saugumo būklės raidos, kurias Taryba patvirtino 2022 m. gegužės 23 d. posėdyje (dok. 9364/22).

[3] Bendras komunikatas Europos Parlamentui ir Tarybai „Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategija“ (JOIN(2020) 18 *final*).

[4] Bendras komunikatas Europos Parlamentui ir Tarybai „ES kibernetinės gynybos politika“, JOIN(2022) 49 *final*.

- stiprinti bendrą ES kibernetinių grėsmių ir incidentų aptikimą ir informuotumą apie padėtį, taip prisidedant prie Europos technologinio suverenumo kibernetinio saugumo srityje;
- stiprinti ypatingos svarbos subjektų parengtį visoje ES ir stiprinti solidarumą plėtojant bendrus reagavimo į reikšmingus arba didelio masto kibernetinio saugumo incidentus pajėgumus, be kita ko, teikiant reagavimo į incidentus paramą su Skaitmeninės Europos programa susijusioms trečiosioms valstybėms;
- didinti Sąjungos atsparumą ir prisidėti prie veiksmingo reagavimo peržiūrint ir įvertinant reikšmingus arba didelio masto incidentus, be kita ko, apibendrinant įgytą patirtį ir, kai tinkama, rengiant rekomendacijas.

Šie tikslai bus įgyvendinami imantis šių veiksmų:

- Europos masto SOC infrastruktūros (Europos kibernetinio saugumo skydo) diegimas siekiant sukurti ir sustiprinti bendrus aptikimo ir informuotumo apie padėtį gebėjimus;
- Reagavimo į kibernetinio saugumo krizes mechanizmo sukūrimas, siekiant padėti valstybėms narėms pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams, į juos reaguoti ir nedelsiant atkurti veiklą. Reagavimo į incidentus parama taip pat teikiama Sąjungos institucijoms, įstaigoms, organams ir agentūroms;
- Europos kibernetinio saugumo incidentų peržiūros mechanizmo sukūrimas, kad būtų galima peržiūrėti ir įvertinti konkrečius reikšmingus arba didelio masto incidentus.

Europos kibernetinio saugumo skydas ir Reagavimo į kibernetinio saugumo krizes mechanizmas bus remiami juos finansuojant pagal Skaitmeninės Europos programą, kurią ši teisinė priemonė iš dalies pakeis, kad būtų nustatyti pirmiau minėti veiksmai, numatyta finansinė parama jiems plėtoti ir paaiškintos finansinės paramos gavimo sąlygos.

- **Suderinamumas su toje pačioje politikos srityje galiojančiomis nuostatomis**

ES sistemą sudaro keli Sąjungos lygmeniu jau priimti arba pasiūlyti teisės aktai, kuriais siekiama sumažinti pažeidžiamumų, padidinti ypatingos svarbos subjektų atsparumą kibernetinio saugumo rizikai ir remti koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą, visų pirma Direktyva dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (TIS 2 direktyva)[5], Kibernetinio saugumo aktas[6], Direktyva dėl atakų prieš informacines sistemas[7] ir Komisijos rekomendacija

[5] 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).

[6] 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).

[7] 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.

(ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes[8].

Pagal Kibernetinio solidarumo aktą siūlomi veiksmai apima informuotumą apie padėtį, dalijimąsi informacija, taip pat paramą pasirengti kibernetiniams incidentams ir į juos reaguoti. Šie veiksmai dera su Sąjungos lygmeniu galiojančios reglamentavimo sistemos tikslais, visų pirma pagal Direktyvą (ES) 2022/2555 (toliau – TIS 2 direktyva), ir juos remia. Kibernetinio solidarumo aktas visų pirma bus grindžiamas esamomis operatyvinio bendradarbiavimo kibernetinio saugumo srityje ir krizių valdymo sistemomis, visų pirma Europos ryšių palaikymo dėl kibernetinių krizių organizaciniu tinklu (EU-CyCLONe) ir reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) tinklu.

Tarpvalstybinių SOC platformos turėtų sukurti naujus pajėgumus, kurie papildytų CSIRT tinklą, kaupiant viešųjų ir privačiųjų subjektų duomenis apie grėsmes kibernetiniam saugumui bei jais dalijantis, didinant tokių duomenų vertę atliekant ekspertų analizę ir taikant pažangiausias priemones, taip pat prisidedant prie Sąjungos pajėgumų ir technologinio suverenumo plėtojimo.

Galiausiai šis pasiūlymas atitinka Tarybos rekomendaciją dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą[9], kurioje valstybės narės raginamos imtis skubių ir veiksmingų priemonių ir lojaliai, 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.

- **Suderinamumas su kitomis Sąjungos politikos sritimis**

Pasiūlymas dera su kitais krizių valdymo mechanizmais ir protokolais, pavyzdžiui, ES integruotu politinio atsako į krizes mechanizmu (IPCR). Kibernetinio solidarumo aktas papildys šias krizių valdymo sistemas ir protokolus, užtikrindamas specialią paramą pasirengimo kibernetinio saugumo incidentams ir reagavimo į juos srityje. Pasiūlymas taip pat derės su ES išorės veiksmais reaguojant į didelio masto incidentus pagal bendrą užsienio ir saugumo politiką (BUSP), be kita ko, pasitelkiant ES Kibernetinio saugumo diplomatijos priemonių rinkinį. Pasiūlymu bus papildyti veiksmai, įgyvendinami pagal Europos Sąjungos sutarties 42 straipsnio 7 dalį arba Sutarties dėl Europos Sąjungos veikimo 222 straipsnyje apibrėžtais atvejais.

[8] Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams, kuriuo iš dalies keičiamas Reglamentas (ES) 2019/1020, COM(2022) 454 *final*.

[9] 2022 m. gruodžio 8 d. Tarybos rekomendacija dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą (Tekstas svarbus EEE) 2023/C 20/01.

Juo taip pat papildomas 2013 m. gruodžio mėn. sukurtas Sąjungos civilinės saugos mechanizmas (SCSM)[10], užbaigtas 2021 m. gegužės mėn. priimtu nauju teisės aktu[11], kuriuo stiprinami SCSM prevencijos, parengties bei reagavimo ramsčiai ir ES suteikiami papildomi pajėgumai reaguoti į naujų rūšių riziką Europoje ir pasaulyje, taip pat padidinamas rezervas „rescEU“.

2. TEISINIS PAGRINDAS, SUBSIDIARUMO IR PROPORCINGUMO PRINCIPAI

• Teisinis pagrindas

Šio pasiūlymo teisinis pagrindas yra Sutarties dėl Europos Sąjungos veikimo (SESV) 173 straipsnio 3 dalis ir 322 straipsnio 1 dalies a punktas. SESV 173 straipsnyje numatyta, kad Sąjunga ir valstybės narės užtikrina, kad būtų sudarytos Sąjungos pramonės konkurencingumui reikalingos sąlygos. Šiuo reglamentu siekiama stiprinti Europos pramonės ir paslaugų sektorių konkurencinę padėtį skaitmeninėje ekonomikoje ir remti jų skaitmeninę transformaciją, didinant kibernetinio saugumo lygį bendrojoje skaitmeninėje rinkoje. Visų pirma juo siekiama padidinti piliečių, įmonių ir subjektų, veikiančių ypatingos svarbos ir itin svarbiuose sektoriuose, atsparumą didėjančioms kibernetinio saugumo grėsmėms, kurios gali padaryti pražūtingą poveikį visuomenei ir ekonomikai.

Pasiūlymas taip pat grindžiamas SESV 322 straipsnio 1 dalies a punktu, nes jame nustatytos specialios perkėlimo į kitą laikotarpį taisyklės, kuriomis nukrypstama nuo metinio periodiškumo principo, nustatyto Europos Parlamento ir Tarybos reglamente (ES, Euratomas) 2018/1046 (toliau – Finansinis reglamentas)[12]. Siekiant patikimo finansų valdymo ir atsižvelgiant į nenuspėjamą, išskirtinį ir specifinį kibernetinio saugumo aplinkos ir kibernetinių grėsmių pobūdį, Reagavimo į kibernetinio saugumo krizes mechanizmui turėtų būti suteiktas tam tikras biudžeto valdymo lankstumas, visų pirma leidžiant nepanaudotus įsipareigojimų ir mokėjimų asignavimus veiksmams, kuriais siekiama šiame reglamente nustatytų tikslų, automatiškai perkelti į kitus finansinius metus. Kadangi dėl šios naujos taisyklės kyla keblumų, susijusių su Finansiniu reglamentu, šis klausimas galėtų būti sprendžiamas šiuo metu vykstančiose derybose dėl Finansinio reglamento išdėstymo nauja redakcija.

• Subsidiarumo principas (neišimtinės kompetencijos atveju)

Dėl svarbaus tarpvalstybinio aspekto, būdingo kibernetinio saugumo grėsmėms, ir didėjančio rizikos rūšių ir incidentų, kurie daro tarpvalstybinį šalutinį poveikį sektoriams ir produktams,

---

[10] 2013 m. gruodžio 17 d. Europos Parlamento ir Tarybos sprendimas Nr. 1313/2013/ES dėl Sąjungos civilinės saugos mechanizmo (Tekstas svarbus EEE).

[11] 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/836, kuriuo iš dalies keičiamas Sprendimas Nr. 1313/2013/ES dėl Sąjungos civilinės saugos mechanizmo (Tekstas svarbus EEE).

[12] 2018 m. liepos 18 d. Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) 2018/1046 dėl Sąjungos bendrajam biudžetui taikomų finansinių taisyklių (OL L 193, 2018 7 30, p. 1).

skaičiaus valstybės narės vienos negali veiksmingai pasiekti dabartinės intervencinės priemonės tikslų, todėl joms reikia bendrų veiksmų ir solidarumo Sąjungos lygmeniu.

Kovos su kibernetinėmis grėsmėmis, kylančiomis dėl karo prieš Ukrainą, patirtis ir patirtis, įgyta Prancūzijos pirmininkavimo laikotarpiu surengus kibernetinio saugumo pratybas (EU CyCLES), parodė, kad siekiant solidarumo ES lygmeniu turėtų būti sukurti konkretūs savitarpio paramos mechanizmai, visų pirma bendradarbiavimo su privačiuoju sektoriumi. Atsižvelgiant į tai, 2022 m. gegužės 23 d. Tarybos išvadose dėl Europos Sąjungos kibernetinio saugumo būklės raidos Komisija raginama pateikti pasiūlymą dėl naujo Reagavimo į kibernetinio saugumo krizes fondo.

Sąjungos lygmens parama ir veiksmai, kuriais siekiama geriau aptikti kibernetinio saugumo grėsmes ir padidinti pasirengimo ir reagavimo pajėgumus, suteikia pridėtinės vertės, nes taip išvengiama Sąjungos ir valstybių narių pastangų dubliavimosi. Tai padėtų geriau panaudoti turimus išteklius ir geriau koordinuoti veiksmus bei keistis informacija apie įgytą patirtį. Reagavimo į kibernetinio saugumo krizes mechanizmu taip pat numatoma iš ES kibernetinio saugumo rezervo teikti paramą su Skaitmeninės Europos programa asocijuotoms trečiosioms valstybėms.

Parama, teikiama pagal įvairias iniciatyvas, kurios turi būti sukurtos ir finansuojamos Sąjungos lygmeniu, papildys nacionalinius pajėgumus, susijusius su kibernetinių grėsmių ir incidentų aptikimu, informuotumu apie padėtį, pasirengimu jiems ir reagavimu į juos, o ne dubliuosis.

- **Proporcingumas**

Veiksmais neviršijama to, kas būtina nustatytiems bendriesiems ir konkretiems reglamento tikslams pasiekti. Šiame reglamente numatyti veiksmai nedaro poveikio valstybių narių atsakomybei už nacionalinį saugumą, visuomenės saugumą, nusikalstamų veikų prevenciją, tyrimą bei atskleidimą ir patraukimą baudžiamojon atsakomybėn už jas. Jie taip pat nedaro poveikio subjektų, veikiančių ypatingos svarbos ir itin svarbiuose sektoriuose, teisinėms pareigoms priimti kibernetinio saugumo priemones pagal TIS 2 direktyvą.

Tokios pastangos ir priemonės papildomos į šį reglamentą įtrauktais veiksmais, remiant infrastruktūros, skirtos geriau aptikti ir analizuoti grėsmes, kūrimą ir teikiant paramą pasirengti ir reaguoti reikšmingų arba didelio masto incidentų atveju.

- **Priemonės pasirinkimas**

Pasiūlymas parengtas kaip Europos Parlamento ir Tarybos reglamentas. Tai tinkamiausia teisinė priemonė, nes tik reglamentu ir jo tiesiogiai taikomomis teisinėmis nuostatomis galima užtikrinti būtiną vienodumo laipsnį, reikalingą Europos kibernetinio saugumo skydo ir Reagavimo į kibernetinio saugumo krizes mechanizmui sukurti ir veikti, numatant paramą iš Skaitmeninės Europos programos jiems sukurti, taip pat aiškias šios paramos naudojimo ir skyrimo sąlygas.

3. *EX POST* VERTINIMO, KONSULTACIJŲ SU SUINTERESUOTOSIOMIS ŠALIMIS IR POVEIKIO VERTINIMO REZULTATAI

- **Konsultacijos su suinteresuotosiomis šalimis**

Šio reglamento veiksmai bus remiami pagal Skaitmeninės Europos programą ir dėl to buvo plačiai konsultuojamasi. Be to, jie bus grindžiami pirmaisiais veiksmais, parengtais glaudžiai bendradarbiaujant su pagrindiniais suinteresuotaisiais subjektais. Kalbant apie SOC, Komisija, glaudžiai bendradarbiaudama su valstybėmis narėmis Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centre (ECCC), parengė koncepcijos dokumentą dėl tarpvalstybinių SOC platformų plėtojimo ir kvietimą pareikšti susidomėjimą. Atsižvelgiant į tai, buvo atliktas nacionalinių SOC pajėgumų tyrimas ir ECCC techninėje darbo grupėje, kurioje susirenka valstybių narių atstovai, aptarti bendri metodai ir techniniai reikalavimai. Be to, pasikeista nuomonėmis su sektoriaus atstovais, visų pirma per ENISA ir Europos kibernetinio saugumo organizacijos (ECSO) sukurtą SOC ekspertų grupę.

Antra, parengties ir reagavimo į incidentus srityje Komisija parengė trumpojo laikotarpio paramos valstybėms narėms programą, skirdama papildomą finansavimą ENISA pagal Skaitmeninės Europos programą, kad būtų nedelsiant sustiprinta parengtis ir pajėgumai reaguoti į didelius kibernetinius incidentus. Valstybių narių ir sektoriaus atstovų atsiliepimai, gauti įgyvendinant šią trumpojo laikotarpio programą, jau suteikia vertingų įžvalgų, kuriomis pasinaudota rengiant siūlomą reglamentą, siekiant pašalinti nustatytus trūkumus. Tai buvo pirmas žingsnis pagal Tarybos išvadas dėl kibernetinio saugumo būklės, kuriose Komisijos prašoma pateikti pasiūlymą dėl naujo Reagavimo į kibernetinio saugumo krizes fondo.

Be to, 2023 m. vasario 16 d. remiantis diskusijoms skirtu dokumentu dėl Reagavimo į kibernetinio saugumo krizes mechanizmo surengtas praktinis seminaras su valstybių narių ekspertais. Tame seminare dalyvavo visos valstybės narės, o dar vienuolika valstybių narių pateikė pastabų raštu.

- **Poveikio vertinimas**

Kadangi pasiūlymas yra skubus, poveikio vertinimas nebuvo atliktas. Šiame reglamente numatyti veiksmai bus remiami pagal Skaitmeninės Europos programą ir atitinka Skaitmeninės Europos programos reglamente nustatytus veiksmus, dėl kurių buvo atliktas specialus poveikio vertinimas. Šiuo reglamentu nebus daroma jokio didelio administracinio ar aplinkosauginio poveikio, išskyrus tą, kuris jau įvertintas Skaitmeninės Europos programos reglamento poveikio vertinime.

Be to, jis grindžiamas pirmaisiais veiksmais, parengtais glaudžiai bendradarbiaujant su pagrindiniais suinteresuotaisiais subjektais, kaip išdėstyta pirmiau, ir atsižvelgiant į valstybių narių raginimą Komisijai iki 2022 m. III ketvirčio pabaigos pateikti pasiūlymą dėl naujo Reagavimo į kibernetinio saugumo krizes fondo.

Kalbant konkrečiai apie informuotumą apie padėtį ir aptikimą pagal Europos kibernetinio saugumo skydą, pagal 2021–2022 m. Skaitmeninės Europos programos kibernetinio saugumo darbo programą parengtas kvietimas pareikšti susidomėjimą bendrai pirkti priemones ir infrastruktūros objektus tarpvalstybiniams SOC steigti, ir kvietimas dėl dotacijų viešąsias ir privačiąsias organizacijas aptarnaujančių SOC pajėgumams stiprinti.

Kaip minėta pirmiau, parengties ir reagavimo į incidentus srityje Komisija parengė trumpojo laikotarpio programą, kuria siekiama Skaitmeninės Europos programos lėšomis remti valstybes nares ir kurią įgyvendina ENISA. Finansuojamos paslaugos apima pasirengimo veiksmus, pavyzdžiui, ypatingos svarbos subjektų skverbimosi testavimą, siekiant nustatyti pažeidžiamumus. Taip pat padidinamos galimybės padėti valstybėms narėms didelių incidentų, darančių poveikį ypatingos svarbos subjektams, atveju. ENISA įgyvendina šią trumpojo laikotarpio programą ir jau pateikė svarbių įžvalgų, į kurias buvo atsižvelgta rengiant šį reglamentą.

