

Kibernetinio saugumo incidentų aptikimas ir reagavimas į juos

ES bendradarbiavimo sistema tobulėja, tačiau dėl vėluojančio įgyvendinimo ir riboto dalijimosi informacija ji tik iš dalies rezultatyvi



EUROPOS
AUDITO
RŪMAI

Turinys

Dalis

01–23 | **Pagrindiniai aspektai** 01

01–07 | Kodėl ši sritis svarbi

08–23 | Ką nustatėme ir rekomenduojame

24–01 | **Mūsų pastabos išsamiau** 02

24–74 | ES kibernetinio saugumo tinklai ir mechanizmai padeda bendradarbiauti ir reaguoti, tačiau dėl riboto dalijimosi informacija ir nebaigto įgyvendinimo mažėja jų rezultatyvumas

24–51 | ES tinklai sudaro sąlygas valstybėms narėms bendradarbiauti, tačiau dėl riboto dalijimosi informacija mažėja jų pridėtinė vertė

52–61 | ES kibernetinio saugumo rezervas sudaro sąlygas sparčiai pasinaudoti reagavimo į incidentus paslaugomis

62–74 | Europos kibernetinio saugumo įspėjimų sistema siekiama pagerinti grėsmių aptikimo pajėgumus, tačiau ji neveikia

75–01 | Pagal Skaitmeninės Europos programą ES finansuojamais projektais siekiama stiprinti kibernetinį saugumą, tačiau susiduriama su įgyvendinimo ir ataskaitų teikimo sunkumais

75–81 | Vėluojama steigti Kibernetinio saugumo kompetencijos bendruomenė negalėjo formuoti Skaitmeninės Europos programos pagal savo poreikius

82–96 | ES finansuojamais projektais siekiama aktualių tikslų, tačiau įgyvendinant daugelį jų susiduriama su veiklos sunkumais

97–01 | Daugumos ES finansuojamų projektų veiklos rezultatų sistemos turi trūkumų, o Skaitmeninės Europos programos kibernetinio saugumo srities veiklos rezultatų duomenys netikslūs

Priedai

I priedas. Apie auditą

II priedas. ES kibernetinio saugumo aplinka

III priedas. Atrinkti kibernetinio saugumo veiksmai

IV priedas. Audito Rūmų atliktas ES finansuojamų kibernetinio saugumo projektų vertinimas

Santrumpos

Žodynėlis

Komisijos atsakymai

Europos kibernetinio saugumo kompetencijos centro (ECCC) atsakymai

Europos Sąjungos kibernetinio saugumo agentūros (ENISA) atsakymai

Chronologija

Audito grupė

01

Pagrindiniai aspektai

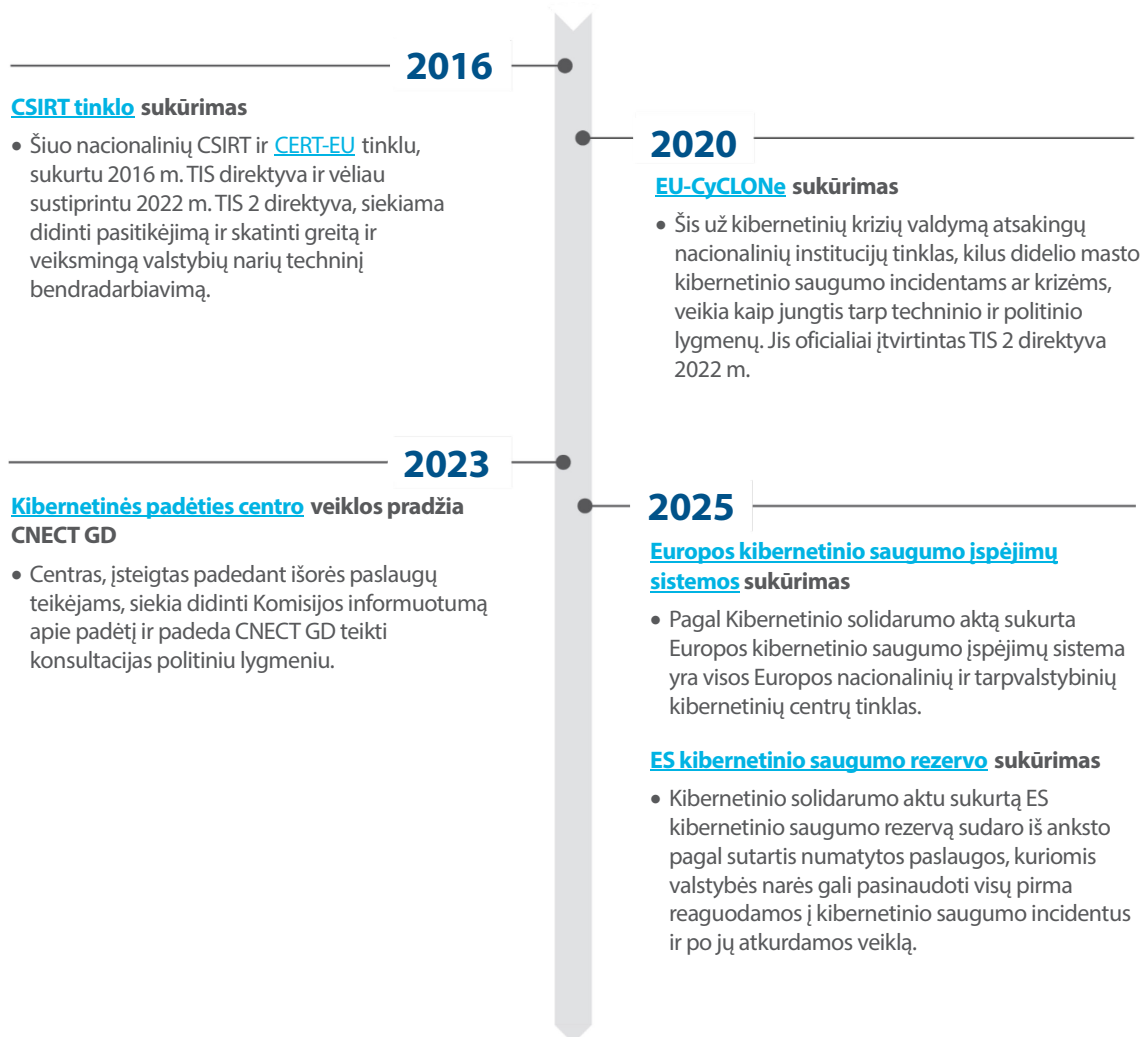
Kodėl ši sritis svarbi

- 01** Ekonomikai ir kasdieniam gyvenimui vis labiau skaitmenėjant didėja kibernetinių išpuolių rizika. Kibernetinis saugumas apibrėžiamas kaip „veikla, būtina tinklų ir informacinėms sistemoms, tokių sistemų naudotojams ir kitiems susijusiems asmenims apsaugoti nuo kibernetinių grėsmių“¹. Kibernetiniam saugumui užtikrinti būtinas visapusiškas požiūris, apimantis kibernetinių grėsmių prevenciją, aptikimą, reagavimą į jas ir veiklos atkūrimą po jų.
- 02** ES kibernetinio saugumo aplinkoje yra daug viešųjų ir privačiųjų subjektų, veikiančių regioniniu, nacionaliniu ir ES lygmenimis civilinėje srityje. Kibernetinis saugumas taip pat yra vienas iš esminių nacionalinio saugumo ir gynybos elementų.
- 03** Valstybėms narėms tenka pagrindinė atsakomybė už joms poveikį darančių kibernetinio saugumo incidentų ir krizių prevenciją, pasirengimą jiems ir reagavimą į juos. Dėl šių incidentų gali sutrikti sklandus vidaus rinkos veikimas, todėl reikšmingo incidento ar krizės atveju svarbus vaidmuo tenka ir Europos Sąjungai. Pastaraisiais metais ES sustiprino savo besiplėtojančią kibernetinio saugumo reguliavimo sistemą² ir sukūrė tinklus bei mechanizmus, parodytus [1 diagramoje](#) ir [II priede](#).

¹ Reglamentas (ES) 2019/881 ([Kibernetinio saugumo aktas](#)).

² Pavyzdžiui, 2025 m. lapkričio mėn. Komisija pasiūlė [Skaitmeninio sektoriaus bendrąjį rinkinį](#), o 2026 m. sausio mėn. – peržiūrėtą [ES kibernetinio saugumo aktą](#).

1 diagrama | ES kibernetinio saugumo tinklai ir mechanizmai 2016–2025 m.



CSIRT – reagavimo į kompiuterių saugumo incidentus tarnyba

CNECT GD – Ryšių tinklų, turinio ir technologijų generalinis direktoratas

EU-CyCLONe – Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas

TIS direktyva – Direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti

TIS 2 direktyva – Direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti

Šaltinis: Audito Rūmai.

- 04** Pagal dabartinę 2021–2027 m. daugiametę finansinę programą pagrindinis kibernetinio saugumo finansavimo šaltinis yra [Skaitmeninės Europos programa](#) (DIGITAL). Jos bendras biudžetas yra 8,1 milijardo eurų, iš kurių 1,4 milijardo eurų skirta kibernetiniam saugumui stiprinti.

- 05** Mūsų audito tikslas buvo įvertinti, ar ES veiksmai rezultatyviai padeda aptikti reikšmingus ir didelio masto kibernetinio saugumo incidentus ir į juos reaguoti. Šiuo tikslu vertinome:
- ES lygmens tinklus ir mechanizmus (t. y. Reagavimo į kompiuterių saugumo incidentus tarnybų tinklą (CSIRT tinklą), Europos ryšių palaikymo dėl kibernetinių krizių organizacinį tinklą (EU-CyCLONe), Europos kibernetinio saugumo įspėjimų sistemą, Kibernetinės padėties centrą ir ES kibernetinio saugumo rezervą);
 - pagal Skaitmeninės Europos programą finansuojamus veiksmus.
- 06** Tikimės, kad mūsų nustatyti faktai padės stiprinti ES kibernetinį atsparumą – dėl jų padidės ES tinklų ir mechanizmų rezultatyvumas ir efektyvumas, taip pat patobulės ES finansuojamų veiksmų atrankos ir stebėsenos būdai.
- 07** Auditas apima 2022–2025 m. laikotarpį. Jis grindžiamas dokumentų peržiūra ir atitinkamų dokumentų analize, audito vizitais trijose valstybės narėse (Airijoje, Graikijoje ir Italijoje), taip pat rašytiniais klausimynais ir interviu su atitinkamais suinteresuotaisiais subjektais. Išsamesnė aiškinamoji informacija ir duomenys apie audito apimtį ir metodą pateikti [I priede](#).

Ką nustatėme ir rekomenduojame

- 08** Apskritai darome išvadą, kad ES veiksmai tik iš dalies padeda aptikti reikšmingus ir didelio masto kibernetinio saugumo incidentus ir į juos reaguoti. Nors bendradarbiavimo sistema buvo nuosekliai kuriama, vis dar dirbama siekiant užtikrinti, kad ji visapusiškai veiktų. Ribotas dalijimasis informacija, pranešimų teikimo trūkumai ir smarkiai vėluojantis įgyvendinimas neleidžia išnaudoti viso ES tinklų ir mechanizmų potencialo. Pagal Skaitmeninės Europos programą finansuojamais projektais siekiama aktualių tikslų, tačiau įgyvendinant kai kuriuos iš jų vėluojama ar susiduriama su veiklos sunkumais, taip pat esama bendros veiklos rezultatų stebėsenos sistemos trūkumų.
- 09** Dabartinė ES tinklų ir mechanizmų sistema, kuria siekiama palengvinti reikšmingų kibernetinio saugumo incidentų aptikimą ir reagavimą į juos, buvo kuriama palaipsniui. 2025 m. Taryba priėmė [Kibernetinio saugumo planą](#), kuriuo nustatyta ES kibernetinių krizių valdymo sistema. Nustatėme, kad Kibernetinio saugumo plane iš esmės paaiškinami su ES kibernetinių krizių valdymu susiję vaidmenys ir atsakomybės sritys. Tačiau dar reikia oficialiai nustatyti procedūrinę tvarką, kaip kartu turėtų veikti CSIRT tinklas (sukurtas 2016 m.) ir EU-CyCLONe (oficialiai įtvirtintas 2023 m.), ([24–30](#) dalys).

- 10** Nustatėme, kad dalijimasis informacija per šiuos tinklus yra ribotas. Tai daugiausia lemia vėlavimas į nacionalinę teisę perkelti [Direktyvą dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti](#) (TIS 2 direktyvą), sunkumai nustatant, ar incidentas turi tarpvalstybinį poveikį, ir nacionalinio saugumo teisės aktai, kuriais neleidžiama dalytis informacija. Tinklų pridėtinė vertė gerokai sumažėja, jeigu valstybės narės nėra linkusios laiku dalytis informacija, kuria remiantis būtų galima imtis veiksmų, ([31–44](#) dalys).