- **Pagrindinės teisės**

Padėdamas didinti skaitmeninės informacijos saugumą, šis pasiūlymas padės apsaugoti teisę į laisvę ir saugumą pagal ES pagrindinių teisių chartijos 6 straipsnį ir teisę į privatų ir šeimos gyvenimą pagal ES pagrindinių teisių chartijos 7 straipsnį. Pasiūlymu siekiama apsaugoti įmones nuo ekonomiškai žalingų kibernetinių išpuolių, tad juo taip pat bus prisidedama prie laisvės užsiimti verslu pagal ES pagrindinių teisių chartijos 16 straipsnį ir teisės į nuosavybę pagal ES pagrindinių teisių chartijos 17 straipsnį. Galiausiai, saugant ypatingos svarbos infrastruktūros objektų vientisumą įvykus kibernetiniams išpuoliams, pasiūlymu bus prisidedama prie teisės į sveikatos priežiūrą pagal ES pagrindinių teisių chartijos 35 straipsnį ir teisės naudotis bendrus ekonominius interesus tenkinančiomis paslaugomis pagal ES pagrindinių teisių chartijos 36 straipsnį.

4. POVEIKIS BIUDŽETUI

Šiame reglamente numatyti veiksmai bus remiami finansavimu pagal Skaitmeninės Europos programos strateginį tikslą „Kibernetinis saugumas“.

Numatytas bendro biudžeto padidinimas 100 mln. EUR; šią sumą šiame reglamente siūloma perskirstyti iš kitų Skaitmeninės Europos programos strateginių tikslų. Tai leis naują bendrą sumą, skirtą kibernetinio saugumo veiksmams pagal Skaitmeninės Europos programą, padidinti iki 842,8 mln. EUR.

Dalimi papildomos 100 mln. EUR sumos bus sustiprintas ECCC valdomas biudžetas, skirtas įgyvendinti veiksmams, susijusiems su SOC ir parengtimi, pagal jų darbo programą (-as). Be to, papildomu finansavimu bus remiamas ES kibernetinio saugumo rezervo sukūrimas.

Juo nuo 2023–2027 m. laikotarpio papildomas jau numatytas biudžetas, skirtas panašiems veiksmams pagal pagrindinę Skaitmeninės Europos programą ir Skaitmeninės Europos

programos kibernetinio saugumo darbo programą, taigi bendra suma 2023–2027 m. galėtų sudaryti 551 mln. EUR, o 115 mln. EUR jau buvo skirta 2021–2022 m. vykdant bandomuosius projektus. Įskaitant valstybių narių įnašus, bendras biudžetas galėtų sudaryti iki 1,109 mlrd. EUR.

Susijusių išlaidų apžvalga pateikta su šiuo pasiūlymu teikiamoje finansinėje teisės akto pažymoje.

5. KITI ELEMENTAI

- **Įgyvendinimo planai ir stebėsena, vertinimas ir ataskaitų teikimo tvarka**

Komisija stebės naujų nuostatų įgyvendinimą, taikymą ir atitiktį joms, kad galėtų įvertinti jų efektyvumą. Komisija ne vėliau kaip praėjus ketveriems metams nuo šio reglamento taikymo pradžios Europos Parlamentui ir Tarybai pateiks jo vertinimo ir peržiūros ataskaitą.

- **Išsamus konkrečių pasiūlymo nuostatų paaiškinimas**

Bendrieji tikslai, dalykas ir apibrėžtys (I skyrius)

I skyriuje nustatyti reglamento tikslai stiprinti Sąjungos lygmens solidarumą, siekiant geriau aptikti kibernetinio saugumo grėsmes ir incidentus, jiems pasirengti ir į juos reaguoti, visų pirma stiprinti bendrą Sąjungos kibernetinių grėsmių ir incidentų aptikimą ir informuotumą apie padėtį, subjektų, veikiančių ypatingos svarbos ir itin svarbiuose sektoriuose visoje Sąjungoje, parengtį ir solidarumą plėtojant bendrus reagavimo į reikšmingus arba didelio masto kibernetinio saugumo incidentus pajėgumus ir didinti Sąjungos atsparumą peržiūrint ir vertinant reikšmingus arba didelio masto incidentus. Šiame skyriuje taip pat nustatomi veiksmai, kuriais bus siekiama šių tikslų: sukurti Europos kibernetinio saugumo skydą, Reagavimo į kibernetinio saugumo krizes mechanizmą ir Kibernetinio saugumo incidentų peržiūros mechanizmą. Jame pateikiamos ir visame dokumente vartojamų terminų apibrėžtys.

Europos kibernetinio saugumo skydas (II skyrius)

II skyriuje nustatomas Europos kibernetinio saugumo skydas ir apibūdinami įvairūs jo elementai bei dalyvavimo jame sąlygos. Pirma, jame pristatomas bendras Europos kibernetinio saugumo skydo tikslas – plėtoti Sąjungos pažangius pajėgumus aptikti, analizuoti ir tvarkyti duomenis apie kibernetines grėsmes ir incidentus Sąjungoje, taip pat konkretūs veiklos tikslai. Jame nurodyta, kad Sąjungos skiriamas Europos kibernetinio saugumo skydo finansavimas teikiamas pagal Skaitmeninės Europos programos reglamentą.

Be to, šiame skyriuje aprašoma subjektų, kurie sudarys Europos kibernetinio saugumo skydą, rūšis. Skydą sudaro nacionaliniai saugumo operacijų centrai (toliau – nacionaliniai SOC) ir tarpvalstybiniai saugumo operacijų centrai (toliau – tarpvalstybiniai SOC). Kiekviena dalyvaujanti valstybė narė paskiria nacionalinį SOC. Tai bus atskaitos taškas, nuo kurio kitoms viešosioms ir privačioms organizacijoms nacionaliniu lygmeniu atsivers galimybė rinkti ir analizuoti informaciją apie kibernetinio saugumo grėsmes bei incidentus ir prisidėti

prie tarpvalstybinio SOC veiklos. Paskelbus kvietimą pareikšti susidomėjimą, ECCC gali atrinkti nacionalinį SOC, kuris dalyvaus bendrame priemonių ir infrastruktūros objektų viešajame pirkime su ECCC ir gaus dotaciją toms priemonėms ir infrastruktūros objektams valdyti. Jei nacionalinis SOC gauna Sąjungos paramą, jis įsipareigoja per dvejus metus pateikti paraišką dalyvauti tarpvalstybinio SOC veikloje.

Tarpvalstybinius SOC sudaro ne mažiau kaip trijų valstybių narių konsorciumas, kuriam atstovauja nacionaliniai SOC, įsipareigoję bendradarbiauti koordinuodami savo kibernetinių grėsmių aptikimo ir stebėsenos veiklą. Po pirminio kvietimo pareikšti susidomėjimą ECCC gali atrinkti prieglobos konsorciumą, kuris dalyvaus kartu su ECCC vykdomame bendrame priemonių ir infrastruktūros objektų viešajame pirkime ir gaus dotaciją toms priemonėms ir infrastruktūros objektams valdyti. Prieglobos konsorciumo nariai sudaro rašytinį konsorciumo susitarimą, kuriame nustatoma jų vidaus tvarka. Po to šiame skyriuje išsamiai aprašomi tarpvalstybinio SOC dalyvių dalijimosi informacija ir tarpvalstybinio SOC ir kitų tarpvalstybinių SOC, taip pat atitinkamų ES subjektų dalijimosi informacija reikalavimai. Tarpvalstybinio SOC veikloje dalyvaujantys nacionaliniai SOC tarpusavyje dalijasi svarbia su kibernetinėmis grėsmėmis susijusia informacija, o išsami informacija, įskaitant įsipareigojimą dalytis dideliu duomenų kiekiu ir jų teikimo sąlygas, turėtų būti nustatyta konsorciumo susitarime. Tarpvalstybiniai SOC užtikrina aukšto lygio tarpusavio sąveikumą. Be to, tarpvalstybiniai SOC su kitais tarpvalstybiniais SOC turėtų sudaryti bendradarbiavimo susitarimus, kuriuose būtų nustatyti dalijimosi informacija principai. Kai tarpvalstybiniai SOC gauna informacijos, susijusios su galimu arba vykstančiu didelio masto kibernetinio saugumo incidentu, jie pateikia atitinkamą informaciją EU-CyCLONe, CSIRT tinklui ir Komisijai, atsižvelgdami į jų atitinkamas krizių valdymo funkcijas pagal Direktyvą (ES) 2022/2555. II skyriaus pabaigoje išdėstytos dalyvavimo Europos kibernetinio saugumo skydo veikloje saugumo sąlygos.

Reagavimo į kibernetinio saugumo krizes mechanizmas (III skyrius)

III skyriuje nustatomas Reagavimo į kibernetinio saugumo krizes mechanizmas, kuriuo siekiama didinti Sąjungos atsparumą didelėms kibernetinio saugumo grėsmėms ir solidariai pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams ar krizėms ir sušvelninti jų poveikį trumpuoju laikotarpiu. Reagavimo į kibernetinio saugumo krizes mechanizmo įgyvendinimo veiksmai remiami Skaitmeninės Europos programos lėšomis. Mechanizme numatyti veiksmai, kuriais remiama parengtis, įskaitant itin svarbiuose sektoriuose veikiančių subjektų koordinuotą testavimą, reagavimą į reikšmingus arba didelio masto kibernetinio saugumo incidentus ir nedelsiamą veiklos atkūrimą arba didelių kibernetinių grėsmių švelninimą ir savitarpio pagalbos veiksmus.

Reagavimo į kibernetinio saugumo krizes mechanizmo pasirengimo veiksmai apima itin svarbiuose sektoriuose veikiančių subjektų koordinuotą parengties testavimą. Komisija, pasikonsultavusi su ENISA ir TIS bendradarbiavimo grupe, turėtų reguliariai nustatyti atitinkamus sektorius ar subsektorius iš Direktyvos (ES) 2022/2555 I priede išvardytų ypatingos svarbos sektorių, kurių subjektams gali būti taikomas ES lygmeniu koordinuojamas parengties testavimas.

Siekiant įgyvendinti siūlomus reagavimo į incidentus veiksmus, šiuo reglamentu sukuriamas ES kibernetinio saugumo rezervas, kurį sudaro reagavimo į incidentus paslaugos, kurias teikia patikimi paslaugų teikėjai, atrinkti pagal šiame reglamente nustatytus kriterijus. ES kibernetinio saugumo rezervo paslaugų naudotojai yra valstybių narių kibernetinio saugumo krizių valdymo institucijos bei CSIRT ir Sąjungos institucijos, įstaigos ir agentūros. Komisijai tenka visa atsakomybė už ES kibernetinio saugumo rezervo įgyvendinimą ir ji gali pavesti ENISA visiškai arba iš dalies valdyti ir administruoti ES kibernetinio saugumo rezervą.

Kad gautų paramą iš ES kibernetinio saugumo rezervo, naudotojai patys turėtų imtis priemonių incidento, dėl kurio prašoma paramos, poveikiui sušvelninti. ES kibernetinio saugumo rezervo paramos prašymuose turėtų būti pateikta būtina svarbi informacija apie incidentą ir priemones, kurių naudotojai jau ėmėsi. Šiame skyriuje taip pat aprašomos įgyvendinimo sąlygos, įskaitant prašymų ES kibernetinio saugumo rezervui vertinimą.

Reglamente taip pat nustatyti viešųjų pirkimų principai ir atrankos kriterijai, susiję su patikimais ES kibernetinio saugumo rezervo paslaugų teikėjais.

Trečiosios valstybės gali prašyti ES kibernetinio saugumo rezervo paramos, jei tai numatyta sudarytuose asociacijos susitarimuose dėl jų dalyvavimo Skaitmeninės Europos programoje. Šiame skyriuje aprašomos papildomos tokio dalyvavimo sąlygos, tvarka ir būdai.

Kibernetinio saugumo incidentų peržiūros mechanizmas (IV skyrius)

Komisijos, EU-CyCLONe arba CSIRT tinklo prašymu ENISA turėtų peržiūrėti ir įvertinti grėsmes, pažeidžiamumus ir poveikio švelninimo veiksmus, susijusius su konkrečiu reikšmingu arba didelio masto kibernetinio saugumo incidentu. ENISA incidentų peržiūros ir vertinimo ataskaitą turėtų pateikti CSIRT tinklui, EU-CyCLONe ir Komisijai, kad padėtų jiems atlikti savo užduotis. Kai incidentas susijęs su trečiąja valstybe, Komisija turėtų pasidalyti ataskaita su vyriausiuoju įgaliotiniu. Ataskaitoje turėtų būti aprašyta įgyta patirtis ir, kai tinkama, rekomendacijos, kaip pagerinti Sąjungos kibernetinio saugumo būklę.

Baigiamosios nuostatos (V skyrius)

V skyriuje pateikiami Skaitmeninės Europos programos reglamento pakeitimai ir nustatoma Komisijos pareiga rengti reguliarias reglamento vertinimo ir peržiūros ataskaitas Europos Parlamentui ir Tarybai. Pagal 21 straipsnyje nurodytą nagrinėjimo procedūrą Komisija įgaliojama priimti įgyvendinimo aktus, kuriais siekiama: nustatyti tokio tarpvalstybinių SOC sąveikumo sąlygas, nustatyti tarpvalstybinių SOC ir Sąjungos subjektų dalijimosi informacija, susijusia su galimu arba vykstančiu didelio masto kibernetinio saugumo incidentu, procedūrinę tvarką, nustatyti techninius reikalavimus, kuriais siekiama užtikrinti aukštą infrastruktūros duomenų ir fizinio saugumo lygį ir apsaugoti Sąjungos saugumo interesus, kai informacija dalijamasi su subjektais, kurie nėra valstybės narės viešosios įstaigos, nurodyti reagavimo paslaugų, kurių reikia ES kibernetinio saugumo rezervui, rūšis ir skaičių ir išsamiau nustatyti ES kibernetinio saugumo rezervo paramos paslaugų skyrimo tvarką.

2023/0109 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės

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,

kadangi:

(1) informacinių ir ryšių technologijų naudojimas ir priklausomumas nuo jų tapo esminiais visų ekonominės veiklos sektorių aspektais, nes mūsų viešojo administravimo institucijos, įmonės ir piliečiai įvairiuose sektoriuose ir įvairiose valstybėse labiau susieti tarpusavyje ir vieni nuo kitų priklausomi, nei bet kada anksčiau;

(2) kibernetinio saugumo incidentų, įskaitant tiekimo grandinės išpuolius, kurių tikslas – kibernetinis šnipinėjimas, išpirkos reikalavimo programinė įranga arba veiklos sutrikdymas, mastas, dažnumas ir poveikis didėja. Tai kelia didelę grėsmę tinklų ir informacinių sistemų veikimui. Turint omenyje sparčiai kintančias grėsmių aplinkybes, dėl galimų didelio masto incidentų, dėl kurių gali kilti didelių sutrikimų ar būti padaryta žala ypatingos svarbos infrastruktūros objektams, grėsmės reikia didinti parengtį visais Sąjungos kibernetinio saugumo sistemos lygmenimis. Ši grėsmė yra susijusi ne vien su Rusijos karine agresija prieš Ukrainą ir, tikėtina, išliks, atsižvelgiant į tai, kad dabartinę geopolitinę įtampą lemia daugybė su valstybe susijusių subjektų, nusikaltėlių ir įsilaužėlių aktyvistų. Tokie incidentai gali trukdyti teikti viešąsias paslaugas ir vykdyti ekonominę veiklą, be kita ko, ypatingos svarbos ar itin svarbiuose sektoriuose, sukelti didelių finansinių nuostolių, pakenkti naudotojų pasitikėjimui, padaryti didelės žalos Sąjungos ekonomikai ir jų padariniai gali būti pavojingi net žmonių sveikatai ar gyvybei. Be to, kibernetinio saugumo incidentai yra nenuspėjami, nes dažnai kyla ir išsiplėtoja per labai trumpą laiką, nėra susiję su jokia

[1] OL C […], […], p. […].
[2] OL C , , p. .
[3] OL C , , p. .

konkrečia geografine teritorija ir vyksta vienu metu arba akimirksniu išplinta daugelyje šalių;

(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[4], būtina didinti piliečių, įmonių ir subjektų, valdančių ypatingos svarbos infrastruktūros objektus, atsparumą didėjančioms kibernetinio saugumo grėsmėms, kurios gali turėti pražūtingą poveikį visuomenei ir ekonomikai. Todėl reikia investuoti į infrastruktūrą ir paslaugas, kurios padėtų greičiau aptikti kibernetinio saugumo grėsmes bei incidentus ir į juos reaguoti, o valstybėms narėms reikia pagalbos geriau pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams ir į juos reaguoti. Sąjunga taip pat turėtų didinti savo pajėgumus šiose srityse, visų pirma susijusius su duomenų apie kibernetinio saugumo 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 direktyvą (ES) 2022/2555[5], Komisijos rekomendaciją (ES) 2017/1584[6], Europos Parlamento ir Tarybos direktyvą 2013/40/ES[7] ir Europos Parlamento ir Tarybos reglamentą (ES) 2019/881[8]. Be to, Tarybos rekomendacijoje dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą valstybės narės raginamos imtis skubių ir veiksmingų priemonių ir lojaliai, 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 kibernetiniai 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 kibernetinio saugumo grėsmes ir incidentus, jiems pasirengti ir į juos reaguoti. Valstybės narės Tarybos išvadose dėl ES kibernetinio saugumo būklės[9] taip pat paragino Komisiją pateikti pasiūlymą dėl naujo Reagavimo į kibernetinio saugumo krizes fondo;

---

4 https://futureu.europa.eu/lt

5 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 (OL L 333, 2022 12 27).

6 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).

7 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).