1 rekomendacija

Stiprinti valstybių narių dalijimąsi informacija

Siekdama pagerinti kibernetinio saugumo incidentų aptikimą ir reagavimą į juos, Komisija, padedant Europos Sąjungos kibernetinio saugumo agentūrai (ENISA), turėtų:

- a) pasiūlyti Tinklų ir informacijos apsaugos bendradarbiavimo grupei atlikti išsamią nacionalinio saugumo apribojimų, kuriais varžomas dalijimasis informacija ir daromas poveikis ES kibernetiniam atsparumui, analizę ir pasiūlyti jai nustatyti teisinės bei techninės priemonės, kurios leistų aktyviau dalytis informacija, kartu paisant nacionalinio saugumo ribų;
- b) nedarydama poveikio teisėkūros institucijų sprendimams ir bendradarbiaudama su valstybėmis narėmis, užtikrinti, kad per Skaitmeninio sektoriaus bendrajame rinkinyje siūlomą vieną bendrą prieigą pranešimams apie incidentus teikti būtų galima aptikti galimus tarpvalstybinius incidentus;
- c) kurti sprendinius, kurie sudarytų sąlygas apie incidentus ENISA pranešti tikruoju laiku.

Tikslinė įgyvendinimo data: a ir b – 2027 m., c – 2028 m.

- 11** 2022 m. Komisija įsteigė savo Kibernetinės padėties centrą, kad būtų geriau informuota apie padėtį ir taip galėtų geriau vykdyti jai tenkančias institucines krizių valdymo pareigas. Centro veikla daugiausia užtikrinama sutartiniu pagrindu pasitelkiant išorės paslaugų teikėjus. Nustatėme, kad išorės paslaugų teikėjų atliekamu darbu iš dalies dubliuojami esami Europos Sąjungos kibernetinio saugumo agentūros (ENISA) pajėgumai informuotumo apie padėtį ir grėsmių stebėsenos srityse. Manome, kad steigiant Kibernetinės padėties centrą nebuvo pakankamai išnaudotos racionalizavimo galimybės, t. y. nepakankamai pasinaudota Komisijos ir ENISA jau turima informacija. Be to, nesant išsamaus ir detalaus ateities plano pasibaigus sutarties galiojimui, kyla rizika Kibernetinės padėties centro veiklai po 2026 m. ([45–51](#) dalys).



2 rekomendacija

Racionalizuoti ES informuotumo apie kibernetinio saugumo padėtį pajėgumus ir optimizuoti informacijos sklaidą

Siekdama padidinti efektyvumą, Komisija, bendradarbiaudama su ENISA, turėtų įvertinti galimybes bendrai gauti ir analizuoti informuotumui apie padėtį reikalingą informaciją. Ji taip pat turėtų užtikrinti, kad ši informacija ir susijusios kibernetinių grėsmių ataskaitos būtų prieinamos atitinkamoms ES tarnyboms ir agentūroms.

Tikslinė įgyvendinimo data: 2027 m.

- 12** 2024 m. priimtu [Kibernetinio solidarumo aktu](#) sukuriamas ES kibernetinio saugumo rezervas, kuriuo siekiama padėti valstybėms narėms reaguoti į didelius kibernetinio saugumo incidentus ir po jų atkurti veiklą. Jį sudaro reagavimo į incidentus paslaugos, kurias visą parą gali teikti kiekvienai valstybei narei atrinkti paslaugų teikėjai. Nors tokiu būdu padedama patenkinti konkrečias valstybių narių reikmes ir stiprinti pasitikėjimą, turimos biudžeto lėšos joms padalijamos po lygiai, neatsižvelgiant į konkrečius kiekvienos valstybės narės poreikius, ([52–57](#) dalys).
- 13** Manome, kad pasitelkiant paslaugų teikėjus, su kuriais iš anksto sudarytos sutartys, galima sparčiai pasinaudoti reagavimo į incidentus paslaugomis. ES kibernetinio saugumo rezervas visų pirma skirtas reagavimui ir veiklos atkūrimui remti, tačiau tada, kai jis nenaudojamas reagavimui į incidentus, jis gali būti naudojamas parengčiai. Taikant tokį lankstumą galima užtikrinti, kad iš anksto apmokėtos paslaugos neliktų nepanaudotos. Vis dėlto kyla rizika, kad rezervas, priešingai jo numatytai paskirčiai, daugiausia bus naudojamas parengčiai, o ne reagavimui, ([58–61](#) dalys).
- 14** Europos kibernetinio saugumo įspėjimų sistema yra nacionalinių ir tarpvalstybinių kibernetinio saugumo centrų, kurių tikslas – gerinti kibernetinių grėsmių aptikimą, analizę ir reagavimą į jas, tinklas. Nustatėme, kad dėl labai vėluojančio priemonių ir paslaugų įsigijimo tuo metu, kai atlikome auditą, du centrai (ATHENA ir ENSOC) dar nevykdė veiklos ir dar neveikė Europos kibernetinio saugumo įspėjimų sistema ([62–70](#) dalys).

- 15** Vienas pagrindinių Europos kibernetinio saugumo įspėjimų sistemos tikslų – skatinti prasmingą dalijimąsi informacija valstybių narių grupėse. Tai gali padėti išspręsti kai kuriuos su dalijimusi informacija susijusius klausimus, tačiau kartu yra labai sunku kibernetinio saugumo centrus integruoti į jau ir taip sudėtingą kibernetinio saugumo aplinką. Nustatėme, kad dar nebuvo sudaryti bendradarbiavimo susitarimai, neparengta bendra taksonomija ir sąveikumo standartai, kurių reikia visapusiškam Europos kibernetinio saugumo įspėjimų sistemos veikimui užtikrinti, (**71–74** dalys).



3 rekomendacija

Integruoti Europos kibernetinio saugumo įspėjimų sistemą į ES kibernetinio saugumo aplinką

Komisija kartu su ENISA ir valstybėmis narėmis turėtų užtikrinti, kad būtų sudaryti bendradarbiavimo susitarimai ir nustatyti sąveikumo standartai, kurie palengvintų dalijimąsi informacija tarp Europos kibernetinio saugumo įspėjimų sistemai priklausančių tarpvalstybinių centrų, CSIRT tinklo ir EU-CyCLONe.

Tikslinė įgyvendinimo data: 2028 m.

- 16** 2018 m. Komisija pasiūlė įsteigti Europos kibernetinio saugumo kompetencijos centrą (ECCC), kuris nuo 2021 m. valdytų Skaitmeninės Europos programos kibernetinio saugumo komponentą. [ECCC reglamentu](#) raginama sukurti kibernetinio saugumo kompetencijos bendruomenę, kurią sudarytų pramonės sektoriaus, akademinės bendruomenės ir mokslinių tyrimų organizacijų atstovai. Atrinkti Kibernetinio saugumo kompetencijos bendruomenės nariai vėliau sudarytų Strateginę patariamąją grupę (SPG) (**75** ir **76** dalys).
- 17** Nustatėme vėlavimų ECCC siekiant finansinio savarankiškumo, taip pat steigiant Kibernetinio saugumo kompetencijos bendruomenę ir SPG. Todėl Kibernetinio saugumo kompetencijos bendruomenė ir SPG negalėjo prisidėti rengiant Skaitmeninės Europos programos darbo programas. Tai vertiname kaip neišnaudotą galimybę (**77–81** dalys).
- 18** Nustatėme, kad visais mūsų tikrintais projektais buvo siekiama aktualių tikslų, kuriais prisidedama prie Skaitmeninės Europos programos kibernetinio saugumo tikslų įgyvendinimo. Tačiau nustatėme atvejų, kai kokybė arba pasiekti rezultatai nebuvo patenkinami, daugiausia dėl įgyvendinimo vėlavimų, (**82–87** dalys).

- 19** Skaitmeninės Europos programos reglamente nustatyta, kad saugumo sumetimais kibernetinio saugumo finansavimas gali būti skiriamas tik valstybėse narėse įsisteigusiems subjektams, kuriuos kontroliuoja valstybės narės arba valstybių narių piliečiai. Šį nuosavybės ir kontrolės vertinimą ECCC vardu atlieka [Europos mokslinių tyrimų vykdomosios įstaigos](#) Centrinė patvirtinimo tarnyba ([88–91](#) dalys).
- 20** Finansinės paramos trečiosioms šalims atveju atsakomybė už nuosavybės ir kontrolės vertinimą tenka projektų naudos gavėjams, kurie jį atlieka pagal savo metodą ir metodiką. Nustatėme, kad ECCC netvirtina naudos gavėjų metodikos ir neatlieka patikrų, kad įsitikintų, jog atrinktos trečiosios šalys atitinka reikalavimą dėl ES nuosavybės ir kontrolės. Mūsų vertinimu, kyla didelė rizika, kad naudos gavėjai gali neturėti pajėgumų tinkamai atlikti šių patikrų. Ši rizika nebuvo tinkamai sumažinta ir gali kelti pavojų didesnės rizikos infrastruktūrai, veiklos duomenims ir saugumui svarbioms technologijoms ([92–96](#) dalys).



4 rekomendacija

Užtikrinti patikimą subjektų, kuriems pagal Skaitmeninės Europos programą skiriamas ES finansavimas, nuosavybės ir kontrolės vertinimą

Europos kibernetinio saugumo kompetencijos centras turėtų:

- a) gauti pagrįstą patikinimą, kad naudos gavėjai, atsakingi už finansinės paramos trečiosioms šalims teikimą, turi administracinių ir techninių pajėgumų, reikalingų tinkamai atlikti nuosavybės ir kontrolės vertinimus pagal jiems prieinamą esamą metodiką;
- b) atrankos būdu tikrinti, ar ES finansavimą gauna tik reikalavimus atitinkantys subjektai.

Tikslinė įgyvendinimo data: a – 2026 m., b – 2027 m.

- 21** ES finansuojamus projektus valdantys naudos gavėjai privalo ECCC teikti ataskaitas dėl projektų pažangos ir rezultatų, remdamiesi tarpinėmis reikšmėmis ir teikiniais. Jie yra esminiai projektų stebėsenos elementai ir turėtų būti tinkamai apibrėžti. Nustatėme, kad rengiant beveik visus projektus nebuvo laikomasi nurodymų, kaip parengti tarpines reikšmes ir teikinius, ir kad daugelis jų nebuvo tinkami pažangai stebėti ([97–99](#) dalys).

- 22** Nustatėme, kad daugelis naudos gavėjų naudojamų veiklos rezultatų rodiklių nėra aktualūs ar išmatuojami ir nenustatyta jų siektina ar pradinė reikšmė. Be to, ataskaitose pateikta informacija apie šiuos rodiklius buvo nepakankama, todėl jomis nebuvo galima remtis vertinant projektų veiklos rezultatus ([100–102](#) dalys).
- 23** Siekiant stebėti visos Skaitmeninės Europos programos pasiekimus, visų projektų ataskaitose privaloma pateikti informaciją apie konkrečius programos rodiklius, kuriais remiamasi rengiant Komisijos metines [programos veiklos rezultatų ataskaitas](#). ECCC yra atsakingas už šių rodiklių duomenų rinkimą ir tikrinimą. Nustatėme keletą problemų, susijusių su duomenų rinkimo būdu ir bendra duomenų kokybe. Neradome įrodymų, kad ECCC būtų tikrinęs, ar pateikti duomenys tikslūs. Remdamiesi atrankinėmis patikromis, vertiname, kad pateikti duomenys tiksliai neatspindi pasiektų rezultatų ([103–106](#) dalys).



5 rekomendacija

Stiprinti Skaitmeninės Europos programos kibernetinio saugumo komponento veiklos rezultatų stebėsenos sistemą

Kad būtų sudarytos sąlygos tinkamai pažangos ir veiklos rezultatų stebėsenai, Europos kibernetinio saugumo kompetencijos centras turėtų:

- a) iki dotacijos susitarimo pasirašymo užtikrinti, kad visuose projektuose būtų nustatytos tarpinės reikšmės, teikiniai ir veiklos rezultatų rodikliai, atitinkantys paraiškos formoje pateiktus nurodymus;
- b) sukurti ir įgyvendinti patikimą Skaitmeninės Europos programos kibernetinio saugumo komponento veiklos rezultatų rodiklių duomenų rinkimo, atsekamumo, tikrinimo ir agregavimo sistemą, kad rodikliai tiksliai atspindėtų pasiektus rezultatus.

Tikslinė įgyvendinimo data: 2027 m.

Mūsų pastabos išsamiau

ES kibernetinio saugumo tinklai ir mechanizmai padeda bendradarbiauti ir reaguoti, tačiau dėl riboto dalijimosi informacija ir nebaigto įgyvendinimo mažėja jų rezultatyvumas

ES tinklai sudaro sąlygas valstybėms narėms bendradarbiauti, tačiau dėl riboto dalijimosi informacija mažėja jų pridėtinė vertė

- 24** Dabartinė ES tinklų ir mechanizmų sistema, skirta padėti aptikti reikšmingus kibernetinio saugumo incidentus ir į juos reaguoti, buvo kuriama palaipsniui, pradedant 2016 m. rugpjūčio mėn. įsigaliojusia [Direktyva dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti](#)³ (TIS direktyva). Dabartinė ES kibernetinio saugumo aplinka pavaizduota [II priede](#).