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

9 Tarybos išvados dėl Europos Sąjungos kibernetinio saugumo būklės raidos, kurias Taryba patvirtino 2022 m. gegužės 23 d. posėdyje (dok. 9364/22).

(6) 2022 m. lapkričio 10 d. priimtame bendrame komunikate dėl ES kibernetinės gynybos politikos[10] 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 kibernetinio saugumo rezervo kūrimą, pasitelkiant patikimų privačių paslaugų teikėjų paslaugas ir, remiantis ES rizikos vertinimais, atlikti ypatingos svarbos subjektų galimų pažeidžiamumų testavimą;

(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 reaguoti į reikšmingus ir didelio masto kibernetinio saugumo incidentus. Taigi turėtų būti įdiegta Europos masto SOC infrastruktūra (Europos kibernetinio saugumo skydas) siekiant sukurti ir sustiprinti bendrus aptikimo ir informuotumo apie padėtį gebėjimus, reikėtų sukurti Reagavimo į kibernetinio saugumo krizes mechanizmą siekiant padėti valstybėms narėms pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams, į juos reaguoti ir nedelsiant po jų atkurti veiklą, turėtų būti sukurtas Kibernetinio saugumo incidentų peržiūros mechanizmas, kad būtų galima peržiūrėti ir įvertinti konkrečius reikšmingus arba didelio masto incidentus. Šie veiksmai nedaro poveikio Sutarties dėl Europos Sąjungos veikimo (toliau – SESV) 107 ir 108 straipsniams;

(8) siekiant šių tikslų taip pat būtina tam tikrose srityse iš dalies pakeisti Europos Parlamento ir Tarybos reglamentą (ES) 2021/694[11]. Visų pirma šiuo reglamentu turėtų būti iš dalies pakeistas Reglamentas (ES) 2021/694, siekiant įtraukti naujus veiklos tikslus, susijusius su Europos kibernetinio saugumo skydu ir Reagavimo į kibernetinio saugumo krizes mechanizmu pagal Skaitmeninės Europos programos 3-ią konkretų tikslą, kuriuo siekiama užtikrinti bendrosios skaitmeninės rinkos atsparumą, vientisumą ir patikimumą, stiprinti kibernetinių išpuolių ir grėsmių stebėsenos bei reagavimo į juos pajėgumus ir stiprinti tarpvalstybinį bendradarbiavimą kibernetinio saugumo srityje. Be to, turėtų būti nustatytos specialios sąlygos, kuriomis šiems veiksmams gali būti skiriama finansinė parama, ir apibrėžti valdymo bei koordinavimo mechanizmai, būtini numatytiems tikslams pasiekti. Kiti Reglamento (ES) 2021/694 pakeitimai turėtų apimti siūlomų veiksmų pagal naujus veiklos tikslus aprašymus, taip pat išmatuojamus šių naujų veiklos tikslų įgyvendinimo stebėsenos rodiklius;

(9) veiksmų finansavimas pagal šį reglamentą turėtų būti numatytas Reglamente (ES) 2021/694, kuris turėtų ir toliau būti svarbus pagrindinis teisės aktas dėl šių veiksmų, įtvirtintų Skaitmeninės Europos programos 3-iame konkrečiame tiksle. Konkrečios dalyvavimo sąlygos, susijusios su kiekvienu veiksmu, bus numatytos atitinkamose darbo programose, laikantis taikytinos Reglamento (ES) 2021/694 nuostatos;

(10) šiam reglamentui taikomos Europos Parlamento ir Tarybos pagal SESV 322 straipsnį priimtos horizontaliosios finansinės taisyklės. Tos taisyklės išdėstytos Finansiniame reglamente – 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 bendrąją Sąjungos biudžeto

[10] Bendras komunikatas Europos Parlamentui ir Tarybai „ES kibernetinės gynybos politika“, JOIN(2022) 49 *final*.

[11] 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).

apsaugos sąlygų sistemą, kaip nustatyta Europos Parlamento ir Tarybos reglamentu (ES, Euratomas) 2020/2092;

(11) siekiant patikimo finansų valdymo, reikėtų nustatyti konkrečias taisykles dėl nepanaudotų įsipareigojimų ir mokėjimų asignavimų perkėlimo. Laikantis principo, kad Sąjungos biudžetas nustatomas kasmet, šiame reglamente, atsižvelgiant į nenuspėjamą, išskirtinį ir specifinį kibernetinio saugumo aplinkos pobūdį, turėtų būti numatyta galimybė nepanaudotas lėšas, be nustatytųjų Finansiniame reglamente, perkelti į kitą laikotarpį, taip kuo labiau padidinant Reagavimo į kibernetinio saugumo krizes mechanizmo pajėgumą padėti valstybėms narėms veiksmingai kovoti su kibernetinėmis grėsmėmis;

(12) siekiant veiksmingiau užkirsti kelią kibernetinėms grėsmėms ir incidentams, juos įvertinti ir į juos reaguoti, būtina kaupti daugiau žinių apie Sąjungos teritorijoje esančiam ypatingos svarbos turtui ir infrastruktūros objektams kylančias grėsmes, įskaitant jų geografinį pasiskirstymą, sąsajas ir galimą poveikį tuos infrastruktūros objektus veikiančių kibernetinių išpuolių atveju. Turėtų būti įdiegta didelio masto Sąjungos SOC infrastruktūra (toliau – Europos kibernetinio saugumo skydas), kurią sudarytų kelios sąveikios tarpvalstybinės platformos, jungiančios po kelis nacionalinius SOC. Ta infrastruktūra turėtų būti naudinga nacionaliniams ir Sąjungos kibernetinio saugumo interesams ir poreikiams, naudojant naujausias pažangių duomenų rinkimo ir analizės priemonių technologijas, stiprinant kibernetinio saugumo grėsmių aptikimo ir valdymo pajėgumus ir užtikrinant informuotumą apie padėtį tikruoju laiku. Ta infrastruktūra turėtų padėti geriau aptikti kibernetinio saugumo grėsmes ir incidentus ir taip papildyti ir remti Sąjungos subjektus ir tinklus, atsakingus už krizių valdymą Sąjungoje, visų pirma ES ryšių palaikymo dėl kibernetinių krizių organizacinį tinklą (EU-CyCLONe), kaip apibrėžta Europos Parlamento ir Tarybos direktyvoje (ES) 2022/2555[12];

(13) kiekviena valstybė narė nacionaliniu lygmeniu turėtų paskirti viešąją įstaigą, kuriai būtų pavesta koordinuoti kibernetinių grėsmių aptikimo veiklą toje valstybėje narėje. Šie nacionaliniai SOC turėtų veikti kaip nacionalinis atskaitos taškas, nuo kurio nacionaliniu lygmeniu atsiveria galimybė dalyvauti Europos kibernetinio saugumo skydo 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;

(14) kaip Europos kibernetinio saugumo skydo dalis, turėtų būti įsteigti keli tarpvalstybiniai kibernetinio saugumo operacijų centrai (toliau – tarpvalstybiniai SOC). Jie turėtų suburti nacionalinius SOC iš bent trijų valstybių narių, kad būtų galima visapusiškai pasinaudoti tarpvalstybinio grėsmių aptikimo, dalijimosi informacija ir valdymo privalumais. Bendras tarpvalstybinių SOC tikslas turėtų būti stiprinti gebėjimus analizuoti kibernetinio saugumo grėsmes, užkirsti joms kelią bei jas aptikti ir remti kokybiškų žvalgybos duomenų apie kibernetinio saugumo grėsmes rengimą, visų pirma dalijantis duomenimis iš įvairių viešųjų ar privačių šaltinių, dalijantis naujausiomis priemonėmis ir jas bendrai naudojant, taip pat bendrai plėtojant aptikimo, analizės ir prevencijos pajėgumus patikimoje aplinkoje. Jie turėtų suteikti

[12] 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).

naujų papildomų pajėgumų, kurie remsis esamų SOC ir reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) bei kitų atitinkamų subjektų veikla ir ją papildys;

(15) nacionaliniu lygmeniu kibernetinių grėsmių stebėseną, aptikimą ir analizę paprastai užtikrina viešųjų ir privačių subjektų SOC kartu su CSIRT. Be to, CSIRT keičiasi informacija CSIRT tinkle pagal Direktyvą (ES) 2022/2555. Tarpvalstybiniai SOC turėtų sukurti naujus pajėgumus, kurie papildytų CSIRT tinklą, kaupiant viešųjų ir privačių subjektų duomenis apie grėsmes kibernetiniam saugumui bei jais dalijantis, didinant tokių duomenų vertę atliekant ekspertų analizę bei kartu įsigyjant infrastruktūros objektus ir taikant pažangiausias priemones, taip pat prisidedant prie Sąjungos pajėgumų ir technologinio suverenumo plėtojimo;

(16) tarpvalstybiniai SOC turėtų veikti kaip centrinis punktas, leidžiantis sutelkti daug svarbių duomenų ir kibernetinių grėsmių žvalgybos informaciją, sudaryti sąlygas skleisti informaciją apie grėsmes dideliam įvairių dalyvių ratui (pvz., kompiuterinių incidentų tyrimo tarnyboms (toliau – CERT), CSIRT, keitimosi informacija ir jos analizės centrams (toliau – ISAC), ypatingos svarbos infrastruktūros objektų operatoriams). Informacija, kuria keičiasi tarpvalstybinio SOC dalyviai, galėtų apimti tinklų ir jutiklių duomenis, grėsmių žvalgybos informacijos santraukas, užvaldymo rodiklius ir kontekstinę informaciją apie incidentus, grėsmes ir pažeidžiamumus. Be to, tarpvalstybiniai SOC taip pat turėtų sudaryti bendradarbiavimo susitarimus su kitais tarpvalstybiniais SOC;

(17) atitinkamų institucijų bendras informuotumas apie padėtį yra būtina Sąjungos masto parengties reikšmingiems ir didelio masto kibernetinio saugumo incidentams ir koordinavimo veiksmų 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, įstaigų ir agentūrų, Direktyva (ES) 2022/2555 įsteigiamas EU-CyCLONe. Rekomendacijoje (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes apibūdinamas visų susijusių subjektų vaidmuo. Be to, Direktyvoje (ES) 2022/2555 primenama Komisijos atsakomybė pagal Sąjungos civilinės saugos mechanizmą (toliau – SCSM), nustatytą Europos Parlamento ir Tarybos sprendimu Nr. 1313/2013/ES, taip pat už analitinių ataskaitų dėl integruoto politinio atsako į krizes mechanizmo (toliau – IPCR) teikimą pagal Įgyvendinimo sprendimą (ES) 2018/1993. Todėl tais atvejais, kai tarpvalstybiniai SOC gauna informacijos, susijusios su galimu arba vykstančiu didelio masto kibernetinio saugumo incidentu, jie turėtų teikti atitinkamą informaciją EU-CyCLONe, CSIRT tinklui ir Komisijai. 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. Šiomis aplinkybėmis reikėtų deramai atsižvelgti į būtinybės žinoti principą ir į galimai neskelbtiną informacijos, kuria dalijamasi, pobūdį;

(18) Europos kibernetinio saugumo skydo veikloje dalyvaujantys subjektai turėtų užtikrinti aukšto lygio tarpusavio sąveikumą, be kita ko, kai tinkama, duomenų formatų, taksonomijos, duomenų tvarkymo ir duomenų analizės priemonių, taip pat saugių ryšio kanalų, minimalaus taikomųjų programų saugumo lygio, informuotumo apie padėtį suvestinės ir rodiklių atžvilgiu. Priimant bendrą taksonomiją ir parengiant padėties ataskaitų šabloną kibernetinio saugumo incidentų techninėms priežastims ir

poveikiui apibūdinti turėtų būti atsižvelgiama į šiuo metu vykdomą pranešimo apie incidentus darbą įgyvendinant Direktyvą (ES) 2022/2555;

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

(20) renkant duomenis, jais dalijantis bei keičiantis, Europos kibernetinio saugumo skydas turėtų stiprinti Sąjungos technologinį suverenumą. Kokybiškų patikrintų duomenų sutelkimas taip pat turėtų padėti plėtoti pažangias dirbtinio intelekto ir duomenų analizės technologijas. Tai turėtų būti lengviau padaryti sujungiant Europos kibernetinio saugumo skydą su visos Europos našiosios kompiuterijos infrastruktūra, sukurta Tarybos reglamentu (ES) 2021/1173[13];

(21) nors Europos kibernetinio saugumo skydas yra civilinis projektas, kibernetinės gynybos bendruomenei galėtų būti naudingi stipresni civiliniai aptikimo ir informuotumo apie padėtį pajėgumai, sukurti ypatingos svarbos infrastruktūrai apsaugoti. Tarpvalstybiniai SOC, padedami Komisijos ir Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro (toliau – ECCC) bei bendradarbiaudami su Sąjungos vyriausiuoju įgaliotiniu užsienio reikalams ir saugumo politikai (toliau – vyriausiasis įgaliotinis), turėtų palaipsniui parengti specialius protokolus ir standartus, kad būtų galima bendradarbiauti su kibernetinės gynybos bendruomene, įskaitant tikrinimo ir saugumo sąlygas. Kuriant Europos kibernetinio saugumo skydą turėtų būti svarstoma galimybė ateityje, glaudžiai bendradarbiaujant su vyriausiuoju įgaliotiniu, bendradarbiauti su tinklais ir platformomis, atsakingais už dalijimąsi informacija kibernetinės gynybos bendruomenėje;

(22) Europos kibernetinio saugumo skydo dalyviai turėtų dalytis informacija laikydamiesi galiojančių teisinių reikalavimų, visų pirma Sąjungos ir nacionalinės duomenų apsaugos teisės, taip pat Sąjungos konkurencijos taisyklių, 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 teikiančią įstaigą, kad duomenys sunaikinti;

(23) nedarant poveikio SESV 346 straipsniui, keitimasis konfidencialia informacija pagal Sąjungos arba nacionalines taisykles turėtų apsiriboti tik tuo, kas yra svarbu ir proporcinga to keitimosi tikslais. Keičiantis tokia informacija turėtų būti saugomas informacijos konfidencialumas ir atitinkamų subjektų saugumo bei komerciniai interesai, visapusiškai saugant komercines ir verslo paslaptis;

(24) atsižvelgiant į didėjančią riziką ir poveikį valstybėms narėms darančių kibernetinių incidentų skaičių, būtina nustatyti paramos krizės atveju priemonę, kuria būtų didinamas Sąjungos atsparumas reikšmingiems ir didelio masto kibernetinio saugumo

[13] 2021 m. liepos 13 d. Tarybos reglamentas (ES) 2021/1173 dėl Europos našiosios kompiuterijos bendrosios įmonės įsteigimo ir kuriuo panaikinamas Reglamentas (ES) 2018/1488 (OL L 256, 2021 7 19, p. 3).

incidentams ir papildomi valstybių narių veiksmai teikiant skubią pasirengimo, reagavimo ir neatidėliojamo esminių paslaugų atkūrimo finansinę paramą. Ta priemonė turėtų sudaryti sąlygas greitai 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 (toliau – ES sutartis) 3 straipsnio 3 dalį, tačiau pirminė atsakomybė už kibernetinio saugumo incidentų ir krizių prevenciją, pasirengimą jiems ir reagavimą į juos pirmiausia tenka valstybėms narėms;

(25) Reagavimo į kibernetinio saugumo krizes mechanizmas turėtų padėti valstybėms narėms papildyti jų pačių priemones bei išteklius ir kitas esamas paramos reaguoti į reikšmingus ir didelio masto kibernetinio saugumo incidentus ir nedelsiant po jų atkurti veiklą galimybes, pavyzdžiui, Europos Sąjungos kibernetinio saugumo agentūros (toliau – 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, PESCO greitojo reagavimo į kibernetinius incidentus komandas[14] ir greitojo reagavimo į hibridines grėsmes grupes. Juo turėtų būti atsižvelgiama į poreikį užtikrinti, kad būtų specialių priemonių, kuriomis būtų remiamas pasirengimas kibernetinio saugumo incidentams ir reagavimas į juos visoje Sąjungoje ir trečiosiose valstybėse;

(26) šia priemone nedaroma poveikio Sąjungos lygmens reagavimo į krizes koordinavimo procedūroms ir sistemoms, visų pirma SCSM[15], IPCR[16],, ir Direktyvai (ES) 2022/2555. Ji gali padėti įgyvendinti veiksmus, įgyvendinamus pagal ES sutarties 42 straipsnio 7 dalį arba SESV 222 straipsnyje apibrėžtais atvejais, arba juos papildyti. Be to, šios priemonės naudojimas, kai tinkama, turėtų būti koordinuojamas su kibernetinio saugumo diplomatijos priemonių rinkinio priemonių įgyvendinimu;

(27) pagal šį reglamentą teikiama pagalba turėtų būti remiami ir papildomi veiksmai, kurių valstybės narės imasi nacionaliniu lygmeniu. Šiuo tikslu turėtų būti užtikrintas glaudus Komisijos ir paveiktos valstybės narės bendradarbiavimas ir konsultacijos. Prašydama paramos pagal reagavimo į kibernetinio saugumo krizes mechanizmą, valstybė narė turėtų pateikti atitinkamą informaciją, pagrindžiančią paramos poreikį;

(28) 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 ir galėtų 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 subjektų rūšis, patenkančius į tos

---

14 2017 m. gruodžio 11 d. TARYBOS SPRENDIMAS (BUSP) 2017/2315, kuriuo nustatomas nuolatinis struktūrizuotas bendradarbiavimas (PESCO) ir nustatomas dalyvaujančių valstybių narių sąrašas.

15 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).