³ Direktyva (ES) 2016/1148.

ES tinklai sudaro sąlygas valstybėms narėms bendradarbiauti techniniu ir operatyviniu lygmenimis

- 25** TIS direktyva sukurtas **CSIRT tinklas**, kurį sudaro **CERT-EU** (Sajungos institucijų, įstaigų, organų ir agentūrų kibernetinio saugumo tarnyba) ir valstybių narių paskirtos CSIRT. Šio tinklo tikslas – stiprinti nacionalinių CSIRT tarpusavio pasitikėjimą ir atsakomybę ir skatinti greitą ir rezultatyvų valstybių narių operatyvinį bendradarbiavimą.
- 26** **EU-CyCLONe** įsteigtas 2020 m. kaip neformalus už kibernetinių krizių valdymą atsakingų nacionalinių institucijų bendradarbiavimo tinklas. Jis veikia kaip jungtis tarp techninio lygmens, kuriame veikia CSIRT tinklas, ir politinio lygmens, kuriame veikia Europos Sąjungos Taryba bei jos **integruoto politinio atsako į krizes** mechanizmas. 2023 m. įsigaliojus TIS 2 direktyvai, EU-CyCLONe vaidmuo oficialiai įtvirtintas ir jam suteikti aiškūs įgaliojimai.
- 27** Vertiname, ar šių ES lygmens tinklų vaidmenys ir atsakomybės sritys tinkamai apibrėžti ir ar jie sudaro sąlygas valstybėms narėms bendradarbiauti.
- 28** **ENISA** atlieka CSIRT tinklo ir EU-CyCLONe sekretoriato funkcijas ir teikia jiems bendradarbiavimui bei saugiam ryšiui dalijantis informacija reikalingus išteklius, ekspertines žinias, infrastruktūrą ir IT priemones. 2025 m. pradžioje atliktoje suinteresuotųjų subjektų pasitenkinimo apklausoje⁴ ENISA veikla atliekant šių tinklų sekretoriato funkcijas įvertinta aukštais balais. Šie teigiami atsiliepimai pasitvirtino ir per mūsų audito vizitus, kurių metu nacionalinės kibernetinio saugumo institucijos palankiai įvertino šią ENISA veiklą.
- 29** 2025 m. Taryba priėmė **Kibernetinio saugumo planą**, kuriame apibrėžiami pagrindinių subjektų (įskaitant CSIRT tinklą ir EU-CyCLONe) vaidmenys ir atsakomybės sritys, taip pat mechanizmai, susiję su didelio masto kibernetinio saugumo incidentais ar kibernetinėmis krizėmis. Nustatėme, kad Kibernetinio saugumo plane iš esmės paaiškinami su ES kibernetinių krizių valdymu susiję vaidmenys ir atsakomybės sritys ir atsižvelgiama į aplinkos pokyčius nuo pirmojo plano priėmimo 2017 m. Jame nustatomi trys bendradarbiavimo lygmenys: techninis, operatyvinis ir politinis; išsamiai aprašomi nuo 2017 m. sukurti nauji tinklai ir struktūros, kaip antai EU-CyCLONe, ES greitojo reagavimo į hibridines grėsmes grupės ir Europos kibernetinio saugumo įspėjimų sistema, taip pat aptariama, kaip kibernetinių krizių valdymas turėtų būti integruotas į platesnę ES reagavimo į krizes sistemą.

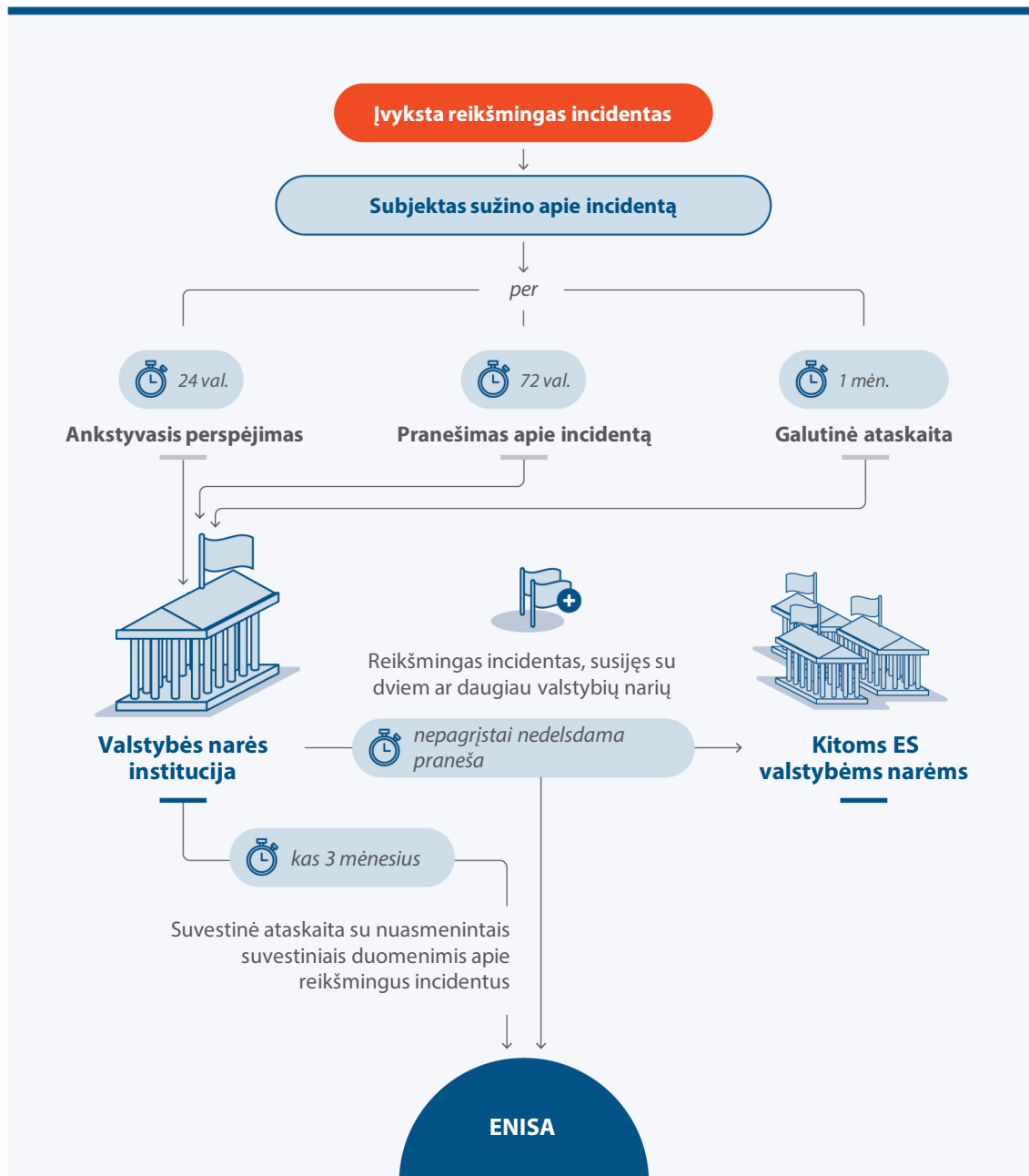
⁴ ENISA 2024 m. konsoliduotoji metinė veiklos ataskaita, p. 33 ir 36.

- 30** Tačiau, nepaisant to, kad CSIRT tinklas oficialiai sukurtas 2016 m., o EU-CyCLONe – 2023 m., abu tinklai dar turi oficialiai įforminti procedūrinę tvarką, pagal kurią jie turėtų veikti kartu. Jie taip pat nėra sutarę dėl kriterijų, pagal kuriuos CSIRT tinklas turėtų pranešti EU-CyCLONe, kad pastebėtas kibernetinio saugumo incidentas laikytinas galimu arba vykstančiu didelio masto kibernetinio saugumo incidentu. Abu tinklai taip pat turi susitarti dėl bendros incidentų sunkumo lygių ir pagrindinių sąvokų, kaip antai „grėsmė“, „priešiškasis subjektas“, „incidentas“ ar „poveikis“, taksonomijos, kuri būtina automatizuotam keitimuisi informacija užtikrinti. Šiuo metu galima įvairiai aiškinti, kada incidentas laikytinas reikšmingu ar didelio masto incidentu. Tai, kad nėra bendros taksonomijos, paminėjo visų trijų mūsų apklauktų valstybių narių kibernetinio saugumo institucijos.

Dėl riboto dalijimosi informacija ir pranešimų teikimo trūkumų gerokai mažėja šių tinklų pridėtinė vertė

- 31** Geografinės sienos neužkerta kelio kibernetinio saugumo incidentams ir kibernetiniams išpuoliams kilti ir plisti. Valstybių narių dalijimasis informacija, pavyzdžiui, apie priešiško subjekto taikomas taktikas ir metodus, taip pat apie skaitmeninius požymius, rodančius, kad į tinklą ar informacinę sistemą buvo įsilaužta, (užvaldymo rodikliai), gali reikšmingai prisidėti prie kibernetinio saugumo didinimo.
- 32** Nustatėme, kad dalijimasis informacija buvo ribotas, o tai gerokai sumažino šių tinklų pridėtinę vertę. Mūsų pastebėti trūkumai daugiausia susiję su vėlavimu į nacionalinę teisę perkelti TIS 2 direktyvą, sunkumais siekiant nustatyti, ar incidentas turi tarpvalstybinį poveikį, nacionalinio saugumo teisės aktais, kuriais ribojamas dalijimasis informacija, ir pasitikėjimo stoka. TIS 2 direktyvoje nustatyta keletas pranešimų teikimo reikalavimų į jos taikymo sritį patenkančioms subjektams ir valstybių narių institucijoms, kaip parodyta [2 diagramoje](#).

2 diagrama | Pranešimų apie incidentus teikimo terminai pagal Direktyvą dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje ES užtikrinti (TIS 2 direktyvą)



Šaltinis: Audito Rūmai, remiantis ENISA.

- 33** Valstybės narės į nacionalinę teisę [TIS 2 direktyvą turėjo perkelti](#) iki 2024 m. spalio mėn., tačiau šio termino laikėsi tik dvi valstybės narės. Vėluojant tai padaryti daromas didelis poveikis dalijimuisi informacija, nes, kol TIS 2 direktyva neperkelta, subjektai, kuriems ji taikoma, apie incidentus teisiškai pranešti neprivalo. Komisija skaičiavimais⁵, TIS direktyva taikoma 15 500 subjektų, o į TIS 2 direktyvos taikymo sritį patenka daugiau kaip 110 000 subjektų. Pavyzdžiui, viešojo administravimo sektorius (dažniausias išpuolių Europos Sąjungoje taikinyis pagal ENISA 2025 m. [grėsmių padėties ataskaitą](#)) pagal TIS direktyvą apie incidentus neprivalėjo pranešti.
- 34** Teikiant duomenis apie incidentus agentūrai ENISA kas tris mėnesius (t. y. praėjus daug laiko po to, kai incidentas galėjo įvykti) ribojama jų pridėtinė vertė. Šie duomenys daugiausia naudojami statistikos tikslais ir ankstesnėms tendencijoms analizuoti, o ne aptikimui ir reagavimui pagerinti. ENISA suteikia valstybėms narėms [internetinę priemonę](#) pranešimams teikti. Pranešimo šablone pateikiamas būtiniausių duomenų, kuriuos reikia pateikti, rinkinys, pavyzdžiui, incidento rūšis ir susijęs sektorius. Be to, ENISA siūlo valstybėms narėms pateikti papildomos informacijos, kad būtų galima atlikti išsamesnę duomenų analizę, pavyzdžiui, susiejant incidentus su konkrečiais pažeidžiamumo aspektais. Tačiau ne visos valstybės narės nusprendžia šią informaciją pateikti, todėl labai sumažėja renkamų duomenų kokybė ir pridėtinė vertė.
- 35** [2024 m. ataskaitoje dėl kibernetinio saugumo padėties ES](#) ENISA nurodė, kad veikiausiai pranešama ne apie visus incidentus, nes incidentų, apie kuriuos pranešta, skaičius yra nedidelis. 2018–2021 m. valstybės narės ENISA kasmet pranešdavo apie 100–500 incidentų. Šis skaičius palaipsniui didėjo ir 2024 m. išaugo iki 1 276⁶.

⁵ Europos Komisija, 2020 m. [poveikio vertinimo ataskaita](#).

⁶ [CIRAS](#) 2024 m. duomenys.