16 Integruotas politinio atsako į krizes mechanizmas (IPCR) pagal 2017 m. rugsėjo 13 d. Komisijos rekomendaciją (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes.

direktyvos taikymo sritį, ir užtikrintų, kad jos turėtų tinkamų išteklių savo užduotims veiksmingai vykdyti. Šiuo reglamentu nedaroma poveikio 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 sušvelninti reikšmingų ir didelio masto kibernetinio saugumo incidentų poveikį, remti nedelsiamą veiklos ir (arba) esminių paslaugų veikimo atkūrimą;

(29) vykdant pasirengimo veiksmus, siekiant skatinti nuoseklų požiūrį ir stiprinti saugumą visoje Sąjungoje ir jos vidaus rinkoje, turėtų būti teikiama parama Direktyvoje (ES) 2022/2555 nustatytuose itin svarbiuose sektoriuose veikiančių subjektų kibernetinio saugumo koordinuotam testavimui ir vertinimui. Šiuo tikslu Komisija, padedama ENISA ir bendradarbiaudama su Direktyva (ES) 2022/2555 įsteigta TIS bendradarbiavimo grupe, turėtų reguliariai nustatyti, kurie atitinkami sektoriai ar subsektoriai turėtų būti tinkami gauti finansinę paramą koordinuotam Sąjungos lygmens testavimui. Sektoriai arba subsektoriai turėtų būti atrinkti iš Direktyvos (ES) 2022/2555 I priedo („Ypatingos svarbos sektoriai“). Koordinuotas 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 Tarybos išvadose dėl Europos Sąjungos kibernetinio saugumo būklės raidos Komisija, vyriausiasis įgaliotinis ir TIS bendradarbiavimo grupė raginami parengti, 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 (BEREC), koordinuotus 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[17]. Atrenkant sektorius taip pat reikėtų atsižvelgti į Tarybos rekomendaciją dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą;

(30) be to, pagal reagavimo į kibernetinio saugumo krizes mechanizmą turėtų būti teikiama parama kitiems pasirengimo veiksmams ir parama parengčiai kituose sektoriuose, kuriems netaikomas koordinuotas itin svarbiuose sektoriuose veikiančių subjektų testavimas. Tie veiksmai galėtų apimti įvairių rūšių nacionalinę pasirengimo veiklą;

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

---

[17] 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.

(32) Reagavimo į kibernetinio saugumo krizes mechanizmu turėtų būti remiama valstybių narių teikiama pagalba valstybei narei, nukentėjusiai nuo reikšmingo ar didelio masto kibernetinio saugumo incidento, be kita ko, teikiama per CSIRT tinklą, įsteigtą pagal Direktyvos (ES) 2022/2555 15 straipsnį. 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;

(33) turėtų būti palaipsniui sukurtas Sąjungos lygmens kibernetinio saugumo rezervas, kurį sudarytų privačių valdomų saugumo paslaugų teikėjų paslaugos, kuriomis būtų remiami reagavimo ir nedelsiamo veiklos atkūrimo veiksmai reikšmingų arba didelio masto kibernetinio saugumo incidentų atvejais. ES kibernetinio saugumo rezervas turėtų užtikrinti paslaugų prieinamumą ir parengtį. ES kibernetinio saugumo rezervo paslaugos turėtų padėti nacionalinėms institucijoms teikti pagalbą paveiktiems subjektams, veikiantiems ypatingos svarbos ar itin svarbiuose sektoriuose, papildant jų pačių veiksmus nacionaliniu lygmeniu. Prašydamos paramos iš ES kibernetinio saugumo rezervo, valstybės narės turėtų nurodyti, kokia parama atitinkamam subjektui teikiama nacionaliniu lygmeniu, ir į tai turėtų būti atsižvelgta vertinant valstybės narės prašymą. ES kibernetinio saugumo rezervo paslaugos taip pat gali būti naudingos panašiomis sąlygomis teikiant paramą Sąjungos institucijoms, įstaigoms ir agentūroms;

(34) siekiant atrinkti privačius paslaugų teikėjus, kurie teiktų paslaugas pagal ES kibernetinio saugumo rezervą, būtina nustatyti minimaliuosius kriterijus, kurie turėtų būti įtraukti į kvietimą teikti pasiūlymus tiems paslaugų teikėjams atrinkti, siekiant užtikrinti, kad būtų tenkinami valstybių narių institucijų ir subjektų, veikiančių ypatingos svarbos ar itin svarbiuose sektoriuose, poreikiai;

(35) siekdama paremti ES kibernetinio saugumo rezervo sukūrimą, Komisija galėtų apsvarstyti galimybę prašyti ENISA pagal Reglamentą (ES) 2019/881 parengti potencialią valdomų saugumo paslaugų sertifikavimo schemą srityse, kurioms taikomas reagavimo į kibernetinio saugumo krizes mechanizmas;

(36) siekiant remti šio reglamento tikslus skatinti bendrą informuotumą apie padėtį, didinti Sąjungos atsparumą ir sudaryti sąlygas veiksmingai reaguoti į reikšmingus ir didelio masto kibernetinio saugumo incidentus, EU-CyCLONe, CSIRT tinklas arba Komisija turėtų turėti galimybę prašyti ENISA peržiūrėti ir įvertinti grėsmes, pažeidžiamumus ir poveikio švelninimo veiksmus, susijusius su konkrečiu reikšmingu ar didelio masto kibernetinio saugumo incidentu. Užbaigusi incidento peržiūrą ir vertinimą, ENISA, bendradarbiaudama su atitinkamais suinteresuotaisiais subjektais, įskaitant privačiojo sektoriaus, valstybių narių, Komisijos ir kitų atitinkamų ES institucijų, įstaigų ir agentūrų atstovus, turėtų parengti incidento peržiūros ataskaitą. Kalbant apie privatųjį sektorių, ENISA kuria informacijos mainų su specializuotais paslaugų teikėjais, įskaitant valdomų saugumo sprendinių teikėjus ir pardavėjus, kanalus, siekdama prisidėti prie ENISA misijos pasiekti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje. Remiantis bendradarbiavimu su suinteresuotaisiais subjektais, įskaitant privatųjį sektorių, konkrečių incidentų peržiūros ataskaitoje turėtų būti siekiama įvertinti incidento priežastis, poveikį ir padarinių švelninimą 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 reikalaujama šiame reglamente. Ataskaita turėtų būti pateikta EU-CyCLONe, CSIRT tinklui ir Komisijai ir ja turėtų

būti remiamasi jų darbe. Kai incidentas susijęs su trečiąja valstybe, Komisija turėtų ja pasidalyti ir su vyriausiuoju įgaliotiniu;

(37) atsižvelgiant į nenuspėjamą kibernetinio saugumo išpuolių pobūdį ir į tai, kad jie neretai nėra susiję su konkrečia geografine vietove ir kelia didelę šalutinio poveikio riziką, didinant kaimyninių šalių atsparumą ir stiprinant gebėjimą veiksmingai reaguoti į reikšmingus ir didelio masto kibernetinio saugumo incidentus prisidedama prie visos Sąjungos apsaugos. Todėl su Skaitmeninės Europos programa asocijuotos trečiosios valstybės gali būti remiamos ES kibernetinio saugumo rezervo lėšomis, jei tai numatyta atitinkamame Skaitmeninės Europos programos asociacijos susitarime. Sąjunga turėtų remti asocijuotųjų trečiųjų valstybių finansavimą pagal toms valstybėms skirtas atitinkamas partnerystes ir finansavimo priemones. Parama turėtų būti skiriama paslaugoms, susijusioms su reagavimu į reikšmingus arba didelio masto kibernetinio saugumo incidentus ir nedelsiamu veiklos atkūrimu po jų. Šiame reglamente ES kibernetinio saugumo rezervui ir patikimiems paslaugų teikėjams nustatytos sąlygos turėtų būti taikomos teikiant paramą Skaitmeninės Europos programos asocijuotosioms trečiosioms valstybėms;

(38) siekiant užtikrinti vienodas šio reglamento įgyvendinimo sąlygas, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai nustatyti tarpvalstybinių SOC sąveikumo sąlygas, nustatyti tarpvalstybinių SOC ir Sąjungos subjektų dalijimosi informacija, susijusia su galimu arba vykstančiu didelio masto kibernetinio saugumo incidentu, procedūrinę tvarką, nustatyti techninius reikalavimus, kuriais užtikrinamas Europos kibernetinio saugumo skydo saugumas, nurodyti reagavimo paslaugų, kurių reikia ES kibernetinio saugumo rezervui, rūšis ir skaičių ir išsamiau nustatyti ES kibernetinio saugumo rezervo paramos paslaugų skyrimo tvarką. Tais įgaliojimais turėtų būti naudojamasi laikantis Europos Parlamento ir Tarybos reglamento (ES) Nr. 182/2011;

(39) šio reglamento tikslo geriau siekti Sąjungos lygmeniu, o ne valstybėse narėse. Todėl, laikydamasi Europos Sąjungos sutarties 5 straipsnyje nustatytų subsidiarumo ir proporcingumo principų, Sąjunga gali patvirtinti priemones. Šiame reglamente nenumatyta nieko, kas nėra būtina siekiant to tikslo,

PRIĖMĖ ŠĮ REGLAMENTĄ:

I skyrius

BENDRIEJI TIKSLAI, DALYKAS IR APIBRĖŽTYS

1 straipsnis

Dalykas ir tikslai

1. Šiuo reglamentu nustatomos priemonės, kuriomis Sąjungoje stiprinami pajėgumai aptikti kibernetinio saugumo grėsmes ir incidentus, jiems pasirengti ir į juos reaguoti, visų pirma imantis šių veiksmų:

a) diegti visos Europos saugumo operacijų centrų infrastruktūrą (Europos kibernetinio saugumo skydą) siekiant sukurti ir sustiprinti bendrus aptikimo ir informuotumo apie padėtį pajėgumus;

b) sukurti Reagavimo į kibernetinio saugumo krizes mechanizmą, skirtą padėti valstybėms narėms pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams, į juos reaguoti ir nedelsiant po jų atkurti veiklą;

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

2. Šiuo reglamentu siekiama stiprinti Sąjungos lygmens solidarumą siekiant šių konkrečių tikslų:

a) stiprinti bendrą Sąjungos kibernetinių grėsmių ir incidentų aptikimą ir informuotumą apie padėtį, taip sudarant sąlygas stiprinti Sąjungos pramonės ir paslaugų sektorių konkurencinę padėtį visoje skaitmeninėje ekonomikoje ir prisidėti prie Sąjungos technologinio suverenumo kibernetinio saugumo srityje;

b) stiprinti subjektų, veikiančių ypatingos svarbos ir itin svarbiuose sektoriuose visoje Sąjungoje, parengtį ir solidarumą plėtojant bendrus reagavimo į reikšmingus arba didelio masto kibernetinio saugumo incidentus pajėgumus, be kita ko, teikiant Sąjungos paramą reaguojant į kibernetinio saugumo incidentus Skaitmeninės Europos programos (SEP) asocijuotosioms trečiosioms valstybėms;

c) didinti Sąjungos atsparumą ir prisidėti prie veiksmingo reagavimo peržiūrint ir įvertinant didelius arba didelio masto incidentus, be kita ko, apibendrinant įgytą patirtį ir, kai tinkama, rengiant rekomendacijas.

3. Šiuo reglamentu nedaroma poveikio pagrindinei valstybių narių atsakomybei už nacionalinį saugumą, visuomenės saugumą ir nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas.

2 straipsnis

Apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1. **tarpvalstybinis saugumo operacijų centras (tarpvalstybinis SOC)** – daugiašalė platforma, kuri į koordinuojamą tinklo struktūrą sujungia bent trijų valstybių narių nacionalinius SOC, sudarančius prieglobos konsorciumą, ir kurios paskirtis – užkirsti kelią kibernetinėms grėsmėms bei incidentams ir padėti rengti aukštos kokybės žvalgybos informaciją, visų pirma keičiantis duomenimis iš įvairių viešųjų ir privačių šaltinių, taip pat dalijantis naujausiomis priemonėmis ir bendrai plėtojant kibernetinių incidentų ir grėsmių aptikimo, analizės, prevencijos ir apsaugos nuo jų pajėgumus patikimoje aplinkoje**;**

2. **viešoji įstaiga** – viešosios teisės reglamentuojamas subjektas, apibrėžtas Europos Parlamento ir Tarybos direktyvos 2014/24/ES[18] 2 straipsnio 1 dalies 4 punkte;

3. **prieglobos konsorciumas** – konsorciumas, sudarytas iš dalyvaujančių valstybių, kurioms atstovauja nacionaliniai SOC ir kurios sutiko sukurti tarpvalstybinio SOC priemones ir infrastruktūrą, prisidėti prie jų įsigijimo ir tarpvalstybinio SOC veikimo;

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

5. **ypatingos svarbos arba itin svarbiuose sektoriuose veikiantys subjektai** – Direktyvos (ES) 2022/2555 I ir II prieduose išvardytų rūšių subjektai;

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

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

8. **didelio masto kibernetinio saugumo incidentas** – incidentas, apibrėžtas Direktyvos (ES) 2022/2555 6 straipsnio 7 punkte;

9. **parengtis** – parengties būsena ir pajėgumas užtikrinti veiksmingą greitą reagavimą į reikšmingą arba didelio masto kibernetinio saugumo incidentą, atlikus rizikos vertinimą ir iš anksto ėmusis stebėsenos veiksmų;

10. **reagavimas** – veiksmai reikšmingo arba didelio masto kibernetinio saugumo incidento atveju, tokio incidento metu ar jam pasibaigus, kuriais siekiama pašalinti jo tiesioginius ir trumpalaikius neigiamus padarinius;

11. **patikimi paslaugų teikėjai** – valdomų saugumo paslaugų teikėjai, apibrėžti Direktyvos (ES) 2022/2555 6 straipsnio 40 punkte, atrinkti pagal šio reglamento 16 straipsnį.

II skyrius

EUROPOS KIBERNETINIO SAUGUMO SKYDAS

3 straipsnis

Europos kibernetinio saugumo skydo sukūrimas

1. Siekiant plėtoti pažangius Sąjungos pajėgumus aptikti kibernetines grėsmes ir incidentus Sąjungoje, juos analizuoti ir tvarkyti duomenis apie juos, sukuriama jungtinė visos Europos saugumo operacijų centrų infrastruktūra (toliau – Europos kibernetinio saugumo skydas). Ją sudaro visi nacionaliniai saugumo operacijų centrai (nacionaliniai SOC) ir tarpvalstybiniai saugumo operacijų centrai (tarpvalstybiniai SOC).

[18] 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).

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

2. Europos kibernetinio saugumo skydas:

a) per tarpvalstybinius SOC telkia įvairių šaltinių duomenis apie kibernetines grėsmes ir incidentus ir jais dalijasi;

b) rengia aukštos kokybės informaciją, kuria remiantis galima imtis veiksmų, ir žvalgybos informaciją apie kibernetines grėsmes, naudodamas naujausias priemones, visų pirma dirbtinio intelekto ir duomenų analizės technologijas;

c) padeda geriau apsisaugoti nuo kibernetinių grėsmių ir į jas reaguoti;

d) padeda sparčiau aptikti kibernetines grėsmes ir didinti informuotumą apie padėtį visoje Sąjungoje;

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

Jis plėtojamas bendradarbiaujant su visos Europos našiosios kompiuterijos infrastruktūra, sukurta pagal Reglamentą (ES) 2021/1173.

4 straipsnis

Nacionaliniai saugumo operacijų centrai

1. Kiekviena valstybė narė paskiria bent po vieną nacionalinį SOC dalyvauti Europos kibernetinio saugumo skydo veikloje. Nacionalinis SOC yra viešoji įstaiga.

Jis yra pajėgus veikti kaip atskaitos taškas ir kreiptis į kitas viešąsias ir privačias nacionalinio lygmens organizacijas, kad rinktų ir analizuotų informaciją apie kibernetinio saugumo grėsmes ir incidentus ir prisidėtų prie tarpvalstybinio SOC veiklos. Jis aprūpinamas naujausiomis technologijomis, kuriomis galima aptikti, kaupti ir analizuoti su kibernetinio saugumo grėsmėmis ir incidentais susijusius duomenis.

2. Paskelbus kvietimą pareikšti susidomėjimą, Europos kibernetinio saugumo kompetencijos centras (ECCC) atrenka nacionalinius SOC dalyvauti bendruose viešuosiuose priemonių ir infrastruktūros pirkimuose su ECCC. ECCC atrinktiems nacionaliniams SOC gali skirti dotacijas šių priemonių ir infrastruktūros veikimui finansuoti. Sąjungos finansiniu įnašu padengiama iki 50 proc. priemonių ir infrastruktūros įsigijimo išlaidų ir iki 50 proc. veiklos išlaidų, o likusias išlaidas padengia valstybė narė. Prieš pradėdami priemonių ir infrastruktūros įsigijimo procedūrą, ECCC ir nacionalinis SOC sudaro prieglobos ir naudojimo susitarimą, kuriuo reglamentuojamas priemonių ir infrastruktūros naudojimas.

3. Pagal 2 dalį atrinktas nacionalinis SOC įsipareigoja pateikti paraišką dalyvauti tarpvalstybiniame SOC per dvejus metus nuo priemonių ir infrastruktūros įsigijimo arba finansavimo dotacijos gavimo dienos, priklausomai nuo to, kuri iš tų datų yra ankstesnė. Jei iki to laiko nacionalinis SOC nepradeda dalyvauti tarpvalstybinio SOC veikloje, jis negali gauti papildomos Sąjungos paramos pagal šį reglamentą.

5 straipsnis

Tarpvalstybiniai saugumo operacijų centrai

1. Teisę dalyvauti steigiant tarpvalstybinį SOC turi prieglobos konsorciumas, kurį sudaro bent trys valstybės narės, atstovaujamos nacionalinių SOC, įsipareigojusių bendradarbiauti koordinuojant savo kibernetinių grėsmių aptikimo ir stebėsenos veiklą.