- 36** 2025 m. [grėsmių padėties ataskaitoje](#), apimančioje laikotarpį nuo 2024 m. birželio mėn. Iki 2025 m. birželio mėn., ENISA nurodė, kad naudodamasi atvirųjų šaltinių žvalgybos informacija, pavyzdžiui, naujienų straipsniais, ji nustatė apie 4 800 kibernetinio saugumo incidentų⁷. Ne apie visus šiuos incidentus būtų reikėję pranešti pagal TIS 2 direktyvą, tačiau rinkdama duomenis ENISA apėmė platesnį incidentų spektrą. Kita vertus, atvirųjų šaltinių žvalgybos informacijoje apie daugelį reikšmingų incidentų nepranešama. Kadangi valstybių narių pateikti duomenys yra nuasmeninti, ENISA negali nustatyti incidentų susieti su valstybių narių praneštais incidentais. Todėl neįmanoma tiksliai nustatyti nepakankamo pranešimo masto, tačiau manome, kad skirtumas tarp valstybių narių praneštų incidentų skaičiaus ir grėsmių padėties ataskaitoje nurodyto skaičiaus rodo, kad pranešama ne apie visus reikšmingus incidentus.
- 37** Kitas nepakankamo pranešimo požymis – pranešimų kitoms paveiktoms valstybėms narėms ir ENISA apie reikšmingus tarpvalstybinius incidentus skaičius. Panašus reikalavimas buvo nustatytas TIS direktyvoje, tačiau buvo laikomas neveiksmingu, nes 2020 m. Komisija padarė išvadą⁸, kad, nepaisant tokios pareigos, pranešimai buvo siunčiami retai. Nepranešimą ji susiejo su tuo, kad nėra aiškių dalijimosi informacija sąlygų ir bendrų tikslų, kuriais būtų skatinamas dalijimasis informacija.
- 38** Pareiga informuoti kitas valstybes nares yra labai svarbi siekiant užkirsti kelią incidentams plisti – to nedarant neigiamai veikiamas ES kibernetinis saugumas. 2025 m. septynios valstybės narės pranešė vos apie 14 reikšmingų tarpvalstybinių incidentų. 2024 m. valstybės narės pateikė du pranešimus apie tarpvalstybinį poveikį galinčius turėti incidentus, 2023 m. – nė vieno, o 2022 m. – tris. Tai rodo, kad apie reikšmingus tarpvalstybinius incidentus pranešama labai retai ir tai neatspindi tikrojo tokių išpuolių masto. Pavyzdžiui, [2024 m. grėsmių padėties ataskaitoje](#) ENISA nustatė 322 incidentus, konkrečiai nukreiptus prieš dvi ar daugiau valstybių narių. Prieš bendrovę „Collins Aerospace“ nukreiptas incidentas (žr. [1 langelį](#)) yra pavyzdys, kai valstybės narės nepraneša apie incidentą, nors jis turi didelį tarpvalstybinį poveikį.

⁷ ENISA [2025 m. grėsmių padėties ataskaita](#).

⁸ Europos Komisija, 2020 m. [poveikio vertinimo ataskaita](#).

1 langelis

Kibernetinio saugumo incidentas sutrikdė oro uostų veiklą

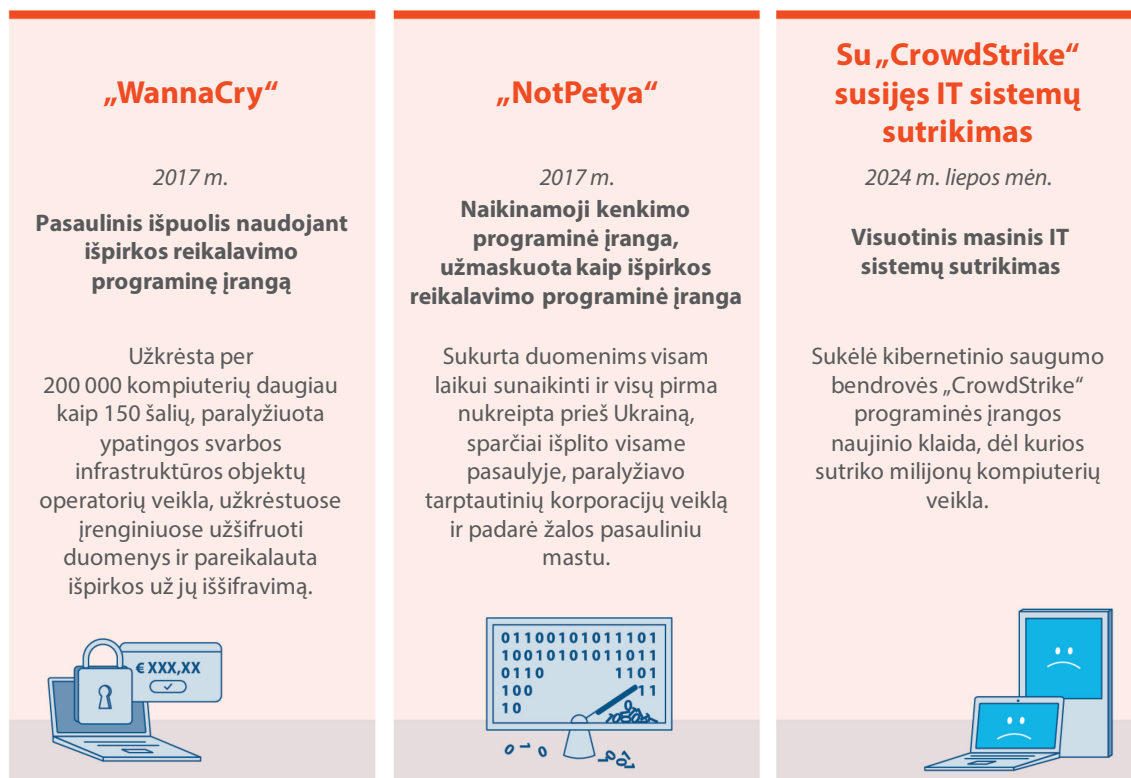
2025 m. rugsėjo mėn. bendrovė „Collins Aerospace“, viena didžiausių aviacijos pramonės technologijų tiekėjų, patyrė didelį išpuolį naudojant išpirkos reikalavimo programinę įrangą, nukreiptą prieš jos keleivių duomenų tvarkymo programinę įrangą. Dėl šio išpuolio didieji Europos oro uostai buvo priversti grįžti prie rankiniu būdu atliekamų operacijų, todėl skrydžiai buvo dažnai atidedami ar atšaukiami. Labiausiai sutrikdyta Londono Hitrou, Briuselio, Berlyno Brandenburgo ir Dublino oro uostų veikla.

Pagal TIS 2 direktyvą incidentas laikomas reikšmingu, jei dėl jo atitinkamas subjektas, be kita ko, patiria didelių paslaugų teikimo sutrikimų arba finansinių nuostolių. Tačiau nė viena valstybė narė šio incidento nelaikė reikšmingu arba didelio masto tarpvalstybiniu incidentu. Taigi nė viena iš paveiktų valstybių narių apie incidentą oficialiai nepranešė ENISA ar kitoms valstybėms narėms. CSIRT tinklas nekonsultavo EU-CyCLONE, todėl pastarasis nepadėjo koordinuotai valdyti incidento.

Šaltinis: Audito Rūmų analizė, pagrįsta interviu su ENISA darbuotojais.

- 39** Kita riboto pranešimo apie tarpvalstybinius incidentus priežastis yra ta, kad pareiga išsiaiškinti, ar praneštas incidentas turi tarpvalstybinį poveikį, ir nustatyti kitas paveiktas valstybes nares tenka kiekvienos valstybės narės institucijai. Remdamasis turima informacija, pranešimą teikiantis subjektas arba valstybės narės institucija gali nežinoti apie tarpvalstybinį kai kurių išpuolių pobūdį. Šiuo metu nėra ES masto platformos, kuri tikruoju laiku gautų visų valstybių narių pranešimus apie incidentus ir galėtų susieti informaciją apie sektorius ar užvaldymo rodiklius, kad būtų galima aptikti tarpvalstybinius incidentus. Todėl kyla didelė rizika, kad kai kurie tarpvalstybiniai incidentai gali būti nenustatyti ir apie juos gali būti nepranešta.
- 40** Nuo 2016 m. nebuvo kibernetinio saugumo incidento, kurį bent viena valstybė narė būtų laikiusi didelio masto incidentu. Iš esmės bet koks incidentas, kuris daro didelį poveikį bent dviem valstybėms narėms, patenka į šios sąvokos apibrėžtį. Vis dėlto net tokie kibernetinio saugumo incidentai, kurie sukėlė pasaulinius trikdžius ir didelę žalą, kaip parodyta [3 diagramoje](#), nebuvo laikomi didelio masto incidentais. Taigi EU-CyCLONE problemų sprendimo procedūra visa apimtimi niekada nebuvo aktyvuota dėl didelio masto kibernetinio saugumo incidento.

3 diagrama | Reikšmingų kibernetinio saugumo incidentų pavyzdžiai



Šaltinis: Audito Rūmai, pritaikyti „Cloudflare“, ENISA, Europolo, „Wired“, IBM, „CrowdStrike“ duomenys.

- 41 Be subjektams ir valstybėms narėms nustatytos pareigos pranešti, siekiant palengvinti dalijimąsi informacija buvo sukurtas CSIRT tinklas. Valstybių narių tarpusavio pasitikėjimas yra šio tinklo, kuriame informacija dalijamasi savanoriškai, pagrindas. Jeigu valstybės narės nėra linkusios laiku dalytis įveiklinamąja informacija, tinklo pridėtinė vertė gerokai sumažėja.
- 42 Dalijimąsi informacija ES lygmeniu riboja kiekvienos valstybės narės nacionalinio saugumo teisės aktai. Jei valstybė narė su kibernetiniu išpuoliu susijusią informaciją apie ypatingos svarbos subjektą vertina kaip įslaptintą arba mano, kad pranešimas apie konkretų incidentą pakenktų jos nacionaliniam saugumui, ji tokia informacija dalytis neprivalo. Mūsų vizitų į valstybes nares metu CSIRT tinklo ir EU-CyCLONE atstovai nurodė, kad informacija gali būti dalijamasi tik tiek, kiek leidžiama pagal nacionalinio saugumo teisės aktus. ES lygmeniu valstybių narių nacionalinių teisinių sistemų ir jų poveikio dalijimuisi informacija analizė nebuvo atlikta.

- 43** 2016 m. CSIRT tinklą sudarė 28 nacionalinės CSIRT; kiekviena valstybė narė turėjo po du atstovus. Nepakankamas dalijimasis informacija buvo nuolatinė problema; [Komisijos atliktame TIS direktyvos vertinime](#) pripažinta, kad „valstybės narės sistemiškai nesidalija informacija viena su kita“, o tai visų pirma neigiamai paveikia kibernetinio saugumo priemonių rezultatyvumą ir bendro informuotumo apie padėtį ES lygmeniu lygį. Daugelis valstybių narių pagal TIS 2 direktyvą paskyrė ne tik nacionalines CSIRT, bet ir sektorių CSIRT, todėl tinklas gerokai išsiplėtė. Audito metu jį sudarė 42 CSIRT ir daugiau kaip 700 atskirų dalyvių. Dėl to stiprinti pasitikėjimą tampa dar sudėtingiau, nes palaikyti glaudžius ryšius tarp visų narių yra sudėtinga.
- 44** CSIRT tinkle žinoma apie dalijimosi informacija problemą ir svarstomi įvairūs veiksmai, kaip stiprinti pasitikėjimą augančiame tinkle. Mažesnės valstybių narių grupės, steigiančios tarpvalstybinius centrus, kaip išsamiau aprašyta [62–74](#) dalyse, yra alternatyva ES masto tinklui, kuri galėtų padėti spręsti šią problemą.

Kibernetinės padėties centro užsakomosios paslaugos iš dalies dubliuoja esamus pajėgumus ir nėra aiški jo veiklos ateitis

- 45** Pagal TIS 2 direktyvą, tais atvejais, kai galimas arba vykstantis didelio masto kibernetinio saugumo incidentas turi arba gali turėti didelį poveikį, Komisija tampa EU-CyCLONe nare⁹. Atsižvelgdama į šį naują vaidmenį ir kintančią grėsmių padėtį, 2022 m. Komisija Ryšių tinklų, turinio ir technologijų generaliniame direktorate (CNECT GD) įsteigė Kibernetinio koordinavimo darbo grupę. Šiai darbo grupei priklauso Kibernetinės padėties centras; jis turėtų padėti Komisijai didinti informuotumą apie padėtį ir taip padėti jai vykdyti institucines krizių valdymo pareigas. Jis taip pat turėtų padėti CNECT GD teikti konsultacijas politiniu lygmeniu.

⁹ [TIS 2 direktyvos](#) 16 straipsnio 2 dalis.

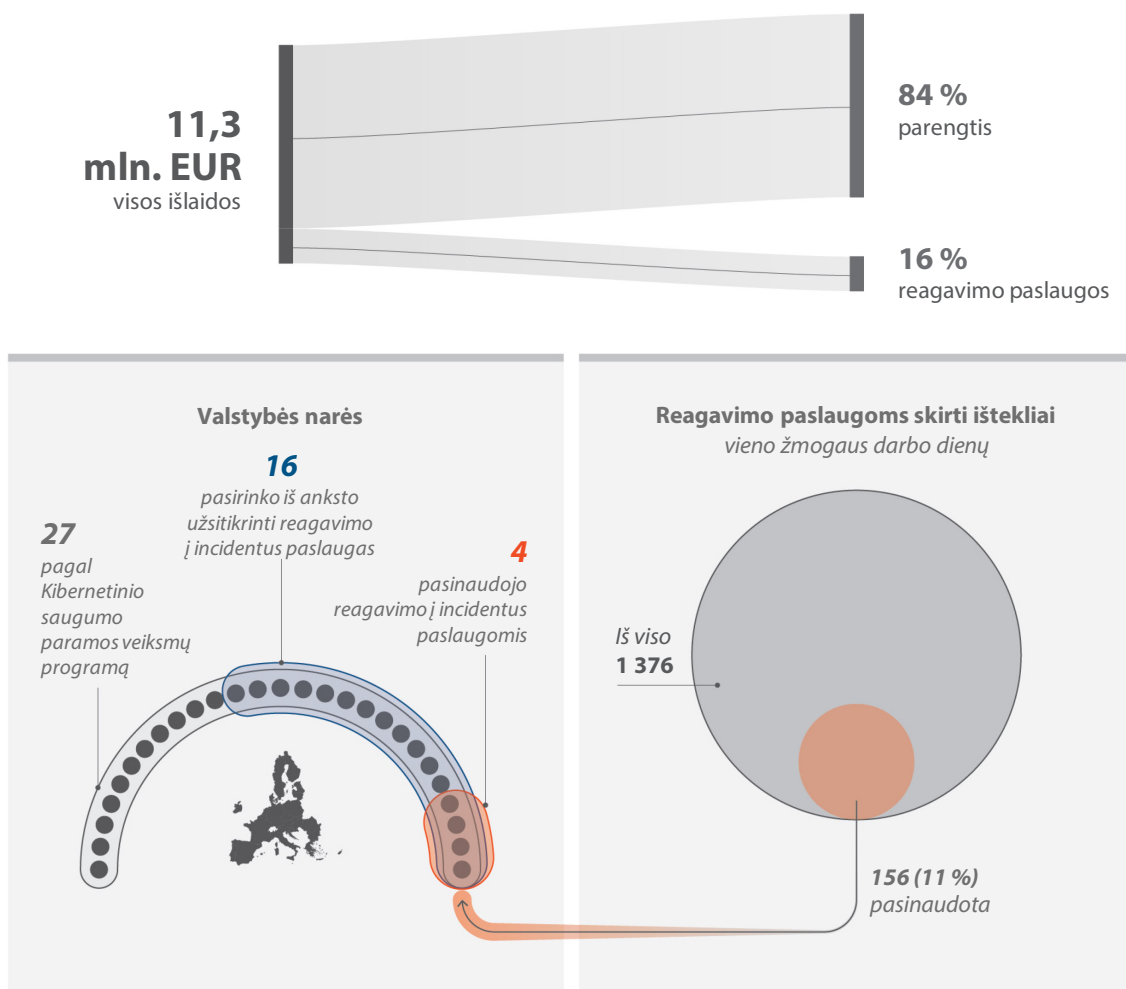
- 46** Steigdamą Kibernetinės padėties centrą Komisija daugiausia remiasi išorės paslaugų teikėjais: 2022 m. gruodžio mėn. su jais sudarytos beveik 18 milijonų eurų vertės ketverių metų [sutartys](#). Įvertinome centro įsteigimą, išdirbius ir Komisijos planus dėl jo veiklos ateities.
- 47** Teikdami paslaugas rangovai sukūrė informacijai apie grėsmes teikti ir ją dalytis skirtą duomenų suvestinę, grindžiamą komerciniais kibernetinių grėsmių žvalgybos duomenų kanalais. Jie taip pat rengia įvairias kibernetinių grėsmių žvalgybos ataskaitas, įskaitant dienos ir savaitės ataskaitas, taip pat temines ataskaitas apie valstybes ar ekonomikos sektorius. Viena iš Komisijos pastatų įrengtas fizinis kibernetinės padėties centras – patalpa, kurioje įrengtos kompiuterizuotos darbo vietos, nuotoliniu būdu prijungtos prie rangovų prieglobos aplinkoje veikiančios duomenų suvestinės. Tuo metu, kai buvo atliekamas auditas, Kibernetinės padėties centre dirbo nedaug Komisijos darbuotojų, kuriems talkino daug rangovų analitikų ir ENISA ekspertai.
- 48** Nustatėme, kad išorės paslaugų teikėjų Kibernetinės padėties centrui atliekamu darbu iš dalies dubliuojami esami ENISA pajėgumai. ENISA turi nuolatinius informuotumo apie padėtį ir grėsmių stebėsenos pajėgumus. Ji reguliariai skelbia kibernetinių grėsmių ataskaitas, įskaitant skubias ataskaitas dėl konkrečių incidentų, ir savaitės ataskaitas, kuriose pateikiama grėsmių apžvalga. Ataskaitos grindžiamos atvirųjų šaltinių žvalgybos informacija ir yra panašios į rangovų rengiamas ataskaitas. Be to, krizės metu ENISA rengia arba padeda rengti politikos formuotojams skirtus aukšto lygio informacinius dokumentus, panašius į Kibernetinės padėties centro rengiamas ataskaitas.
- 49** Be to, duomenys, kuriuos Kibernetinės padėties centras naudoja šioms ataskaitoms rengti, yra grindžiami komerciniais kibernetinių grėsmių žvalgybos duomenų kanalais ir yra panašūs į duomenis, kuriuos naudoja kiti Komisijos padaliniai, pavyzdžiui, Skaitmeninių paslaugų generalinis direktoratas, taip pat CERT-EU. Manome, kad steigiant Kibernetinės padėties centrą nebuvo pakankamai išnaudotos racionalizavimo galimybės, t. y. nepakankamai pasinaudota Komisijos ir ENISA jau turima informacija.
- 50** Sutarties galiojimas baigsis 2026 m. gruodžio mėn., paskui rangovai Kibernetinės padėties centrui paslaugų nebeteiks. Šios paslaugos apima į suvestinę įtraukiamų duomenų teikimą ir grėsmių ataskaitų rengimą ir sudaro didžiąją centro veiklos dalį. Suvestinė bus perduota Komisijai, tačiau ji neteks pridėtinės vertės, jei nebus nuolat pildoma nauja kibernetinių grėsmių žvalgybos informacija.
- 51** Tuo metu, kai buvo atliekamas auditas, Komisija neturėjo planų dėl išorės paslaugų teikėjų paramos Kibernetinės padėties centro veiklai, pasibaigus sutarties galiojimui. Mūsų vertinimu, nesant išsamaus ir detalaus ateities plano pasibaigus sutarties galiojimui, kyla rizika Kibernetinės padėties centro veiklai po 2026 m.

ES kibernetinio saugumo rezervas sudaro sąlygas sparčiai pasinaudoti reagavimo į incidentus paslaugomis

- 52** 2022 m., iškart po Rusijos karinės agresijos prieš Ukrainą, pripažindama, kad didelio masto kibernetiniai išpuoliai tapo dažnesni, Komisija suteikė ENISA 15 milijonų eurų išimtinį finansavimą 2023 m. pradėtiems kibernetinio saugumo paramos veiksmams išbandyti. 2023 m. Komisija skyrė papildomą finansavimą (apie 20 milijonų eurų), kad programa būtų pratęsta iki 2026 m. pabaigos.
- 53** Kad būtų pasirengta didelio masto kibernetinio saugumo incidentams, Komisija taip pat pasiūlė Kibernetinio solidarumo aktą; jis priimtas 2024 m. gruodžio mėn. Šiuo aktu sukuriamas ES kibernetinio saugumo rezervas, kurį sudaro patikimų paslaugų teikėjų reagavimo į incidentus paslaugos. Nuo 2025 m. jis pradėjo palaipsniui veikti; 2025–2027 m. laikotarpiui jam skirtas 36 milijonų eurų biudžetas.
- 54** Vertiname, kaip buvo organizuota Kibernetinio saugumo paramos veiksmų programa, nes ji yra ES kibernetinio saugumo rezervo pagrindas. Taip pat tikrinome, ar kuriant ES kibernetinio saugumo rezervą buvo pasinaudota nuo 2022 m. įgyta patirtimi.
- 55** Kibernetinio saugumo paramos veiksmų programą ENISA sukūrė kaip mechanizmą, skirtą teikti paslaugoms, kuriomis remiama valstybių narių parengtis didelio masto kibernetinio saugumo incidentams ar krizėms ir reagavimas į juos. ENISA iš anksto sudaro sutartis dėl visų paslaugų, tai reiškia, kad paslaugų teikėjai gali pradėti dirbti iš karto, kai tik valstybės narės paprašo jas suteikti. Tą lemia ir ENISA veiklos organizavimas: užtikrinama, kad visą parą budėtų pareigūnas, atsakingas už valstybių narių prašymų nagrinėjimą.
- 56** ENISA nusprendė turimą biudžetą valstybėms narėms paskirstyti po lygiai. Praktiškai agentūra paskelbė atvirą konkursą, suskirstytą į 27 pirkimo dalis – po vieną kiekvienai valstybei narei, – kad atrinktų ne daugiau kaip po tris privačius saugumo paslaugų teikėjus, kurie teiktų paslaugas iki 2026 m. pabaigos. Be to, kai kuriuos paslaugų teikėjus ENISA atrinko pagal Europos masto pirkimo dalį, kad šie teiktų paslaugas reikalavimus atitinkančioms ES nepriklausančioms valstybėms, taip pat ES institucijoms, organams ir agentūroms arba padėtų reaguoti į tarpvalstybinius incidentus.
- 57** Taikydama tokį metodą ENISA galėjo atsižvelgti į konkrečius nacionalinius reikalavimus, įskaitant reikalavimus dėl kalbos, nacionalinių patikimumo pažymėjimų arba įsisteigimo valstybėse narėse. Kita vertus, kadangi paslaugų teikėjai nebuvo atrinkti taip, kad galėtų teikti paslaugas visoje ES, didelis šio metodo trūkumas yra tas, kad valstybei narei nepasinaudojus paslaugomis, dėl kurių iš anksto sudarytos sutartys, tokioms paslaugoms konkrečiai valstybei narei įsipareigota biudžeto suma negali būti naudojama padėti kitai valstybei narei.

- 58** Pagal Kibernetinio saugumo paramos veiksmų programą valstybės narės galėjo rinktis parengties ar reagavimo paslaugas arba abiejų rūšių paslaugų derinį. Valstybės narės turimas lėšas visų pirma rinkosi naudoti parengčiai gerinti (84 % išlaidų 2023 m.). Valstybės narės, pasirinkusios sudaryti susitarimą dėl reagavimo į incidentus paslaugų teikimo kilus poreikiui, t. y. iš anksto apibrėžtą susitarimą su paslaugų teikėju, kuriuo valstybei narei užtikrinama galimybė pasinaudoti paslaugų teikėjo paslaugomis, kad būtų skubiai reaguojama į kibernetinio saugumo incidentus, tokia galimybe naudojosi retai (žr. 4 diagramą). Trijose aplankytose valstybėse narėse institucijos pareiškė palankiai vertinančios tai, kaip ENISA valdo Kibernetinio saugumo paramos veiksmų programą.

4 diagrama | ENISA kibernetinio saugumo paramos veiksmų programa iki 2023 m.



Šaltinis: Audito Rūmai, remiantis ENISA duomenimis.

- 59** 2024–2026 m. laikotarpiu tik devynios valstybės narės paprašė sudaryti susitarimą dėl reagavimo į incidentus paslaugų teikimo kilus poreikiui. Mūsų pokalbiai su ENISA ir trijų valstybių narių institucijomis patvirtino, kad pirmenybė tvirtai teikiama parengties veiklai.
- 60** Nors ES kibernetinio saugumo rezervas visų pirma skirtas remti reagavimui į didelius kibernetinio saugumo incidentus ir veiklos atkūrimui po jų, pagal šį rezervą iš anksto įsipareigosios teikti reagavimo į incidentus paslaugos, kuriomis nepasinaudota, gali būti pakeistos parengties paslaugomis. Taikant tokį lankstumą galima užtikrinti, kad iš anksto apmokėtos paslaugos neliktų nepanaudotos.
- 61** Manome, kad pasirinktas ES kibernetinio saugumo rezervo modelis grindžiamas patirtimi, įgyta įgyvendinant Kibernetinio saugumo paramos veiksmų programą. Tačiau duomenys apie naudojamą Kibernetinio saugumo paramos veiksmų programą leidžia įžvelgti riziką, kad ES kibernetinio saugumo rezervas, priešingai Kibernetinio solidarumo akte nustatytam tikslui, gali būti visų pirma naudojamas parengčiai, o ne reagavimui.