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

3. Prieglobos konsorciumo nariai sudaro rašytinį konsorciumo susitarimą, kuriame nustatoma prieglobos ir naudojimo susitarimo įgyvendinimo vidaus tvarka.

4. Tarpvalstybiniam SOC teisiškai atstovauja koordinuojantysis nacionalinis SOC arba prieglobos konsorciumas, jei jis turi juridinio asmens statusą. Koordinuojantysis SOC yra atsakingas už prieglobos ir naudojimo susitarimo ir šio reglamento reikalavimų laikymąsi.

6 straipsnis

Bendradarbiavimas ir keitimasis informacija tarpvalstybiniuose SOC ir tarp jų

1. Prieglobos konsorciumo nariai tarpvalstybiniame SOC keičiasi svarbia informacija, įskaitant informaciją, susijusią 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 kibernetinius išpuolius rekomendacijomis, kai tokiu dalijimusi informacija:

a) siekiama užkirsti kelią incidentams, juos aptikti, į juos reaguoti ar po jų atkurti veiklą, arba sumažinti jų poveikį;

b) didinamas kibernetinis saugumas, visų pirma 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, švelninimo strategijas ar 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 dalytis dideliu kiekiu 1 dalyje nurodytų duomenų ir sąlygos, kuriomis turi būti keičiamasi ta informacija;

b) valdymo sistema, kuria visi dalyviai skatinami dalytis informacija;

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

3. Siekiant skatinti tarpvalstybinius SOC keistis informacija tarpusavyje, tarpvalstybiniai SOC užtikrina aukštą tarpusavio sąveikos lygį. Siekdama palengvinti tarpvalstybinių SOC sąveiką, Komisija, pasikonsultavusi su ECCC, šios sąveikos sąlygas gali nustatyti įgyvendinimo aktais. Tie įgyvendinimo aktai priimami laikantis šio reglamento 21 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

4. Tarpvalstybiniai SOC sudaro tarpusavio bendradarbiavimo susitarimus, kuriuose nustatomi tarpvalstybinių platformų keitimosi informacija principai.

7 straipsnis

Bendradarbiavimas ir dalijimasis informacija su Sąjungos subjektais

1. Kai tarpvalstybiniai SOC gauna informacijos, susijusios su galimu arba tebesitęsiančiu didelio masto kibernetinio saugumo incidentu, jie nepagrįstai nedelsdami pateikia atitinkamą informaciją Europos ryšių palaikymo dėl kibernetinių krizių organizaciniam tinklui (EU-CyCLONe), reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) tinklui ir Komisijai, atsižvelgiant į jų atitinkamus krizių valdymo vaidmenis pagal Direktyvą (ES) 2022/2555.

2. Komisija įgyvendinimo aktais gali nustatyti 1 dalyje nurodyto dalijimosi informacija procedūrinę tvarką. Tie įgyvendinimo aktai priimami laikantis šio reglamento 21 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

8 straipsnis

Saugumas

1. Europos kibernetinio saugumo skydo veikloje dalyvaujančios valstybės narės užtikrina aukštą Europos kibernetinio saugumo skydo infrastruktūros duomenų saugumo ir fizinio saugumo lygį ir užtikrina, kad infrastruktūra būtų tinkamai valdoma ir kontroliuojama taip, kad būtų apsaugota nuo grėsmių ir būtų užtikrintas jos ir sistemų, įskaitant duomenis, kuriais keičiamasi per infrastruktūrą, saugumas.

2. Europos kibernetinio saugumo skydo veikloje dalyvaujančios valstybės narės užtikrina, kad dalijimasis informacija Europos kibernetinio saugumo skydo sistemoje su subjektais, kurie nėra valstybių narių viešosios įstaigos, nedarytų neigiamo poveikio Sąjungos saugumo interesams.

3. Komisija gali priimti įgyvendinimo aktus, kuriais nustatomi techniniai reikalavimai, kurių laikydamosi valstybės narės vykdo 1 ir 2 dalyse nustatytą pareigą. Tie įgyvendinimo aktai priimami laikantis šio reglamento 21 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros. Tai darydama Komisija, padedama vyriausiojo įgaliotinio, atsižvelgia į atitinkamus gynybos lygio saugumo standartus, kad palengvintų bendradarbiavimą su kariniais subjektais.

III skyrius

REAGAVIMO Į KIBERNETINIO SAUGUMO KRIZES MECHANIZMAS

9 straipsnis

Reagavimo į kibernetinio saugumo krizes mechanizmo sukūrimas

1. Siekiant padidinti Sąjungos atsparumą didelėms kibernetinio saugumo grėsmėms ir solidariai pasirengti trumpalaikiam reikšmingų ir didelio masto kibernetinio saugumo incidentų poveikiui ir jį sušvelninti, sukuriamas Reagavimo į kibernetinio saugumo krizes mechanizmas (toliau – mechanizmas).

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

10 straipsnis

Veiksmų rūšys

1. Mechanizmu remiami šių rūšių veiksmai:

a) pasirengimo veiksmai, įskaitant koordinuotą subjektų, veikiančių itin svarbiuose sektoriuose visoje Sąjungoje, parengties testavimą;

b) reagavimo veiksmai, kuriais remiamas reagavimas į reikšmingus ir didelio masto kibernetinio saugumo incidentus ir nedelsiamas veiklos atkūrimas po jų ir kuriuos turi vykdyti patikimi paslaugų teikėjai, dalyvaujantys ES kibernetinio saugumo rezerve, sukurtame pagal 12 straipsnį;

c) savitarpio pagalbos veiksmai, t. y. pagalba, kurią vienos valstybės narės nacionalinės institucijos teikia kitai valstybei narei, visų pirma kaip nustatyta Direktyvos (ES) 2022/2555 11 straipsnio 3 dalies f punkte.

11 straipsnis

Koordinuotas subjektų parengties testavimas

1. Siekdama remti koordinuotą 10 straipsnio 1 dalies a punkte nurodytą subjektų parengties testavimą visoje Sąjungoje, Komisija, pasikonsultavusi su TIS bendradarbiavimo grupe ir ENISA, iš Direktyvos (ES) 2022/2555 I priede išvardytų ypatingos svarbos sektorių atrenka sektorius arba subsektorius, kurių subjektams gali būti taikomas koordinuotas parengties testavimas, atsižvelgdama į esamus ir planuojamus suderintus rizikos vertinimus ir atsparumo bandymus Sąjungos lygmeniu.

2. TIS bendradarbiavimo grupė, bendradarbiaudama su Komisija, ENISA ir vyriausiuoju įgaliotiniu, parengia bendrus rizikos scenarijus ir koordinuoto testavimo metodikas.

12 straipsnis

ES kibernetinio saugumo rezervo sukūrimas

1. Siekiant padėti 3 dalyje nurodytiems naudotojams reaguoti į reikšmingus arba didelio masto kibernetinio saugumo incidentus arba teikti reagavimo į tokius incidentus ir nedelsiamo veiklos atkūrimo po jų paramą, sukuriamas ES kibernetinio saugumo rezervas.

2. ES kibernetinio saugumo rezervą sudaro reagavimo į incidentus paslaugos, kurias teikia patikimi paslaugų teikėjai, atrinkti pagal 16 straipsnyje nustatytus kriterijus. Į rezervą įtraukiamos iš anksto įsipareigotos teikti paslaugos. Paslaugos diegiamos visose valstybėse narėse.

3. Be kitų, 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) Sąjungos institucijos, įstaigos ir agentūros.

4. 3 dalies a punkte nurodyti naudotojai naudojasi ES kibernetinio saugumo rezervo paslaugomis, kad reaguotų į reikšmingus arba didelio masto incidentus, darančius poveikį ypatingos svarbos ar itin svarbiuose sektoriuose veikiantiems subjektams, arba padėtų į juos reaguoti ir nedelsiant po jų atkurti veiklą.

5. Komisijai tenka bendra atsakomybė už ES kibernetinio saugumo rezervo įgyvendinimą. Komisija, atsižvelgdama į 3 dalyje nurodytų naudotojų poreikius, 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.

6. Komisija, sudarydama susitarimus dėl įnašų, gali pavesti ENISA visiškai arba iš dalies užtikrinti ES kibernetinio saugumo rezervo veikimą ir administravimą.

7. Siekdama padėti Komisijai sukurti ES kibernetinio saugumo rezervą, ENISA, pasikonsultavusi su valstybėmis narėmis ir Komisija, parengia reikiamų paslaugų aprašą. ENISA, pasikonsultavusi su Komisija, parengia panašų aprašą, kad nustatytų trečiųjų valstybių, galinčių gauti paramą iš ES kibernetinio saugumo rezervo pagal 17 straipsnį, poreikius. Kai tikslinga, Komisija konsultuojasi su vyriausiuoju įgaliotiniu.

8. Komisija įgyvendinimo aktais gali nustatyti ES kibernetinio saugumo rezervui reikalingų reagavimo paslaugų rūšis ir skaičių. Tie įgyvendinimo aktai priimami laikantis 21 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

13 straipsnis

Prašymai suteikti paramą iš ES kibernetinio saugumo rezervo

1. 12 straipsnio 3 dalyje nurodyti naudotojai gali prašyti ES kibernetinio saugumo rezervo paslaugų, kad padėtų reaguoti į reikšmingus arba didelio masto kibernetinio saugumo incidentus ir nedelsiant po jų atkurti veiklą.

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

3. Šio reglamento 12 straipsnio 3 dalies a punkte nurodytų naudotojų paramos prašymai Komisijai ir ENISA perduodami per valstybės narės pagal Direktyvos (ES) 2022/2555 8 straipsnio 3 dalį paskirtą arba įsteigtą bendrą kontaktinį punktą.

4. Valstybės narės informuoja CSIRT tinklą ir, kai tinkama, EU-CyCLONe apie savo prašymus suteikti reagavimo į incidentus ir nedelsiamo veiklos atkūrimo paramą pagal šį straipsnį.

5. Prašyme suteikti reagavimo į incidentus ir nedelsiamo veiklos atkūrimo paramą pateikiama:

a) tinkama informacija apie paveiktą subjektą ir galimą incidento poveikį bei planuojamą prašomos paramos panaudojimą, taip pat nurodant numatomus poreikius;

b) informacija apie priemones, kurių imtasi incidento, dėl kurio prašoma paramos, poveikiui sušvelninti, kaip nurodyta 2 dalyje;

c) informacija apie kitų formų paramą, kurią gali gauti paveiktas subjektas, įskaitant sutartinius susitarimus dėl reagavimo į incidentus ir nedelsiamo veiklos atkūrimo paslaugų, taip pat apie draudimo sutartis, kurios gali apimti tokio pobūdžio incidentus.

6. ENISA, bendradarbiaudama su Komisija ir TIS bendradarbiavimo grupe, parengia šabloną, kad būtų lengviau teikti prašymus suteikti paramą iš ES kibernetinio saugumo rezervo.

7. Komisija gali priimti įgyvendinimo aktus, kuriais išsamiau nustatoma išsami ES kibernetinio saugumo rezervo paramos paslaugų skyrimo tvarka. Tie įgyvendinimo aktai priimami laikantis 21 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.

14 straipsnis

ES kibernetinio saugumo rezervo paramos įgyvendinimas

1. Prašymus suteikti paramą iš ES kibernetinio saugumo rezervo vertina Komisija, padedama ENISA arba kaip nustatyta susitarimuose dėl įnašų pagal 12 straipsnio 6 dalį, o atsakymas nedelsiant perduodamas 12 straipsnio 3 dalyje nurodytiems naudotojams.

2. Kai tuo pačiu metu gaunama daug prašymų, jų pirmenybė nustatoma, kai aktualu, atsižvelgiant į šiuos kriterijus:

a) kibernetinio saugumo incidento sunkumą;

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

c) galimą poveikį paveiktai valstybei narei (-ėms) ar naudotojams;

d) galimą tarpvalstybinį incidento pobūdį ir išplitimo į kitas valstybes nares ar persidavimo kitiems naudotojams riziką;

e) priemones, kurių naudotojas ėmėsi siekdamas padėti reaguoti, ir nedelsiamo veiklos atkūrimo pastangas, nurodytas 13 straipsnio 2 dalyje ir 13 straipsnio 5 dalies b punkte.

3. ES kibernetinio saugumo rezervo paslaugos teikiamos pagal konkrečius paslaugų teikėjo ir naudotojo, kuriam teikiama parama iš ES kibernetinio saugumo rezervo, susitarimus. Į tuos susitarimus įtraukiamos atsakomybės sąlygos.

4. 3 dalyje nurodyti susitarimai gali būti grindžiami šablonais, kuriuos parengė ENISA, pasikonsultavusi su valstybėmis narėmis.

5. Komisija ir ENISA neprisiima sutartinės atsakomybės už žalą, trečiosioms šalims padarytą dėl paslaugų, teikiamų įgyvendinant ES kibernetinio saugumo rezervą.

6. Per vieną mėnesį nuo paramos veiksmo pabaigos naudotojai pateikia Komisijai ir ENISA apibendrinamąją suteiktos paslaugos, pasiektų rezultatų ir įgytos patirties ataskaitą. Kai naudotojas yra iš trečiosios valstybės, kaip nurodyta 17 straipsnyje, tokia ataskaita dalijamasi su vyriausiuoju įgaliotiniu.

7. Komisija TIS bendradarbiavimo grupei reguliariai teikia paramos panaudojimo ir rezultatų ataskaitas.

15 straipsnis

Koordinavimas su krizių valdymo mechanizmais

1. Tais atvejais, kai reikšmingo arba didelio masto kibernetinio saugumo incidento priežastis arba pasekmė yra Sprendime 1313/2013/ES[19] apibrėžta nelaimė, reagavimo į tokius incidentus parama pagal šį reglamentą papildo pagal Sprendimą Nr. 1313/2013/ES vykdomus veiksmus ir nedaro poveikio jo taikymui.

2. Didelio masto tarpvalstybinio kibernetinio saugumo incidento, kai pradedamas taikyti integruoto politinio atsako į krizes mechanizmas (IPCR), atveju pagal šį reglamentą teikiama reagavimo į tokį incidentą parama valdoma pagal atitinkamus IPCR protokolus ir procedūras.

3. Konsultuojantis su vyriausiuoju įgaliotiniu, 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. Ji taip pat gali papildyti vienos valstybės narės kitai valstybei narei teikiamą pagalbą pagal Europos Sąjungos sutarties 42 straipsnio 7 dalį arba ja gali būti prisidedama prie tokios pagalbos.

4. Parama pagal reagavimo į kibernetinio saugumo krizes mechanizmą gali būti kaip bendro Sąjungos ir valstybių narių atsako Sutarties dėl Europos Sąjungos veikimo 222 straipsnyje nurodytose situacijose dalis.

16 straipsnis

Patikimi paslaugų teikėjai

[19] 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).

1. Viešojo pirkimo procedūrose, vykdomose siekiant sukurti ES kibernetinio saugumo rezervą, perkančioji organizacija veikia laikydamasi Reglamente (ES, Euratomas) 2018/1046 nustatytų principų ir šių principų:

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

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

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

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

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

b) paslaugų teikėjas, jo patronuojamosios įmonės ir subrangovai turi įdiegtą su paslauga susijusios neskelbtinos informacijos, visų pirma įrodymų, išvadų ir ataskaitų, apsaugos sistemą ir laikosi Sąjungos saugumo taisyklių dėl ES įslaptintos informacijos apsaugos;

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

d) paslaugų teikėjas yra atlikęs tinkamą patikimumo patikrinimą, bent jau personalo, kurį ketina dislokuoti paslaugoms teikti;

e) paslaugų teikėjas užtikrina tinkamą savo IT sistemų saugumo lygį;

f) paslaugų teikėjas turi techninę ir programinę įrangą, kurios reikia prašomai paslaugai teikti;

g) paslaugų teikėjas geba įrodyti, kad turi panašių paslaugų teikimo atitinkamoms nacionalinėms valdžios institucijoms ar subjektams, veikiantiems ypatingos svarbos ar itin svarbiuose sektoriuose, patirties;

h) paslaugų teikėjas geba suteikti paslaugą per trumpą laikotarpį valstybėje narėje (-ėse), kurioje (-iose) jis gali teikti paslaugą;

i) paslaugų teikėjas geba teikti paslaugą valstybės narės (-ių), kurioje (-iose) jis gali teikti paslaugą, vietos kalba;

j) kai pagal Reglamentą (ES) 2019/881 bus įdiegta valdomų saugumo paslaugų ES sertifikavimo sistema, paslaugų teikėjas turės būti sertifikuotas pagal tą sistemą.

17 straipsnis

Parama trečiosioms valstybėms

1. Trečiosios valstybės gali prašyti paramos iš ES kibernetinio saugumo rezervo, jei tai numatyta sudarytuose asociacijos susitarimuose dėl jų dalyvavimo Skaitmeninės Europos programoje.

2. Parama iš ES kibernetinio saugumo rezervo teikiama pagal šį reglamentą ir visas 1 dalyje nurodytuose asociacijos susitarimuose nustatytas specialiąsias sąlygas.

3. Naudotojai iš asocijuotųjų trečiųjų valstybių, turintys teisę gauti paslaugas iš ES kibernetinio saugumo rezervo, apima kompetentingas institucijas, tokias kaip CSIRT ir kibernetinių krizių valdymo institucijas.