Europos kibernetinio saugumo įspėjimų sistema siekiama pagerinti grėsmių aptikimo pajėgumus, tačiau ji neveikia

- 62** Vienas pagrindinių Europos kibernetinio saugumo įspėjimų sistemos tikslų – skatinti prasmingą dalijimąsi informacija, kad būtų geriau aptinkamos ir analizuojamos kibernetinės grėsmės ir į jas reaguojama. Dalyvavimas įspėjimų sistemoje yra savanoriškas, tačiau valstybės narės, nusprendusios prisijungti prie tarpvalstybinio kibernetinio saugumo centro, turi įsipareigoti dalytis atitinkama informacija su kitais jo nariais. Dirbdamos grupėse patikimoje ir saugioje aplinkoje, valstybės narės galėtų išvengti kai kurių su dalijimusi informacija susijusių problemų, nustatytų [31–44](#) dalyse.
- 63** Audito metu prisijungti prie Europos kibernetinio saugumo įspėjimų sistemos buvo nusprendusios 13 valstybių narių; įsteigti du tarpvalstybiniai centrai: ATHENA ir ENSOC. Be to, skirtas finansavimas 2026 m. steigti trečiam tarpvalstybiniam kibernetinio saugumo centrui – NBCC. Taigi tinklo narių skaičius iš viso padidėjo iki 20 valstybių (18 valstybių narių, taip pat Islandija ir Norvegija¹⁰), kaip parodyta [5 diagramoje](#).

¹⁰ Asocijuotosios ES nepriklausančios valstybės pagal Reglamento (ES) 2021/694 10 straipsnio 1 dalies a punktą.

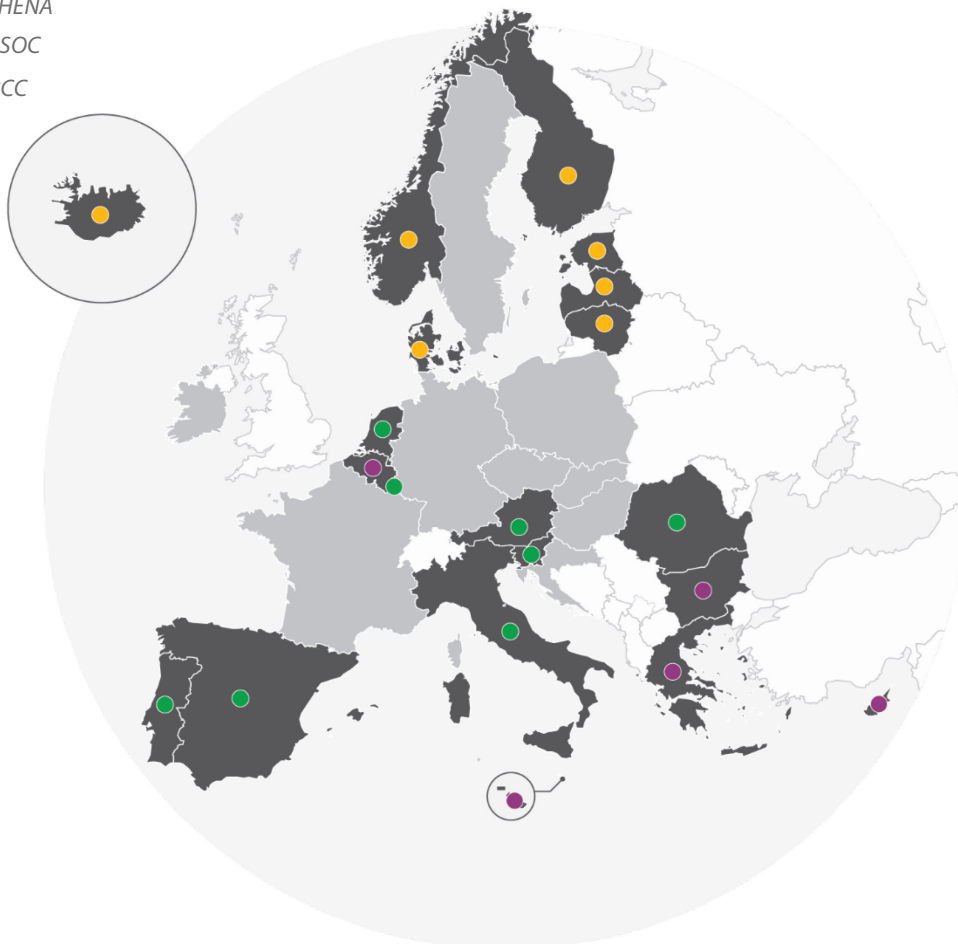
5 diagrama | Europos kibernetinio saugumo įspėjimų sistemoje dalyvaujančios valstybės

■ Europos kibernetinio saugumo įspėjimų sistemoje dalyvaujančios valstybės

● ATHENA

● ENSOC

● NBCC



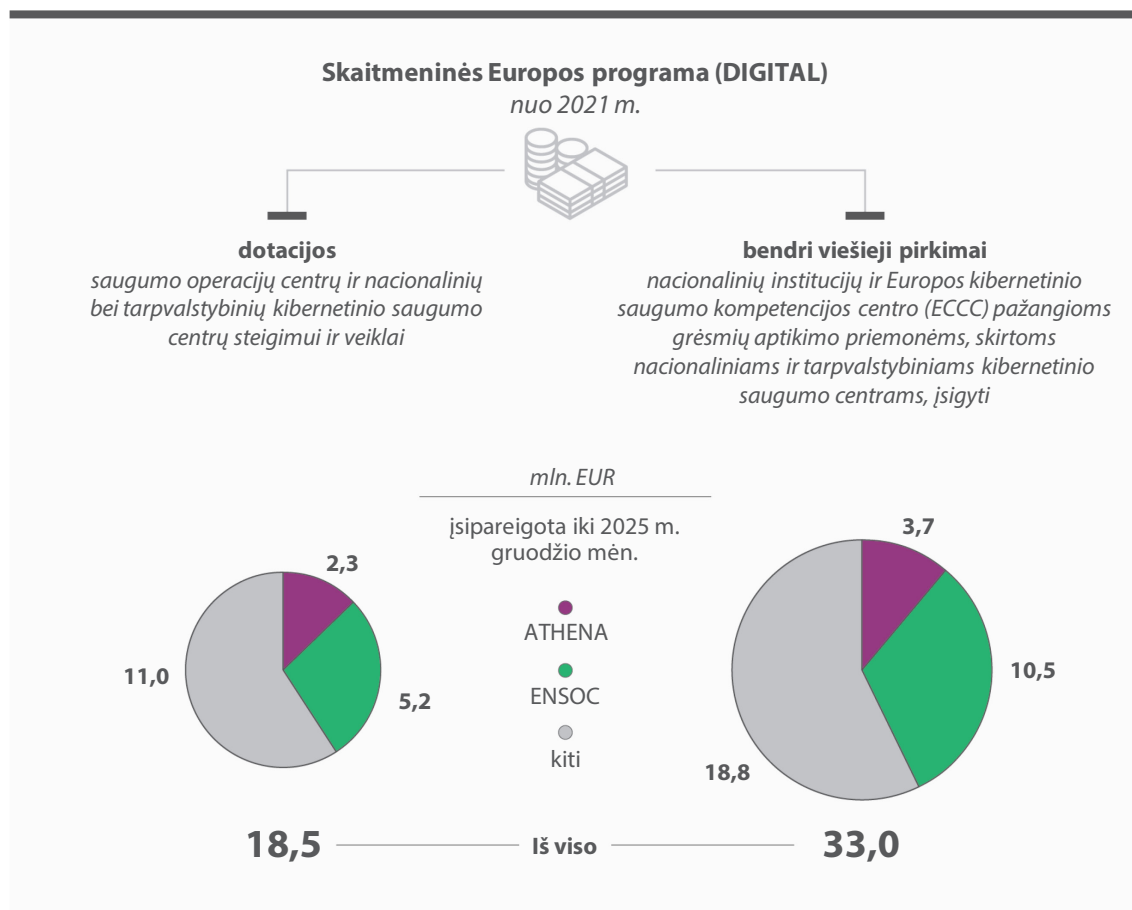
Šaltinis: Audito Rūmai.

- 64** Vertiname, kaip buvo įsteigti pirmieji du tarpvalstybiniai kibernetinio saugumo centrai, taip pat jų pažangą siekiant Europos kibernetinio saugumo įspėjimų sistemos tikslų. Taip pat nagrinėjome, kaip steigiami tarpvalstybiniai kibernetinio saugumo centrai įsilieja į platesnę kibernetinio saugumo aplinką ir kaip jie sąveikauja su esamais tinklais ir struktūromis.

Dėl didelių vėlavimų vykdant viešuosius pirkimus konkrečių rezultatų kol kas nepasiekta

- 65** Finansavimas nacionalinių ir tarpvalstybinių kibernetinių centrų steigimui remti pagal Skaitmeninės Europos programą teikiamas nuo 2021 m. Šis finansavimas teikiamas taikant sudėtingą procedūrą, pagal kurią lygiagrečiai skiriamos įprastos dotacijos centrų steigimui ir veiklai remti ir vykdomi bendri viešieji pirkimai pažangioms grėsmių aptikimo priemonėms įsigyti, kaip parodyta **6 diagramoje**. Po 2022 m. lapkričio mėn. paskelbto kvietimo teikti pasiūlymus ATHENA ir ENSOC pradėjo veiklą 2024 m. sausio mėn.

6 diagrama | Kibernetinio saugumo centrams pagal Skaitmeninės Europos programą skirtas finansavimas



Šaltinis: Audito Rūmai, remiantis ECCC duomenimis.

- 66** Dviejų etapų ribotą konkursą¹¹ organizavo ATHENA ir ENSOC nariai, taip pat CNECT GD (pirmasis etapas) ir naujai įsteigtas ECCC (antrasis etapas). Dviejų etapų metodu siekiama apriboti neskelbtinos informacijos sklaidą: išsamios techninės specifikacijos pateikiamos tik per pirmąjį etapą atrinktiems kandidatams.
- 67** Pirmasis ENSOC konkurso etapas pradėtas 2024 m. gegužės mėn., o pirmasis ATHENA konkurso etapas – 2024 m. liepos mėn. Susidomėjusios įmonės turėjo vieną mėnesį paraiškoms pateikti. Tačiau atrinktiems kandidatams pranešta tik 2025 m. balandžio mėn., t. y. praėjus beveik metams nuo procedūros pradžios.
- 68** Be to, tuo metu nei ENSOC, nei ATHENA atveju nebuvo galima pradėti antrojo konkurso etapo, nes šių centrų nariai ir ECCC negalėjo į trumpąjį sąrašą įtrauktoms įmonėms pateikti pasiūlymui parengti būtinų techninių specifikacijų, nes šios dar nebuvo galutinai parengtos.
- 69** Antrasis konkurso etapas dėl kai kurių ENSOC pirkimo dalių prasidėjo tik 2025 m. rugpjūčio mėn., o ATHENA atveju buvo planuojamas pradėti 2026 m. pradžioje. Audito metu, praėjus 18 mėnesių nuo konkurso pradžios, dėl nė vienos pirkimo dalies nebuvo pasirašyta sutartis. Manome, kad nepakankamas pasirengimas ir viešųjų pirkimų procedūrų sudėtingumas trukdė jas užbaigti laiku.
- 70** Todėl nustatėme, kad tarpvalstybiniai centrai nėra pajėgūs pasiekti savo tikslų pagal nustatytą tvarkaraštį. Neturėdami priemonių grėsmėms aptikti ir dalytis informacija, jie faktiškai nevykdo veiklos, o Europos kibernetinio saugumo įspėjimų sistema dar neveikia, todėl vėluojama rezultatyviai plėtoti pažangius kibernetinių grėsmių ir incidentų aptikimo ir prevencijos pajėgumus. Siekiant atsižvelgti į iki šiol susidariusius viešųjų pirkimų procedūrų vėlavimus, pasirašyti pakeitimai, kuriais pratęsimas dotacijų susitarimų galiojimas (15 mėnesių ATHENA atveju ir 18 mėnesių ENSOC atveju).

¹¹ ENSOC kvietimas dalyvauti konkurse ir ATHENA kvietimas dalyvauti konkurse.

Tarpvalstybiniai kibernetinio saugumo centrai sukuria papildomų ryšių kanalų, kurie dar labiau padidina sudėtingumą

- 71** Viena iš pagrindinių tarpvalstybinių kibernetinio saugumo centrų užduočių – dalytis svarbia informacija, kad būtų pagerintas grėsmių aptikimas ir reagavimas į jas. Tai apima informaciją apie kibernetines grėsmes, pažeidžiamumą, užvaldymo rodiklius ir priešiškus subjektus. Tarpvalstybinių kibernetinio saugumo centrų užduotys iš dalies sutampa su nacionalinių CSIRT ir CSIRT tinklo užduotimis, visų pirma susijusiomis su dalijimusi informacija apie kibernetines grėsmes ir pažeidžiamumą. Aiškos ribos tarp tarpvalstybinių kibernetinių centrų ir CSIRT vaidmenų nėra. Pagal 2025 m. Kibernetinio saugumo planą (29 dalis) tarpvalstybiniai kibernetinio saugumo centrai turėtų veikti tiek techniniu lygmeniu (kaip nacionalinės CSIRT ir CSIRT tinklas), tiek operatyviniu lygmeniu (kaip EU-CyCLONe).
- 72** Kibernetinio solidarumo akte reikalaujama, kad tarpvalstybiniai kibernetinio saugumo centrai pasirašytų tarpusavio bendradarbiavimo susitarimus, kad būtų sudarytos palankesnės sąlygos dalytis informacija. Kaip nustatyta Kibernetinio solidarumo akte, ENISA iki 2026 m. vasario mėn. turėtų paskelbti tarpvalstybinių kibernetinių centrų sąveikos gaires. 2025 m. gruodžio mėn. ECCC skyrė dotaciją konsorciui (įskaitant tam tikrus ENSOC ir ATHENA narius), kad jis nustatytų tarpvalstybinių kibernetinio saugumo centrų sąveikos techninę sistemą. Tačiau gairės ir sistema bus parengtos tik tada, kai tarpvalstybiniai kibernetinio saugumo centrai pradės veikti. Kaip nurodėme savo 2023 m. nuomonėje dėl Pasiūlymo dėl kibernetinio solidarumo akto¹², kyla rizika, kad, jei nebus greitai susitarta, gali būti sukurtos tarpusavyje nesuderinamos sistemos, o tai lemtų didesnes išlaidas.
- 73** Tarpvalstybiniai kibernetinio saugumo centrai taip pat privalo nepagrįstai nedelsdami dalytis atitinkama informacija apie didelio masto kibernetinio saugumo incidentus su EU-CyCLONe ir CSIRT tinklu. Valstybių narių lygmeniu nacionalinių kibernetinio saugumo centrų kūrimas ir dalyvavimas tarpvalstybiniuose kibernetinio saugumo centruose sukuria papildomus komunikacijos lygmenis. Sudėtingumas didėja ir dėl koordinavimo su ES nepriklausančiomis valstybėmis¹³, kurios nėra CSIRT tinklo ar EU-CyCLONe narės.

¹² Nuomonės 02/2023 dėl Pasiūlymo 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, 26 dalis.

¹³ Islandija ir Norvegija.

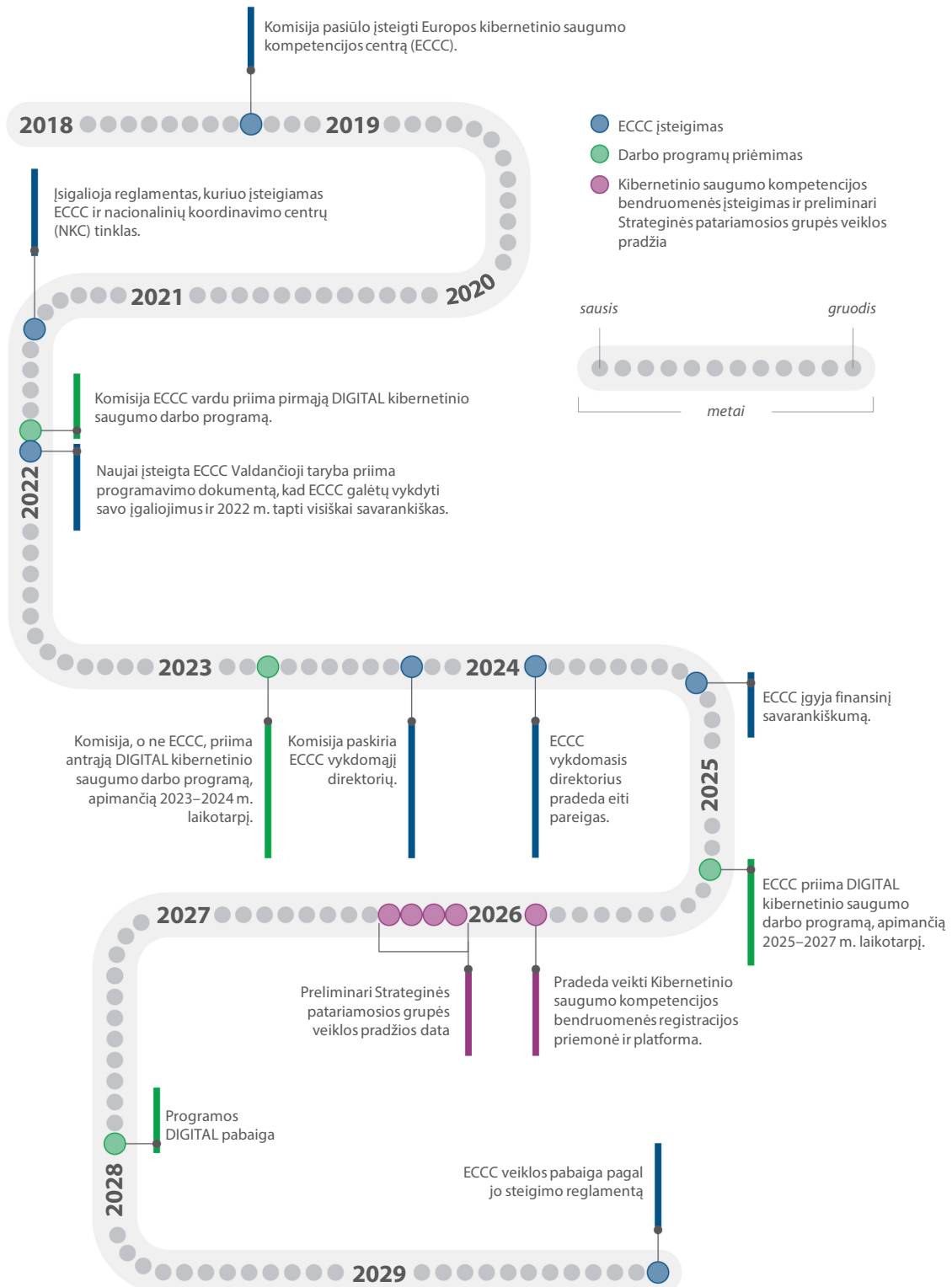
- 74** Būtinai aiškūs bendradarbiavimo susitarimai, kuriais būtų suderinta bendra taksonomija ir dalijimosi informacija tvarka, taip pat užtikrintas sąveikumas. Iš CSIRT tinklo patirties matyti, kad tai yra didelis iššūkis. Nustatėme, kad audito metu dėl procedūrinės bendradarbiavimo ir dalijimosi informacija tvarkos susitarta nebuvo. Manome, kad steigiant nacionalinius ir tarpvalstybinius kibernetinius centrus galėtų būti paskatintas veiksmingesnis dalijimasis informacija. Tačiau integruoti tarpvalstybinius centrus į jau ir taip sudėtingą kibernetinio saugumo aplinką bus sunku ir tam reikės papildomų ryšių kanalų ir bendradarbiavimo susitarimų.

Pagal Skaitmeninės Europos programą ES finansuojamais projektais siekiama stiprinti kibernetinį saugumą, tačiau susiduriama su įgyvendinimo ir ataskaitų teikimo sunkumais

Vėluojama steigti Kibernetinio saugumo kompetencijos bendruomenė negalėjo formuoti Skaitmeninės Europos programos pagal savo poreikius

- 75** Siekdama valdyti Skaitmeninės Europos programos kibernetinio saugumo komponentą, 2018 m. Komisija pasiūlė įsteigti Europos kibernetinio saugumo kompetencijos centrą (ECCC). ECCC reglamente numatyta, kad ECCC veiklą rems 29 nacionalinių koordinavimo centrų (NKC) tinklas – po vieną NKC kiekvienoje valstybėje narėje, taip pat Islandijoje ir Norvegijoje. Jame taip pat numatyta sukurti Kibernetinio saugumo kompetencijos bendruomenę (toliau – Bendruomenė), kurią sudarytų pramonės, akademinės bendruomenės ir mokslinių tyrimų organizacijų, taip pat kitų atitinkamų pilietinės visuomenės asociacijų atstovai.
- 76** Į Strateginę patariamąją grupę (SPG), kuri yra viena iš trijų ECCC struktūros sudedamųjų dalių, turėjo būti skiriama iki 20 Bendruomenės narių. Viena iš pagrindinių SPG užduočių – rengti viešas konsultacijas, kurių rezultatais būtų remiamasi rengiant ECCC darbotvarkę ir Skaitmeninės Europos programos darbo programas.
- 77** Vertiname, ar Skaitmeninės Europos programa ir jos darbo programos buvo priimtos remiantis patikima poreikių analize, taip pat tai, kaip rengiant darbo programas galėjo prisidėti ECCC, NKC tinklas, Bendruomenė ir SPG. Praktiškai ECCC, NKC tinklas, Bendruomenė ir SPG buvo steigiami palaipsniui per kelerius metus (žr. [7 diagramą](#)).

7 diagrama | Europos kibernetinio saugumo kompetencijos centro, nacionalinių koordinavimo centrų tinklo, Bendruomenės ir Strateginės patiriamosios grupės steigimo chronologija



Šaltinis: Audito Rūmai.

- 78** Kadangi ECCC visu pajėgumu pradėjo veikti tik 2024 m. rugsėjo mėn., Komisija ECCC vardu priėmė 2021–2022 m. ir 2023–2024 m. darbo programas. Rengiant šias abi darbo programas nebuvo galima pasinaudoti Bendruomenės indėliu.
- 79** Tuo metu valstybės narės pradėjo steigti savo NKC, kurie veikia kaip Bendruomenės nacionalinio lygmens kontaktiniai punktai. Jų steigimas ir veikla bendrai finansuojami pagal Skaitmeninės Europos programą: iki audito pradžios buvo skirta daugiau kaip 90 milijonų eurų ES lėšų, įskaitant maždaug 44 milijonus eurų, kurie bus toliau paskirstyti kaip finansinė parama trečiosioms šalims. NKC remti iki 2027 m. biudžete numatyta dar 38 milijonai eurų.
- 80** Nustatėme, kad 2025 m. gruodžio mėn., praėjus ketveriems metams nuo ECCC ir NKC tinklo įsteigimo, Bendruomenė dar nebuvo įsteigta, o SPG nariai dar nebuvo paskirti. 2025 m. kovo 14 d. ECCC priėmė naujausią Skaitmeninės Europos programos kibernetinio saugumo darbo programą, apimančią 2025–2027 m. laikotarpį. Nors ECCC savo darbo programą parengė ir priėmė po išsamių konsultacijų su valstybėmis narėmis ir NKC tinklu, jis negalėjo pasinaudoti Bendruomenės ar SPG indėliu ir rekomendacijomis. Tai prieštarauja ECCC steigimo reglamento nuostatomis, todėl tai vertiname kaip neišnaudotą galimybę.
- 81** Skaitmeninės Europos programa baigs galioti 2027 m. ir, jei ECCC įgaliojimai nebus pratęsti, jo veikla turėtų nutrūkti 2029 m. Todėl parama, kurią teiks NKC tinklas, Bendruomenė ir SPG, kai šios struktūros pradės veikti, gali būti aktuali tik trumpą laikotarpį.

ES finansuojamais projektais siekiama aktualių tikslų, tačiau įgyvendinant daugelį jų susiduriama su veiklos sunkumais

82 Sudarėme imtį iš 11 projektų, susijusių su kibernetinio saugumo incidentų aptikimu ir reagavimu į juos ir 2022–2025 m. finansuotų pagal Skaitmeninės Europos programą, (žr. *I priedo 5 diagramą* ir *III priedą*). Vertinome, ar:

- projektų tikslai derėjo su numatomais rezultatais, nurodytais kvietimuose teikti pasiūlymus, ir apskritai su Skaitmeninės Europos programos tikslais;
- iki šiol įgyvendinant projektus pasiekti planuoti išdirbiai ir rezultatai;
- projektų išdirbiai sukurti laiku.

Šio vertinimo rezultatus pateikiame *IV priede*.

Kai kuriais projektais jau pasiekti pirmieji rezultatai, tačiau įgyvendinant daugelį jų vėluojama ar susiduriama su veiklos sunkumais

83 Nustatėme, kad visais projektais siekiama tikslų, kuriais prisidedama prie Skaitmeninės Europos programos kibernetinio saugumo tikslų¹⁴, ir kad jais įgyvendinama dauguma kvietimuose teikti pasiūlymus nustatytų tikslų¹⁵.

84 Iš 11 į mūsų imtį įtrauktų projektų du buvo dar tik pradėti įgyvendinti, todėl negalėjome padaryti išvados dėl jų veiklos rezultatų. Iš likusių projektų keturis įvertinome kaip patenkinamus, atsižvelgdami į pasiektus planuotus išdirbius ir rezultatus. Nustatėme, kad du projektai turi tam tikrų trūkumų, o tris įvertinome kaip nepatenkinamus (žr. *IV priedą*).

85 Skaitmeninės Europos programa aiškiai siekiama padidinti mažųjų ir vidutinių įmonių (MVĮ) kibernetinio saugumo lygį. Šiuo atžvilgiu keliuose projektuose siūlomi konkretūs MVĮ skirti sprendiniai (žr. *2 langelį*).

¹⁴ Reglamento (ES) 2021/694, kuriuo nustatoma Skaitmeninės Europos programa, 6 straipsnis.