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

5. Prieš gaudamos paramą iš ES kibernetinio saugumo rezervo, trečiosios valstybės pateikia Komisijai ir vyriausiajam įgaliotiniui informaciją apie savo kibernetinį atsparumą ir rizikos valdymo pajėgumus, įskaitant bent informaciją apie nacionalines priemones, kurių imtasi siekiant pasirengti reikšmingiems ar didelio masto kibernetinio saugumo incidentams, taip pat informaciją apie atsakingus nacionalinius subjektus, įskaitant CSIRT arba lygiaverčius subjektus, jų pajėgumus ir jiems skirtus išteklius. Kai šio reglamento 13 ir 14 straipsnių nuostatose daroma nuoroda į valstybes nares, jos taikomos trečiosioms valstybėms, nurodytoms 1 dalyje.

6. Komisija gautų trečiųjų valstybių prašymų ir joms iš ES kibernetinio saugumo rezervo skirtos paramos įgyvendinimo klausimus koordinuoja su vyriausiuoju įgaliotiniu.

IV skyrius

KIBERNETINIO SAUGUMO INCIDENTŲ PERŽIŪROS MECHANIZMAS

18 straipsnis

Kibernetinio saugumo incidentų peržiūros mechanizmas

1. Komisijos, EU-CyCLONe arba CSIRT tinklo prašymu ENISA peržiūri ir įvertina su konkrečiu reikšmingu arba didelio masto kibernetinio saugumo incidentu susijusias grėsmes, pažeidžiamumus ir poveikio švelninimo veiksmus. Užbaigusi incidento peržiūrą ir vertinimą, ENISA pateikia incidento peržiūros ataskaitą CSIRT tinklui, EU-CyCLONe ir Komisijai, kad padėtų joms atlikti savo užduotis, visų pirma užduotis, nustatytas Direktyvos (ES) 2022/2555 15 ir 16 straipsniuose. Kai aktualu, Komisija ataskaita dalijasi su vyriausiuoju įgaliotiniu.

2. Rengdama 1 dalyje nurodytą incidento peržiūros ataskaitą, ENISA bendradarbiauja su visais atitinkamais suinteresuotaisiais subjektais, įskaitant valstybių narių, Komisijos, kitų atitinkamų ES institucijų, įstaigų ir agentūrų, valdomų saugumo paslaugų teikėjų ir kibernetinio saugumo paslaugų naudotojų atstovus. Kai tinkama, ENISA taip pat bendradarbiauja su reikšmingų arba didelio masto kibernetinio saugumo incidentų paveiktais subjektais. Atlikdama peržiūrą, ENISA gali konsultuotis ir su kitais suinteresuotaisiais subjektais. Atstovai, su kuriais konsultuojamasi, atskleidžia informaciją apie bet kokį galimą interesų konfliktą.

3. Ataskaitoje pateikiama konkretaus reikšmingo arba didelio masto kibernetinio saugumo incidento apžvalga ir analizė, apimanti pagrindines priežastis, pažeidžiamumus ir įgytą patirtį.

Konfidenciali informacija joje apsaugoma pagal Sąjungos ar nacionalinę teisę dėl neskelbtinos ar įslaptintos informacijos apsaugos.

4. Kai tinkama, ataskaitoje pateikiamos rekomendacijos, kaip pagerinti Sąjungos kibernetinio saugumo būklę.

5. Jei įmanoma, ataskaitos versija skelbiama viešai. Šioje versijoje pateikiama tik vieša informacija.

V skyrius

BAIGIAMOSIOS NUOSTATOS

19 straipsnis

Reglamento (ES) 2021/694 pakeitimai

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

1) 6 straipsnis iš dalies keičiamas taip:

a) 1 dalis iš dalies keičiama taip:

1. įterpiamas aa punktas:

„aa) remti ES kibernetinio saugumo skydo plėtojimą, įskaitant nacionalinių ir tarpvalstybinių SOC platformų, kurios padeda didinti informuotumą apie padėtį Sąjungoje ir stiprinti Sąjungos kibernetinių grėsmių žvalgybos pajėgumus, kūrimą, diegimą ir veikimą;“;

2. pridedamas g punktas:

„g) sukurti ir valdyti reagavimo į kibernetinio saugumo krizes mechanizmą, skirtą padėti valstybėms narėms pasirengti reikšmingiems kibernetinio saugumo incidentams ir į juos reaguoti, papildant nacionalinius išteklius bei pajėgumus ir kitų formų Sąjungos lygmeniu teikiamą paramą, įskaitant ES kibernetinio saugumo rezervo sukūrimą.“;

b) 2 dalis pakeičiama taip:

„2. Veiksmai pagal 3 konkretų tikslą įgyvendinami visų pirma per Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrą ir Nacionalinių koordinavimo centrų tinklą, vadovaujantis Europos Parlamento ir Tarybos

reglamentu (ES) 2021/887[20], išskyrus ES kibernetinio saugumo rezervo įgyvendinimo veiksmus, kuriuos įgyvendina Komisija ir ENISA.“;

2) 9 straipsnis iš dalies keičiamas taip:

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

„b) 1 776 956 000 EUR skiriama 2 konkrečiam tikslui „Dirbtinis intelektas“;

c) 1 629 566 000 EUR skiriama 3 konkrečiam tikslui „Kibernetinis saugumas ir pasitikėjimas“;

d) 482 347 000 EUR skiriama 4 konkrečiam tikslui „Aukšto lygio skaitmeniniai įgūdžiai“;“;

b) pridedama 8 dalis:

„8. Nukrypstant nuo Reglamento (ES, Euratomas) 2018/1046 12 straipsnio 4 dalies, nepanaudoti įsipareigojimų ir mokėjimų asignavimai, skirti veiksmams, 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.“;

3) 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, apibrėžti Europos Parlamento ir Tarybos direktyvose 2014/24/ES[27] ir 2014/25/ES[28].

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 Reglamento (ES) 2023/XX 12 straipsniu įsteigtam ES kibernetinio saugumo rezervui skirtas viešųjų pirkimų procedūras, Komisija ir ENISA gali veikti kaip centrinė perkančioji organizacija, perkanti 10 straipsnio reikalavimus atitinkančioms Programos asocijuotosioms trečiosioms valstybėms arba jų vardu.

[20] 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. 1–31).

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 Reglamento (ES) XXX/XXXX [nauja Finansinio reglamento redakcija] 169 straipsnio 3 dalies, pavienės trečiosios valstybės prašymo pakanka, kad Komisija arba ENISA būtų įgaliota imtis veiksmų.

Įgyvendindamos Reglamento (ES) 2023/XX 12 straipsniu įsteigtam ES kibernetinio saugumo rezervui skirtas viešųjų pirkimų procedūras, Komisija ir ENISA gali veikti kaip centrinė perkančioji organizacija, perkanti Sąjungos institucijoms, įstaigoms ir 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, įstaigoms ir agentūroms. Nukrypstant nuo Reglamento (ES) XXX/XXXX [nauja Finansinio reglamento redakcija] 169 straipsnio 3 dalies, pavienės Sąjungos institucijos, įstaigos ar agentūros prašymo pakanka, kad Komisija arba ENISA būtų įgaliota imtis veiksmų.

Pagal Programą finansavimas gali būti teikiamas ir finansinėmis priemonėmis, naudojant derinimo operacijas.“;

4) pridedamas 16a straipsnis:

„Veiksmų, kuriais įgyvendinamas Reglamento (ES) 2023/XX 3 straipsniu sukurtas Europos kibernetinio saugumo skydas, atveju taikomos Reglamento (ES) 2023/XX 4 ir 5 straipsniuose nustatytos taisyklės. Jei šio reglamento nuostatos prieštarauja Reglamento (ES) 2023/XX 4 ir 5 straipsniams, pirmenybė teikiama pastarajam reglamentui ir jis taikomas tiems konkretiems veiksmams.“;

5) 19 straipsnis pakeičiamas taip:

„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 Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras gali tiesiogiai skirti Reglamento XXXX 4 straipsnyje nurodytiems nacionaliniams saugumo operacijų centrams ir Reglamento XXXX 5 straipsnyje nurodytam prieglobos konsorciumui, neskelbdamas kvietimo teikti pasiūlymus.

Pagal Finansinio reglamento 195 straipsnio 1 dalies d punktą Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras valstybėms narėms gali tiesiogiai skirti Reglamento XXXX 10 straipsnyje nustatytą reagavimo į kibernetinio saugumo krizes mechanizmo paramą dotacijų forma, neskelbdamas kvietimo teikti pasiūlymus.

Reglamento 202X/XXXX 10 straipsnio 1 dalies c punkte nurodytų veiksmų atveju Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos

centras informuoja Komisiją ir ENISA apie valstybių narių prašymus skirti tiesiogines dotacijas neskelbiant kvietimo teikti pasiūlymus.

Teikiant savitarpio pagalbą reaguojant į reikšmingą arba didelio masto kibernetinio saugumo incidentą, kaip apibrėžta Reglamento XXXX 10 straipsnio c punkte, ir pagal Finansinio reglamento 193 straipsnio 2 dalies antros pastraipos a punktą tinkamai pagrįstais atvejais išlaidos gali būti laikomos tinkamomis finansuoti, net jei jos buvo patirtos prieš pateikiant dotacijos paraišką.“;

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

20 straipsnis

Vertinimas

Iki [ketveri metai nuo šio reglamento taikymo pradžios dienos] Komisija pateikia Europos Parlamentui ir Tarybai šio reglamento vertinimo ir peržiūros ataskaitą.

21 straipsnis

Komiteto procedūra

1. Komisijai padeda Skaitmeninės Europos programos koordinavimo komitetas, įsteigtas Reglamentu (ES) 2021/694. Tas komitetas – tai komitetas, kaip nustatyta Reglamente (ES) Nr. 182/2011.
2. Kai daroma nuoroda į šią dalį, taikomas Reglamento (ES) Nr. 182/2011 5 straipsnis.

22 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 Strasbūre

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkas / Pirmininkė	*Pirmininkas / Pirmininkė*

FINANSINĖ TEISĖS AKTO PASIŪLYMO PAŽYMA

1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA

1,1. Pasiūlymo (iniciatyvos) pavadinimas

1.2. Atitinkama (-os) politikos sritis (-ys)

1.3. Pasiūlymas (iniciatyva) susijęs (-usi) su:

1.4. Tikslas (-ai)

1.4.1. Bendrasis (-ieji) tikslas (-ai)

1.4.2. Konkretus (-ūs) tikslas (-ai)

1.4.3. Numatomas (-i) rezultatas (-ai) ir poveikis

1.4.4. Veiklos rezultatų rodikliai

1.5. Pasiūlymo (iniciatyvos) pagrindas

1.5.1. Trumpalaikiai arba ilgalaikiai poreikiai, įskaitant išsamų iniciatyvos įgyvendinimo pradinio etapo tvarkaraštį

1.5.2. Sąjungos dalyvavimo pridėtinė vertė (gali būti susijusi su įvairiais veiksniais, pvz., koordinavimo nauda, teisiniu tikrumu, didesniu veiksmingumu ar papildomumu). Šiame punkte „Sąjungos dalyvavimo pridėtinė vertė“ – dalyvaujant Sąjungai užtikrinama vertė, papildanti vertę, kuri būtų užtikrinta vien valstybių narių veiksmais.

1.5.3. Panašios patirties išvados

1.5.4. Suderinamumas su daugiamete finansine programa ir galima sinergija su kitomis atitinkamomis priemonėmis

1.5.5. Įvairių turimų finansavimo galimybių vertinimas, įskaitant perskirstymo mastą

1.6. Pasiūlymo (iniciatyvos) trukmė ir finansinis poveikis

1.7. Planuojamas (-i) biudžeto vykdymo metodas (-ai)

2. VALDYMO PRIEMONĖS

2.1. Stebėsenos ir atskaitomybės taisyklės

2.2. Valdymo ir kontrolės sistema (-os)

2.2.1. Valdymo būdo (-ų), finansavimo įgyvendinimo mechanizmo (-ų), mokėjimo tvarkos ir siūlomos kontrolės strategijos pagrindimas

2.2.2. Informacija apie nustatytą riziką ir jai sumažinti įdiegtą (-as) vidaus kontrolės sistemą (-as)

2.2.3. Kontrolės išlaidų efektyvumo apskaičiavimas ir pagrindimas (kontrolės sąnaudų ir susijusių valdomų lėšų vertės santykis) ir numatomo klaidų rizikos lygio vertinimas (atliekant mokėjimą ir užbaigiant programą)

2.3. Sukčiavimo ir pažeidimų prevencijos priemonės

3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS

3.1. Atitinkama (-os) daugiametės finansinės programos išlaidų kategorija (-os) ir biudžeto išlaidų eilutė (-ės)

3.2. Numatomas pasiūlymo finansinis poveikis asignavimams

3.2.1. Numatomo poveikio veiklos asignavimams santrauka

3.2.2. Numatomas veiklos asignavimais finansuojamas atliktas darbas

3.2.3. Numatomo poveikio administraciniams asignavimams santrauka

3.2.3.1. Numatomi žmogiškųjų išteklių poreikiai

3.2.4. Suderinamumas su dabartine daugiamete finansine programa

3.2.5. Trečiųjų šalių įnašai

3.3. Numatomas poveikis pajamoms

1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA

1.1. Pasiūlymo (iniciatyvos) pavadinimas

Europos Parlamento ir Tarybos reglamentas, kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje ir į juos reaguoti didinimo priemonės

1.2. Atitinkama (-os) politikos sritis (-ys)

Prie skaitmeninio amžiaus prisitaikiusi Europa

Europos strateginės investicijos

Veikla: Europos skaitmeninės ateities formavimas

1.3. Pasiūlymas (iniciatyva) susijęs (-usi) su:

☒ **nauju veiksmu**

☐ **nauju veiksmu, kai bus įgyvendintas bandomasis projektas ir (arba) atlikti parengiamieji veiksmai**[33]

☐ **esamo veiksmo galiojimo pratęsimu**

☐ **vieno ar daugiau veiksmų sujungimu arba nukreipimu į kitą / naują veiksmą**

1.4. Tikslas (-ai)

1.4.1. Bendrasis (-ieji) tikslas (-ai)

Kibernetinio solidarumo aktas sustiprins solidarumą Sąjungos lygmeniu, kad būtų galima geriau aptikti kibernetinio saugumo grėsmes ir incidentus, jiems pasirengti ir į juos reaguoti. Juo siekiama:

a) stiprinti bendrą ES kibernetinių grėsmių ir incidentų aptikimo pajėgumą ir gerinti informuotumą apie padėtį;

b) stiprinti subjektų, veikiančių ypatingos svarbos ir itin svarbiuose sektoriuose visoje Sąjungoje, parengtį ir solidarumą plėtojant bendrus reagavimo į reikšmingus arba didelio masto kibernetinio saugumo incidentus pajėgumus, be kita ko, teikiant Sąjungos paramą reaguojant į kibernetinio saugumo incidentus Skaitmeninės Europos programos (SEP) asocijuotosioms trečiosioms valstybėms;

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

1.4.2. Konkretus (-ūs) tikslas (-ai)

Pagal Kibernetinio solidarumo aktą tikslai bus pasiekti:

[33] Kaip nurodyta Finansinio reglamento 58 straipsnio 2 dalies a arba b punkte.

a) diegiant visos Europos saugumo operacijų centrų infrastruktūrą (Europos kibernetinio saugumo skydą), siekiant sukurti ir sustiprinti bendrus aptikimo ir informuotumo apie padėtį pajėgumus;

b) sukuriant reagavimo į kibernetinio saugumo krizes mechanizmą, skirtą padėti valstybėms narėms pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams, į juos reaguoti ir nedelsiant po jų atkurti veiklą. Reagavimo į incidentus parama taip pat teikiama Sąjungos institucijoms, įstaigoms, organams ir agentūroms.

Šie veiksmai bus remiami Skaitmeninės Europos programos finansavimu, kuri šiuo teisėkūros procedūra priimamu aktu bus iš dalies pakeista, nustatant pirmiau minėtus veiksmus, numatant finansinę paramą jiems plėtoti ir paaiškinant finansinės paramos gavimo sąlygas;

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

1.4.3. Numatomas (-i) rezultatas (-ai) ir poveikis

Nurodyti poveikį, kurį pasiūlymas (iniciatyva) turėtų padaryti tiksliniams gavėjams (tikslinėms grupėms).

Pasiūlymu būtų suteikta didelės naudos įvairiems suinteresuotiesiems subjektams. Europos kibernetinio saugumo skydas pagerins valstybių narių kibernetinių grėsmių aptikimo pajėgumus. Reagavimo į kibernetinio saugumo krizes mechanizmas papildys valstybių narių veiksmus, teikdamas skubią paramą pasirengti, reaguoti ir kuo greičiau atsigauti ir (arba) atkurti pagrindinių paslaugų veikimą.

Šiais veiksmais bus sustiprinta pramonės ir verslo konkurencinė padėtis Europoje visoje skaitmenizuotoje ekonomikoje ir remiama jų skaitmeninė transformacija, stiprinant kibernetinio saugumo lygį bendrojoje skaitmeninėje rinkoje. Visų pirma juo siekiama didinti piliečių, įmonių ir subjektų, veikiančių ypatingos svarbos arba itin svarbiuose sektoriuose, atsparumą didėjančioms kibernetinio saugumo grėsmėms, kurios gali turėti pražūtingą poveikį visuomenei ir ekonomikai. Tai bus daroma investuojant į priemones, kurios padės greičiau aptikti kibernetinio saugumo grėsmes ir incidentus ir į juos reaguoti, taip pat padės valstybėms narėms geriau pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams ir į juos reaguoti. Tai taip pat turėtų padėti suteikti Europai daugiau pajėgumų šiose srityse, visų pirma duomenų apie kibernetinio saugumo grėsmes ir incidentus rinkimo ir analizės srityje.

1.4.4. Veiklos rezultatų rodikliai

Nurodyti pažangos ir laimėjimų stebėsenos rodiklius.

Siekiant skatinti solidarumą Sąjungos lygmeniu, būtų galima atsižvelgti į kelis rodiklius:

1) Bendrai įsigytų kibernetinės infrastruktūros objektų arba priemonių ar tiek objektų, tiek priemonių, skaičius

2) Veiksmų, kuriais remiamas pasirengimas kibernetinio saugumo incidentams ir reagavimas į juos pagal reagavimo į kibernetinio saugumo krizes mechanizmą, skaičius.

1.5. Pasiūlymo (iniciatyvos) pagrindas

1.5.1. Trumpalaikiai arba ilgalaikiai poreikiai, įskaitant išsamų iniciatyvos įgyvendinimo pradinio etapo tvarkaraštį

Šis reglamentas turėtų būti visapusiškai taikomas netrukus po jo priėmimo, t. y. dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

1.5.2. Sąjungos dalyvavimo pridėtinė vertė (gali būti susijusi su įvairiais veiksniais, pvz., koordinavimo nauda, teisiniu tikrumu, didesniu veiksmingumu ar papildomumu). Šiame punkte „Sąjungos dalyvavimo pridėtinė vertė“ – dalyvaujant Sąjungai užtikrinama vertė, papildanti vertę, kuri būtų užtikrinta vien valstybių narių veiksmais.

Dėl stipraus tarpvalstybinio kibernetinio saugumo grėsmių pobūdžio apskritai ir didėjančio rizikos ir incidentų, kurių poveikis pasireiškia ne vienoje valstybėje ar sektoriuje ir ne vienam produktui, skaičiaus valstybės narės vienos negali veiksmingai pasiekti dabartinės intervencijos tikslų ir tam reikia bendrų veiksmų ir solidarumo Sąjungos lygmeniu. Kovos su kibernetinėmis grėsmėmis, kylančiomis dėl karo prieš Ukrainą, patirtis, taip pat patirtis, įgyta pirmininkaujant Prancūzijai surengus kibernetinio saugumo pratybas (EU CyCLES) parodė, kad siekiant solidarumo ES lygmeniu turėtų būti sukurti konkretūs savitarpio paramos mechanizmai, visų pirma bendradarbiavimo su privačiuoju sektoriumi. Atsižvelgiant į tai, 2022 m. gegužės 23 d. Tarybos išvadose dėl Europos Sąjungos kibernetinio saugumo būklės raidos Komisija raginama pateikti pasiūlymą dėl naujo Reagavimo į kibernetinio saugumo krizes fondo. Sąjungos lygmens parama ir veiksmai, kuriais siekiama geriau aptikti kibernetinio saugumo grėsmes ir didinti parengties bei reagavimo pajėgumus, suteikia pridėtinės vertės, nes taip išvengiama pastangų dubliavimo visoje Sąjungoje ir valstybėse narėse. Tai padėtų geriau panaudoti turimus išteklius ir geriau koordinuoti veiklą bei keistis informacija apie įgytą patirtį.

1.5.3. Panašios patirties išvados

Kalbant apie informuotumą apie padėtį ir aptikimą pagal Europos kibernetinio saugumo skydo sistemą, pagal SEP 2021–2022 m. kibernetinio saugumo darbo programą buvo paskelbtas kvietimas pareikšti susidomėjimą bendrai pirkti priemones ir infrastruktūrą tarpvalstybiniams SOC įsteigti, taip pat kvietimas dėl dotacijų viešąsias ir privačias organizacijas aptarnaujančių SOC pajėgumams stiprinti.

Kalbant apie parengtį ir reagavimą į incidentus, Komisija parengė trumpojo laikotarpio programą, skirtą padėti valstybėms narėms skiriant papildomą finansavimą ENISA, kad būtų nedelsiant sustiprinta parengtis ir reagavimo į didelius kibernetinius incidentus pajėgumai. Finansuojamos paslaugos apima pasirengimo veiksmus, pvz., ypatingos svarbos subjektų skverbties testavimą, siekiant nustatyti pažeidžiamumus. Ji padidins ir galimybes padėti valstybėms narėms didelių incidentų, darančių poveikį ypatingos svarbos subjektams, atveju. ENISA įgyvendina šią trumpojo laikotarpio programą ir jau pateikė svarbių vertingų įžvalgų, į kurias atsižvelgta rengiant šį reglamentą.

1.5.4. Suderinamumas su daugiamete finansine programa ir galima sinergija su kitomis atitinkamomis priemonėmis

Kibernetinio solidarumo aktas bus grindžiamas veiksmais, kuriuos šiuo metu remia Sąjunga ir valstybės narės, siekdamos didinti informuotumą apie padėtį ir nustatyti kibernetines grėsmes, taip pat reaguoti į didelio masto ir tarpvalstybinius kibernetinio

saugumo incidentus. Be to, priemonė dera su kitomis krizių valdymo sistemomis, įskaitant IPCR, bendrą saugumo ir gynybos politiką, įskaitant greitojo reagavimo į kibernetinius incidentus komandas, ir pagalbą, kurią viena valstybė narė teikia kitai valstybei narei pagal Europos Sąjungos sutarties 42 straipsnio 7 dalį. Naujuoju pasiūlymu taip pat būtų papildomos ir remiamos struktūros, sukurtos pagal kitas kibernetinio saugumo priemones, pvz., Direktyvą (ES) 2022/2555 (TIS 2 direktyva) arba Reglamentą 2019/881 (Kibernetinio saugumo aktas).

1.5.5. Įvairių turimų finansavimo galimybių vertinimas, įskaitant perskirstymo mastą

ENISA priskirtų veiklos sričių valdymas atitinka jos turimus įgaliojimus ir bendrąsias užduotis. Šioms veiklos sritims gali prireikti specialių profilių arba naujų užduočių, tačiau juos jas būtų galima įsisavinti naudojant esamus ENISA išteklius ir perskirstant arba susiejant įvairias užduotis. ENISA šiuo metu įgyvendina trumpojo laikotarpio programą, kurią 2022 m. parengė Komisija, siekdama nedelsiant sustiprinti parengtį ir reagavimo į didelius kibernetinius incidentus pajėgumus. Paslaugos apima galimybes padėti valstybėms narėms didelių incidentų, darančių poveikį ypatingos svarbos subjektams, atveju. ENISA įgyvendina šią trumpojo laikotarpio programą ir jau pateikė svarbių vertingų įžvalgų, į kurias atsižvelgta rengiant šį reglamentą. Trumpojo laikotarpio programai skirti ištekliai gali būti naudojami ir taikant šį reglamentą.

1.6. Pasiūlymo (iniciatyvos) trukmė ir finansinis poveikis

☒ **ribotos trukmės**

– ☒ prasideda nuo pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje ir į juos reaguoti didinimo priemonės, (Kibernetinio solidarumo akto) priėmimo dienos.

– ☒ Įsipareigojimų asignavimų finansinis poveikis nuo 2023 iki 2027 m., o mokėjimų asignavimų – nuo 2023 iki 2031 m.[34].

☐ **neribotos trukmės**

– įgyvendinimo pradinis laikotarpis – nuo MMMM iki MMMM,

– vėliau – visuotinis taikymas.

1.7. Planuojamas (-i) biudžeto vykdymo metodas (-ai)[35]

☒ **Tiesioginis valdymas**, vykdomas Komisijos:

– ☒ padalinių, įskaitant Sąjungos delegacijų darbuotojus;

– ☐ vykdomųjų įstaigų.

☐ **Pasidalijamasis valdymas** su valstybėmis narėmis

☒ **Netiesioginis valdymas**, biudžeto vykdymo užduotis pavedant:

– ☐ trečiosioms valstybėms arba jų paskirtoms įstaigoms;

– ☐ tarptautinėms organizacijoms ir jų agentūroms (nurodyti);

– ☐ EIB ir Europos investicijų fondui;

– ☒ įstaigoms, nurodytoms Finansinio reglamento 70 ir 71 straipsniuose;

– ☐ viešosios teisės reglamentuojamoms įstaigoms;

– ☐ įstaigoms, kurių veiklą reglamentuoja privatinė teisė ir kurioms pavesta teikti viešąsias paslaugas, tiek, kiek joms užtikrinamos pakankamos finansinės garantijos;

– ☐ įstaigoms, kurių veiklą reglamentuoja valstybės narės privatinė teisė, kurioms pavesta įgyvendinti viešojo ir privačiojo sektorių partnerystę ir kurioms užtikrinamos pakankamos finansinės garantijos;

– ☐ atitinkamame pagrindiniame akte nurodytiems asmenims, kuriems pavesta vykdyti konkrečius veiksmus BUSP srityje pagal ES sutarties V antraštinę dalį.

– *Jei nurodomas daugiau kaip vienas valdymo būdas, išsamią informaciją pateikti šio punkto pastabų skiltyje.*

Pastabos

Su Europos kibernetinio saugumo skydu susijusius veiksmus įgyvendins EKSKC. Kol EKSKC negalės vykdyti savo biudžeto, Europos Komisija EKSKC vardu įgyvendins tiesioginio valdymo veiksmus. EKSKC, remdamasis kvietimais pareikšti susidomėjimą, gali

[34] Akte numatyti veiksmai turėtų būti remiami pagal kitą daugiametę finansinę programą.

[35] Informacija apie biudžeto valdymo būdus ir nuorodos į Finansinį reglamentą pateikiamos svetainėje „BUDGpedia“ https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

atrinkti subjektus dalyvauti bendruose priemonių viešuosiuose pirkimuose. EKSKC gali skirti dotacijas šių priemonių naudojimui užtikrinti.

Be to, ECCC gali skirti dotacijas pasirengimo veiksmams pagal reagavimo į kibernetinio saugumo krizes mechanizmą.

Komisijai tenka bendra atsakomybė už ES kibernetinio saugumo rezervo įgyvendinimą. Komisija, sudarydama susitarimus dėl įnašų, gali visiškai arba iš dalies patikėti ES kibernetinio saugumo rezervo veikimą ir administravimą ENISA. Šiuo reglamentu ENISA paskirti veiksmai atitinka jos dabartinius įgaliojimus. Tie veiksmai apima: i) paramą TIS bendradarbiavimo grupei rengti pasirengimo veiksmus remiantis rizikos vertinimais; ii) paramą Komisijai kurti ir prižiūrėti ES kibernetinio saugumo rezervo įgyvendinimą, įskaitant paramos prašymų gavimą ir tvarkymą; iii) šablonų rengimą siekiant sudaryti palankesnes sąlygas teikti prašymus dėl paramos ir sudaryti konkrečius paslaugų teikėjo ir naudotojo, kuriam teikiama parama iš ES kibernetinio saugumo rezervo, susitarimus; iv) su konkrečiais reikšmingais arba didelio masto kibernetinio saugumo incidentais susijusių grėsmių, pažeidžiamumų ir poveikio mažinimo veiksmų peržiūrą ir vertinimą ir jų ataskaitų rengimą.

Apskaičiuota, kad visos šios užduotys sudarys apie 7 etato ekvivalentus iš esamų ENISA išteklių, remiantis patirtimi ir parengiamuoju darbu, kurį ENISA šiuo metu atlieka vykdydama bandomąjį skubios pasirengimo ir reagavimo į incidentus paramos bandomąjį projektą.

2. VALDYMO PRIEMONĖS

2.1. Stebėsenos ir atskaitomybės taisyklės

Nurodyti dažnumą ir sąlygas.

Komisija stebės naujų nuostatų įgyvendinimą, taikymą ir laikymąsi, kad galėtų įvertinti jų efektyvumą. Komisija ne vėliau kaip praėjus ketveriems metams nuo šio reglamento taikymo pradžios dienos pateikia Europos Parlamentui ir Tarybai šio reglamento vertinimo ir peržiūros ataskaitą.

2.2. Valdymo ir kontrolės sistema (-os)

2.2.1. Valdymo būdo (-ų), finansavimo įgyvendinimo mechanizmo (-ų), mokėjimo tvarkos ir siūlomos kontrolės strategijos pagrindimas

Reglamentu nustatoma ES finansavimo įgyvendinimo sistema, kuria siekiama didinti kibernetinio saugumo atsparumą imantis veiksmų, kuriais stiprinami reikšmingų ir didelio masto kibernetinio saugumo incidentų aptikimo, reagavimo į juos ir veiklos atkūrimo po jų pajėgumai. Už politikos sritį atsakingi Ryšių tinklų, turinio ir technologijų GD skyriai valdys direktyvos įgyvendinimą.

Siekiant vykdyti naujas užduotis, būtina užtikrinti, kad Komisijos tarnybos turėtų pakankamai išteklių. Apskaičiuota, kad siekiant įgyvendinti naująjį reglamentą, reikės 6 etato ekvivalentų (3 AD ir 3 CA), kurie apims šias užduotis:

- pasirengimo veiksmų nustatymas remiantis rizikos vertinimais;
- tarpvalstybinių SOC platformų sąveikumo užtikrinimas;
- galimų įgyvendinimo aktų (dviejų dėl SOC ir dviejų dėl reagavimo į kibernetinio saugumo krizes mechanizmo) rengimas;
- susitarimų dėl SOC prieglobos ir naudojimo valdymas;
- ES kibernetinio saugumo rezervo sukūrimas ir valdymas tiesiogiai arba pagal susitarimą dėl įnašo su ENISA. Susitarimo dėl įnašo su ENISA atveju – susitarimo dėl įnašo, susijusio su ENISA pavestomis užduotimis, rengimas ir įgyvendinimo priežiūra;
- dalyvavimas konsultacijų grupėse, kurias ENISA suburia siekdama atlikti reikšmingų ir didelio masto kibernetinio saugumo incidentų peržiūrą ir vertinimą ir parengti ataskaitas.

2.2.2. Informacija apie nustatytą riziką ir jai sumažinti įdiegtą (-as) vidaus kontrolės sistemą (-as)

Nustatyta su Europos kibernetinio saugumo skydu susijusi rizika yra ta, kad valstybės narės nepakankamai dalysis atitinkama informacija apie kibernetines grėsmes nei tarpvalstybinių SOC platformose, nei tarpvalstybinėse platformose ar kituose atitinkamuose ES lygmens subjektuose. Siekiant sumažinti šią riziką, finansavimas bus skiriamas paskelbus kvietimą pareikšti susidomėjimą, kai valstybės narės įsipareigoja dalytis tam tikra informacija ES lygmeniu. Šis įsipareigojimas bus oficialiai įtvirtintas prieglobos ir naudojimo susitarime, kuriuo EKSKC bus suteikti įgaliojimai atlikti auditą siekiant užtikrinti, kad bendrai įsigytos priemonės ir infrastruktūra būtų naudojamos pagal susitarimą. Įsipareigojimai užtikrinti aukšto

lygio keitimąsi informacija tarpvalstybiniuose SOC bus oficialiai įtvirtinti konsorciumo susitarime.

Nustatyta su reagavimo į kibernetinio saugumo krizes mechanizmu susijusi rizika yra ta, kad mechanizme dalyvaujantys naudotojai nesiims pakankamų priemonių, kad užtikrintų pasirengimą kibernetiniams išpuoliams. Todėl, kad galėtų gauti paramą iš ES kibernetinio saugumo rezervo, naudotojai įpareigojami imtis tokių pasirengimo priemonių. Teikdami ES kibernetinio saugumo rezervo paramos prašymus naudotojai turi paaiškinti, kokių priemonių jau ėmėsi siekdami reaguoti į incidentą, ir į tai bus atsižvelgta vertinant ES kibernetinio saugumo rezervo paramos prašymus.

2.2.3. Kontrolės išlaidų efektyvumo apskaičiavimas ir pagrindimas (kontrolės sąnaudų ir susijusių valdomų lėšų vertės santykis) ir numatomo klaidų rizikos lygio vertinimas (atliekant mokėjimą ir užbaigiant programą)

Kadangi dalyvvimo Skaitmeninės Europos programoje taisyklės, taikytinos paramai pagal Kibernetinio solidarumo aktą, yra panašios į tas, kurias savo darbo programose naudos Komisija, ir kadangi paramos gavėjų populiacija bus panašaus rizikos profilio kaip ir tiesiogiai valdomų programų paramos gavėjai, galima tikėtis, kad klaidų lygis bus panašus į tą, kurį Komisija numatė Skaitmeninės Europos programos atveju, t. y. suteikti pakankamą užtikrinimą, kad klaidų rizika daugiamečiu išlaidų laikotarpiu kasmet svyruotų nuo 2 iki 5 %, o galutinis tikslas būtų užtikrinti, kad daugiamečių programų įgyvendinimo pabaigoje likutinių klaidų dydis būtų kuo artimesnis 2 % (atsižvelgus į visų auditų, taisomųjų ir susigrąžinimo priemonių finansinį poveikį).

2.3. Sukčiavimo ir pažeidimų prevencijos priemonės

Nurodyti dabartines arba numatytas prevencijos ir apsaugos priemones, pvz., išdėstytas Kovos su sukčiavimu strategijoje.

Europos kibernetinio saugumo skydo atveju EKSKC, remdamasis prieiga prie informacijos ir patikrinimais vietoje, turės įgaliojimus atlikti bendrai įsigytų priemonių ir infrastruktūros auditą pagal prieglobos ir naudojimo susitarimą, kurį turi pasirašyti prieglobos konsorciumas ir EKSKC.

Papildomi asignavimai, reikalingi šiam reglamentui, bus padengiami esamomis Sąjungos institucijoms, įstaigoms ir agentūroms taikomomis sukčiavimo prevencijos priemonėmis.

3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS

3.1. Atitinkama (-os) daugiametės finansinės programos išlaidų kategorija (-os) ir biudžeto išlaidų eilutė (-ės)

- Dabartinės biudžeto eilutės

Daugiametės finansinės programos išlaidų kategorijas ir biudžeto eilutes nurodyti eilės tvarka.

Daugiametės finansinės programos išlaidų kategorija	Biudžeto eilutė	Išlaidų rūšis	Įnašas			
	Numeris	DA / NDA[36]	ELPA šalių[37]	valstybių kandidačių ir potencialių kandidačių [38]	kitų trečiųjų valstybių	kitų asignuotųjų pajamų
1	02 04 01 10 – Skaitmeninės Europos programa – kibernetinis saugumas	DA	TAIP	TAIP	NE	NE
1	02 04 01 11 – Skaitmeninės Europos programa – Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras	DIF	TAIP	TAIP	NE	NE
1	02 04 03 – Skaitmeninės Europos programa – dirbtinis intelektas	DIF	TAIP	TAIP	NE	NE
1	02 04 04 – Skaitmeninės Europos programa – įgūdžiai	DIF	TAIP	TAIP	NE	NE
1	02 01 30 – Rėmimo išlaidos Skaitmeninės Europos programai	NDA	TAIP	TAIP	NE	NE

[36] DA – diferencijuotieji asignavimai, NDA – nediferencijuotieji asignavimai.
[37] ELPA – Europos laisvosios prekybos asociacija.
[38] Valstybės kandidatės ir, kai taikytina, potencialios valstybės kandidatės.

3.2. Numatomas pasiūlymo finansinis poveikis asignavimams

3.2.1. Numatomo poveikio veiklos asignavimams santrauka

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti veiklos asignavimai nenaudojami

– ☒ Pasiūlymui (iniciatyvai) įgyvendinti veiklos asignavimai naudojami taip:

mln. EUR (tūkstantųjų tikslumu)

Daugiametės finansinės programos išlaidų kategorija	Numeris	1 **Bendroji rinka, inovacijos ir skaitmeninė ekonomika**

Pasiūlymas nepadidins bendro įsipareigojimų pagal Skaitmeninės Europos programą lygio. Iš tiesų įnašas į šią iniciatyvą yra įsipareigojimų, prisiimtų iš KT2 ir KT4, perskirstymas siekiant padidinti KT3 ir EKSKC biudžetą. Bet koks įsipareigojimų pagal Skaitmeninės Europos programą padidinimas dėl DFP peržiūros galėtų būti panaudotas šiai iniciatyvai įgyvendinti.

CONNECT GD			**2025** metai	**2026** metai	**2027** metai	**2028** m. ir vėliau	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)			**IŠ VISO**
○ Veiklos asignavimai										
Biudžeto eilutė[39] 02.040110 (perskirstymas iš 02.0403 ir 02.0404)	Įsipareigojimai	(1a)	15.000	15.000	6.000	p. m.				**36.000**
	Mokėjimai	(2a)	15.000	15.000	6.000					**36.000**
Biudžeto eilutė 02.040111.02 (perskirstymas iš 02.0403 ir 02.0404)	Įsipareigojimai	(1b)	13.000	23.000	28.000	p. m.				**64.000**
	Mokėjimai	(2b)	8.450	18.200	25.250	12.100				**64.000**
Administracinio pobūdžio asignavimai, finansuojami iš konkrečių programų paketo lėšų[40]										
02.0130 biudžeto eilutė		(3)	0.150	0.150	0.150	p. m.				0.450

[39] Pagal oficialią biudžeto nomenklatūrą.

[40] Techninė ir (arba) administracinė parama bei išlaidos ES programų ir (arba) veiksmų įgyvendinimui remti (buvusios BA eilutės), netiesioginiai moksliniai tyrimai, tiesioginiai moksliniai tyrimai.

IŠ VISO asignavimų CNECT GD	Įsipareigojimai	=1a+1b +3	**28.150**	**38.150**	**34.150**	**p. m.**				**100.450**
	Mokėjimai	=2a+2b +3	**23.600**	**33.350**	**31.400**	**12.100**				**100.450**

○ IŠ VISO veiklos asignavimų	Įsipareigojimai	(4)	28.000	38.000	34.000	p. m.				**100.000**
	Mokėjimai	(5)	23.450	33.200	31.250	12.100				**100.000**
○ IŠ VISO administracinio pobūdžio asignavimų, finansuojamų iš konkrečių programų paketo lėšų		(6)	0.150	0.150	0.150	p. m.				**0.450**
IŠ VISO asignavimų pagal daugiametės finansinės programos **1 IŠLAIDŲ KATEGORIJĄ**	Įsipareigojimai	=4+ 6	**28.150**	**38.150**	**34.150**	**p. m.**				**100.450**
	Mokėjimai	=5+ 6	**23.600**	**33.350**	**31.400**	**12.100**				**100.450**

Jei pasiūlymas (iniciatyva) daro poveikį kelioms veiklos išlaidų kategorijoms, pakartokite pirmiau pateiktą dalį:

○ IŠ VISO veiklos asignavimų (visose veiklos išlaidų kategorijose)	Įsipareigojimai	(4)	28.000	38.000	34.000	p. m.				**100.000**
	Mokėjimai	(5)	23.450	33.200	31.250	12.100				**100.000**
IŠ VISO administracinio pobūdžio asignavimų, finansuojamų iš konkrečių programų paketo lėšų (visose veiklos išlaidų kategorijose)		(6)	0.150	0.150	0.150					**0.450**
IŠ VISO asignavimų pagal daugiametės finansinės programos **1–6 IŠLAIDŲ KATEGORIJAS** (Orientacinė suma)	Įsipareigojimai	=4+ 6	**28.150**	**38.150**	**34.150**	**p. m.**				**100.450**
	Mokėjimai	=5+ 6	**23.600**	**33.350**	**31.400**	**12.100**				**100.450**

Daugiametės finansinės programos išlaidų kategorija	**7**	„Administracinės išlaidos“

Šią dalį pildyti naudojant administracinio pobūdžio biudžeto duomenų lentelę, kuri pirmiausia bus pateikta finansinės teisės akto pasiūlymo pažymos priede (Komisijos sprendimo dėl Europos Sąjungos bendrojo biudžeto Komisijos skirsnio įgyvendinimo vidaus taisyklių 5 priedas) ir įkelta į DECIDE tarnybų tarpusavio konsultacijoms.

mln. EUR (tūkstantųjų tikslumu)

		2025 metai	2026 metai	2027 metai	**2028** m. ir vėliau	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)			**IŠ VISO**
GD: CONNECT									
○ Žmogiškieji ištekliai		0.786	0.786	0.786	p. m.				**2.358**
○ Kitos administracinės išlaidos		0.035	0.035	0.035	p. m.				**0.105**
IŠ VISO GD CONNECT	Asignavimai	**0.821**	**0.821**	**0.821**					**2.463**

IŠ VISO asignavimų pagal daugiametės finansinės programos **7 IŠLAIDŲ KATEGORIJĄ**	(Iš viso įsipareigojimų = Iš viso mokėjimų)	**0.821**	**0.821**	**0.821**					**2.463**

mln. EUR (tūkstantųjų tikslumu)

		2025 metai	2026 metai	2027 metai	**2028** m. ir vėliau	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)			**IŠ VISO**
IŠ VISO asignavimų pagal daugiametės finansinės programos **1–7 IŠLAIDŲ KATEGORIJAS**	Įsipareigojimai	**28.971**	**38.971**	**34.971**	**p. m.**				**102.913**
	Mokėjimai	**24.421**	**34.171**	**32.221**	**12.100**				**102.913**

3.2.2. Numatomas veiklos asignavimais finansuojamas atliktas darbas

Įsipareigojimų asignavimai mln. EUR (tūkstantųjų tikslumu)

Nurodyti tikslus ir atliktus darbus ⇩			**N** metai		**N+1** metai		**N+2** metai		**N+3** metai		Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)						**IŠ VISO**	
	ATLIKTI DARBAI																	
	Rūšis [41]	Vidutinės sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Bendras skaičius	Iš viso sąnaudų
1 KONKRETUS TIKSLAS[42]																		
- Atliktas darbas																		
- Atliktas darbas																		
- Atliktas darbas																		
1 konkretaus tikslo tarpinė suma																		
2 KONKRETUS TIKSLAS ...																		
- Atliktas darbas																		
2 konkretaus tikslo tarpinė suma																		
IŠ VISO																		

[41] Atlikti darbai – tai būsimi produktai ir paslaugos (pvz., finansuota studentų mainų, nutiesta kelių kilometrų ir kt.).

[42] Kaip apibūdinta 1.4.2 skirsnyje. „Konkretus (-ūs) tikslas (-ai)...“.

3.2.3. Numatomo poveikio administraciniams asignavimams santrauka

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimų nenaudojama

– ☒ Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimai naudojami taip:

mln. EUR (tūkstantųjų tikslumu)

	2025 metai	2026 metai	2027 metai	N+3 metai	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)			**IŠ VISO**
Daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJA								
Žmogiškieji ištekliai	0.786	0.786	0.786					**2.358**
Kitos administracinės išlaidos	0.035	0.035	0.035					**0.105**
Daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJOS tarpinė suma	**0.821**	**0.821**	**0.821**					**2.463**
Neįtraukta į daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJĄ[43]								
Žmogiškieji ištekliai								
Kitos administracinio pobūdžio išlaidos	0.150	0.150	0.150					**0.450**
Tarpinė suma, neįtraukta į daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJĄ	**0.150**	**0.150**	**0.150**					**0.450**
IŠ VISO	**0.971**	**0.971**	**0.971**					**2.913**

Žmogiškųjų išteklių ir kitų administracinio pobūdžio išlaidų asignavimų poreikiai bus tenkinami iš GD asignavimų, jau paskirtų veiksmui valdyti ir (arba) perskirstytų generaliniame direktorate, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam GD gali būti skiriamos pagal metinę lėšų skyrimo procedūrą ir atsižvelgiant į biudžeto apribojimus.

[43] Techninė ir (arba) administracinė parama bei išlaidos ES programų ir (arba) veiksmų įgyvendinimui remti (buvusios BA eilutės), netiesioginiai moksliniai tyrimai, tiesioginiai moksliniai tyrimai.

3.2.3.1. Numatomi žmogiškųjų išteklių poreikiai

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškųjų išteklių nenaudojama.

– ☒ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškieji ištekliai naudojami taip:

Sąmatą surašyti etatų vienetais

		2025 metai	**2026** metai	2027 metai	**N+3** metai	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)		
O Etatų plano pareigybės (pareigūnai ir laikinieji darbuotojai)								
20 01 02 01 (Komisijos būstinė ir atstovybės)		3	3	3				
20 01 02 03 (Delegacijos)								
01 01 01 01 (Netiesioginiai moksliniai tyrimai)								
01 01 01 11 (Tiesioginiai moksliniai tyrimai)								
Kitos biudžeto eilutės (nurodyti)								
O Išorės darbuotojai (etatų vienetais – FTE)[44]								
20 02 01 (AC, END, INT finansuojami iš bendrojo biudžeto)		3	3	3				
20 02 03 (AC, AL, END, INT ir JPD delegacijose)								
XX 01 xx **yy zz** [45]	- būstinėje							
	- delegacijose							
01 01 01 02 (AC, END, INT – netiesioginiai moksliniai tyrimai)								
01 01 01 12 (AC, END, INT – tiesioginiai moksliniai tyrimai)								
Kitos biudžeto eilutės (nurodyti)								
IŠ VISO		**6**	**6**	**6**				

XX yra atitinkama politikos sritis arba biudžeto antraštinė dalis.

Žmogiškųjų išteklių poreikiai bus tenkinami panaudojant GD darbuotojus, jau paskirtus veiksmui valdyti ir (arba) perskirstytus generaliniame direktorate, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam GD gali būti skiriamos pagal metinę lėšų skyrimo procedūrą ir atsižvelgiant į biudžeto apribojimus.

Vykdytinų užduočių aprašymas:

Pareigūnai ir laikinieji darbuotojai	- pasirengimo veiksmų nustatymas remiantis rizikos vertinimais (11 str.); - galimų įgyvendinimo aktų (dviejų dėl SOC ir dviejų dėl reagavimo į kibernetinio saugumo krizes mechanizmo) rengimas; - susitarimų dėl SOC prieglobos ir naudojimo valdymas; - ES kibernetinio saugumo rezervo sukūrimas ir valdymas tiesiogiai arba pagal susitarimą dėl įnašo su ENISA.
Išorės darbuotojai	Prižiūrint pareigūnui, - pasirengimo veiksmų nustatymas remiantis rizikos vertinimais (11 str.); - galimų įgyvendinimo aktų (dviejų dėl SOC ir dviejų dėl reagavimo į kibernetinio saugumo krizes mechanizmo) rengimas; - susitarimų dėl SOC prieglobos ir naudojimo valdymas; - ES kibernetinio saugumo rezervo sukūrimas ir valdymas tiesiogiai arba pagal susitarimą dėl įnašo su ENISA.

[44] AC – sutartininkas, AL – vietinis darbuotojas, END – deleguotasis nacionalinis ekspertas, INT – per agentūrą įdarbintas darbuotojas, JPD – jaunesnysis delegacijos specialistas.

[45] Neviršijant viršutinės ribos, nustatytos išorės darbuotojams, finansuojamiems iš veiklos asignavimų (buvusių BA eilučių).

3.2.4. Suderinamumas su dabartine daugiamete finansine programa

Pasiūlymui (iniciatyvai):

– [X] galima užtikrinti visišką finansavimą perskirstant asignavimą atitinkamoje daugiametės finansinės programos (DFP) išlaidų kategorijoje.

Paaiškinti, kaip reikia pakeisti programavimą, ir nurodyti atitinkamas biudžeto eilutes bei sumas. Jeigu programavimas keičiamas iš esmės, pateikti „Excel“ lentelę.

	23	24	25	26	27	Iš viso
KT1	16,232,897	20,528,765	17,406,899	16,223,464	10,022,366	80,414,391
KT2 pradinis	226,316,819	295,067,000	195,649,000	221,809,000	246,608,000	1,185,449,819
CYBER iniciatyvai			18,000,000	28,000,000	19,000,000	65,000,000
NAUJAS KT2	**226,316,819**	**295,067,000**	**177,649,000**	**193,809,000**	**227,608,000**	**1,120,449,819**
KT3 DB 24	24,361,553	35,596,172	3,638,000	3,638,000	11,175,000	78,408,725
Iš KT2–KT4			15,000,000	15,000,000	6,000,000	36,000,000
Naujas KT3	**24,361,553**	**35,596,172**	**18,638,000**	**18,638,000**	**17,175,000**	**114,408,725**
ECCC pradinis	176,222,303	208,374,879	104,228,130	90,704,986	84,851,497	664,381,795
Iš KT2–KT4			13,000,000	23,000,000	28,000,000	64,000,000
Naujas ECCC	**176,222,303**	**208,374,879**	**117,228,130**	**113,704,986**	**112,851,497**	**728,381,795**
KT4 pradinis	66,902,708	64,892,032	56,577,977	70,477,245	72,107,201	330,957,163
CYBER iniciatyvai			10,000,000	10,000,000	15,000,000	35,000,000
NAUJAS KT4	**66,902,708**	**64,892,032**	**46,577,977**	**60,477,245**	**57,107,201**	**295,957,163**

– [ ] reikia panaudoti nepaskirstytą maržą pagal atitinkamą DFP išlaidų kategoriją ir (arba) specialias priemones, kaip apibrėžta DFP reglamente.

Paaiškinti, ką reikia atlikti, ir nurodyti atitinkamas išlaidų kategorijas, biudžeto eilutes bei sumas ir pasiūlytas naudoti priemones.

– [ ] reikia persvarstyti DFP.

Paaiškinti, ką reikia atlikti, ir nurodyti atitinkamas išlaidų kategorijas, biudžeto eilutes ir sumas.

3.2.5. Trečiųjų šalių įnašai

Pasiūlyme (iniciatyvoje):

– [X] nenumatyta bendro su trečiosiomis šalimis finansavimo

– [ ] numatytas trečiųjų šalių bendras finansavimas apskaičiuojamas taip:

Asignavimai mln. EUR (tūkstantųjų tikslumu)

	N[46] metai	**N+1 metai**	**N+2 metai**	**N+3 metai**	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)	Iš viso

[46] N metai yra pasiūlymo (iniciatyvos) įgyvendinimo pradžios metai. Pakeiskite „N“ numatomais pirmaisiais įgyvendinimo metais (pvz., 2021). Atitinkamai pakeiskite vėlesnius metus.

Nurodyti bendrą finansavimą teikiančią įstaigą								
IŠ VISO bendrai finansuojamų asignavimų								

3.3. Numatomas poveikis pajamoms

– ☒ Pasiūlymas (iniciatyva) neturi finansinio poveikio pajamoms.

– ☐ Pasiūlymas (iniciatyva) turi finansinį poveikį:

  – ☐ nuosaviems ištekliams

  – ☐ kitoms pajamoms

  – nurodyti, jei pajamos priskirtos išlaidų eilutėms ☐

mln. EUR (tūkstantųjų tikslumu)

Biudžeto pajamų eilutė:	Einamųjų finansinių metų asignavimai	Pasiūlymo (iniciatyvos) poveikis[47]						
		N metai	**N+1 metai**	**N+2 metai**	**N+3 metai**	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)		
……. straipsnis								

Asignuotųjų pajamų atveju nurodyti biudžeto išlaidų eilutę (-es), kuriai (-oms) daromas poveikis.

[…]

Kitos pastabos (pvz., poveikio pajamoms apskaičiavimo metodas (formulė) arba kita informacija).

[…]

[47] Tradiciniai nuosavi ištekliai (muitai, cukraus mokesčiai) turi būti nurodomi grynosiomis sumomis, t. y. iš bendros sumos atskaičius 20 % surinkimo sąnaudų.