¹⁵ Kvietimai dėl saugumo operacijų centrų pajėgumų stiprinimo; nacionalinių koordinavimo centrų tinklo diegimo valstybėse narėse; parengties paramos ir savitarpio pagalbos ir saugumo operacijų centrams skirtų naujoviškų DI ir kitų didelio poveikio technologijų taikmenų.

2 langelis

MVĮ apčiuopiamų rezultatų teikiančių projektų pavyzdžiai

Projekto **GR-SME-SOC** (6 projektas **III priede**) tikslas – Graikijos MVĮ suteikti kibernetinio saugumo priemones ir paslaugas įsteigiant jų poreikiams pritaikytą saugumo operacijų centrą (SOC). Projektas pradėtas 2024 m. sausio mėn. Jį įgyvendina penkių Graikijos organizacijų konsorciumas. Planuojama, kad kibernetinio saugumo paslaugos 120 MVĮ vienus metus bus teikiamos nemokamai, o vėliau – komercinėmis sąlygomis. Pagal šį projektą MVĮ siūlomos pažangios paslaugos, tokios kaip tikralaikė stebėseną, DI grindžiamas grėsmių aptikimas ir operatyvus reagavimas į incidentus.

Įgyvendindamas projektą **NCC-IE** (3 projektas **III priede**), projekto koordinatorių suteikė maždaug 1,8 milijono eurų dotacijų daugiau kaip 50 Airijos MVĮ jų kibernetiniam saugumui didinti. Pagal dotacijų schemą parama suteikta įvairiuose sektoriuose veikiančioms įmonėms, kuriose dirba nuo 2 iki maždaug 200 darbuotojų, įskaitant šeimos verslo įmones, startuolius ir pasauliniu mastu eksportuojančias įmones. Dotacijos buvo skirtos tik įmonėms, kurių kibernetinio saugumo peržiūrą anksčiau atliko vyriausybės agentūra „Enterprise Ireland“. Dotacija padengė 80 % išlaidų (iki 60 000 eurų), patirtų įgyvendinant peržiūros rekomendacijas.

Šaltinis: Audito Rūmai.

- 86** Įgyvendinant daugelį į mūsų imtį įtrauktų projektų sudėtinga laikytis terminų arba kyla veiklos sunkumų (žr. **IV priedą**). Nustatėme, kad keturių projektų atveju vėluojama labai smarkiai. Tarp jų – su ENSOC ir ATHENA susiję projektai, kaip išsamiau aprašyta **65–70** dalyse. Kitus pavyzdžius pateikiame **3 langelyje**.

3 langelis

Projektų, kuriuos įgyvendinant susiduriama su veiklos sunkumais ir vėlavimais, pavyzdžiai

Airijoje vietos valdžios valdymo institucija LGMA yra vienintelė projekto **ILG-SOC** (8 projektas **III priede**) dotacijos gavėja. Projekto tikslas – įsteigti centrinį saugumo operacijų centrą 31 vietos valdžios institucijai, kad šios galėtų naudotis pažangiomis grėsmių aptikimo ir reagavimo į jas priemonėmis. Projektas pradėtas įgyvendinti 2023 m. spalio mėn., jo trukmė – treji metai. Atlikus laikotarpio vidurio peržiūrą nė vienas teikinyss nebuvo patvirtintas. Projektas apima keletą viešųjų pirkimų procedūrų, kurios buvo nesėkmingos arba vėlavo. Projekto trukmė bus pratęsta (neskiriant papildomo finansavimo), o tai galėtų suteikti pakankamai laiko projektui sėkmingai užbaigti.

Graikijoje projektu **EL-SOC** (5 projektas **III priede**) siekiama sukurti nacionaliniu lygmeniu konsoliduotą SOC, kuriame būtų sutelkta sektorių SOC informacija. Taip būtų užtikrinta tikralaikė išsami kibernetinio saugumo padėties apžvalga. Projektas įgyvendinamas nuo 2024 m. sausio mėn. iki 2026 m. gruodžio mėn. Planiniai aparatinės įrangos ir paslaugų viešieji pirkimai buvo atidėti dėl problemų, susijusių su konkurso techninių specifikacijų užbaigimu ir paskelbimu. Kaip vėlavimo priežastis projekto koordinatorių taip pat nurodė sunkumus užtikrinant nacionalinį bendrą finansavimą ir viešųjų pirkimų darbuotojų trūkumą.

Šaltinis: Audito Rūmai.

- 87** Kitų dviejų į mūsų imtį įtrauktų projektų įgyvendinimas šiek tiek vėluoja. Trijų projektų išdirbiai buvo pasiekti laiku. O du projektai dar tik pradėti įgyvendinti, todėl negalime padaryti išvados.

Dėl saugumo apribojimų kilo veiklos sunkumų, o patikros, kurias atlieka naudos gavėjai, kelia reikšmingą riziką

- 88** Skaitmeninės Europos programos reglamente nustatyta, kad dėl saugumo priežasčių kibernetinio saugumo finansavimas gali būti skiriamas tik ES įsisteigusiesiems subjektams, kuriuos kontroliuoja valstybės narės arba ES piliečiai. Šiuo apribojimu siekiama sumažinti ES nepriklausančių valstybių kišimosi ar įtakos riziką ir užkirsti kelią dalijimuisi neskelbtina saugumo informacija su ES nepriklausančių valstybių institucijomis.

- 89** ES nuosavybės ir kontrolės pareiga taikoma ne tik dotacijų gavėjams, bet ir jų subrangovams bei visiems finansinės paramos trečiosioms šalims gavėjams. Išskyrus pastarąją kategoriją (žr. **92–96** dalis), vertinimą atlieka [Europos mokslinių tyrimų vykdomosios įstaigos](#) Centrinė patvirtinimo tarnyba. Tačiau galutinį sprendimą dėl tinkamumo dalyvauti ribotuose konkursuose vis tiek priima dotaciją teikianti institucija, t. y. CNECT GD arba ECCC.
- 90** Audito metu naudos gavėjai ne kartą minėjo praktinius iššūkius, kylančius dėl nuosavybės ir kontrolės vertinimų. ES atsakomybės ir kontrolės vertinimas gali būti sudėtingas ir ilgas procesas: reikia išanalizuoti kiekvienos organizacijos visą nuosavybės struktūrą ir kontrolės grandinę, įskaitant visus nuosavybės lygmenis iki tikrųjų savininkų. Centrinė patvirtinimo tarnyba reikalauja, kad kiekvienas subjektas pateiktų išsamius [patvirtinamuosius dokumentus](#) apie savo nuosavybės struktūrą ir konkrečias teises, įmonės valdymą ir visus komercinius, finansinius ar kitus ryšius, dėl kurių įgyjama kontrolė.
- 91** Trijuose į mūsų imtį įtrauktuose ES finansuojamuose projektuose bent vienas konsorciumo naudos gavėjas vėliau buvo pašalintas, nes buvo laikoma, kad jis nuosavybės teise priklauso už ES ribų įsisteigusiems subjektams arba yra jų kontroliuojamas. Konsorciumo narių pašalinimas rodo, kad ne visi Skaitmeninės Europos programos dalyviai tinkamai supranta ES nuosavybės ir kontrolės sąvoką. Apskritai, remiantis Centrinės patvirtinimo tarnybos duomenimis, 2022–2025 m. 7 % visų subjektų, pateikusių paraiškas dėl kibernetinio saugumo srities dotacijų pagal Skaitmeninės Europos programą, arba subrangovų buvo įvertinti neigiamai. Kai į kvietimą teikti pasiūlymus atsiliepia reikalavimų neatitinkantys dalyviai, atsiranda vėlavimų (žr. **4 langelį**).

4 langelis

Atvejis, kai naudos gavėjai buvo pašalinti po neigiamų saugumo patikrų rezultatų

Dviejų projekto [NG-SOC](#) (7 projektas [III priede](#)) konsorciumo narių nuosavybės ir kontrolės vertinimo rezultatai buvo neigiami. Rezultatai buvo paskelbti likus maždaug mėnesiui iki dotacijos susitarimo pasirašymo termino. Projekto koordinatorių turėjo sutikti perimti darbus, kurie buvo pavesti dviem pašalintiems nariams, nes nebebuvo laiko rasti naują partnerį. Vienas iš pašalintų narių vykdė veiklą konkrečioje pramonės šakoje, kurioje sukurtas sprendinys turėjo būti išbandytas. Todėl didelė projekto dalis, susijusi su sprendinių išbandymu praktikoje, negalėjo būti įgyvendinama taip, kaip buvo numatyta. Vėliau ši padėtis buvo ištaisyta iš dalies pakeitus dotacijos susitarimą, kad būtų įtraukti nauji nariai.

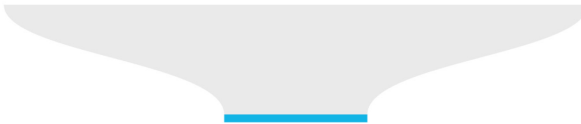
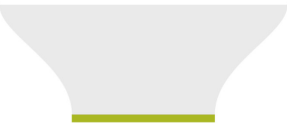
- 92** Pagal du mūsų peržiūrėtus projektus (NCC-IE ir „CYberSynchrony“) finansinė parama teikiama trečiosioms šalims. Šis finansavimo mechanizmas suteikia galimybę dotacijų gavėjams dalį dotacijos lėšų panaudoti kitiems subjektams finansuoti skelbiant atvirus kvietimus. Tokiu būdu gali būti sudaromos palankesnės sąlygos gauti ES finansavimą. Šiuo atveju už nuosavybės ir kontrolės vertinimą atsako tik naudos gavėjai, o Centrinė patvirtinimo tarnyba nedalyvauja.
- 93** 2021 m. Komisija paraiškų dalyvauti ribotuose konkursuose teikėjams paskelbė bendras viešas gaires, kurios buvo atnaujintos 2026 m. Nors finansinės paramos trečiosioms šalims galimybė pagal Skaitmeninės Europos programos kvietimus numatyta nuo 2021 m., nei Komisija, nei ECCC naudos gavėjams nepateikė išsamios metodikos, kaip atlikti trečiųjų šalių, kurioms jie teikia finansinę paramą, nuosavybės ir kontrolės vertinimo patikras. 2025 m. liepos mėn. ECCC pasidalijo neprivalomomis gairėmis, kuriose NKC tinklui pateikiamas struktūrinis nuosavybės ir kontrolės vertinimų atlikimo metodas. Gairėse išdėstyti bendrieji principai ir veiksmai, kurių būtų galima imtis, tačiau nenurodoma, kaip patikros turėtų būti atliekamos, todėl naudos gavėjams tenka patiemis parengti savo metodus.
- 94** Nustatėme, kad ECCC netvirtina naudos gavėjų priimtų metodikos ir neatlieka intimi grindžiamų patikrų, kad įsitikintų, jog metodika yra pakankamai patikima, o atrinkti finansinės paramos gavėjai iš tiesų atitinka reikalavimą dėl ES nuosavybės ir kontrolės.
- 95** Savo [2024 m. metinėje ataskaitoje](#) konstatavome, kad naudos gavėjai, kuriems Komisija pavedė valdyti finansinę paramą trečiosioms šalims (mokslinių tyrimų srityje), neprivalo įrodyti, kad jų patikros yra veiksmingos siekiant užtikrinti ES išlaidų tvarkingumą. ECCC taip pat nevertina naudos gavėjų administracinių ir techninių pajėgumų tinkamai valdyti nuosavybės ir kontrolės vertinimus. Kaip išsamiai aprašyta [90](#) dalyje, šis vertinimas gali būti sudėtingas ir jį ES lygmeniu atlieka speciali tarnyba, turinti reikiamą ekspertinę kompetenciją.
- 96** Mūsų vertinimu, šiomis aplinkybėmis kyla didelė rizika, kad už nuosavybės ir kontrolės vertinimo patikras atsakingi naudos gavėjai gali neturėti pajėgumų jas tinkamai atlikti. Atsižvelgiant į finansuojamos veiklos pobūdį, dėl šio trūkumo gali kilti pavojus didesnės rizikos infrastruktūrai, veiklos duomenims ir saugumui svarbioms technologijoms.

Daugumos ES finansuojamų projektų veiklos rezultatų sistemos turi trūkumų, o Skaitmeninės Europos programos kibernetinio saugumo srities veiklos rezultatų duomenys netikslūs

Daugumos ES finansuojamų projektų veiklos rezultatų sistemos turi trūkumų

- 97** ES finansuojamus projektus valdantys naudos gavėjai privalo ECCC pranešti apie projektų pažangą ir rezultatus, remdamiesi tarpinėmis reikšmėmis, teikiniais ir rodikliais, kaip pavaizduota **8 diagramoje**. Vertinome, ar pagal kiekvienam projektui nustatytas tarpines reikšmes ir teikinius galima tinkamai vykdyti projektų stebėseną. Taip pat vertinome, ar jų veiklos rezultatų rodikliai yra aktualūs ir išmatuojami ir ar nustatytos jų pradinės ir siektinos reikšmės.

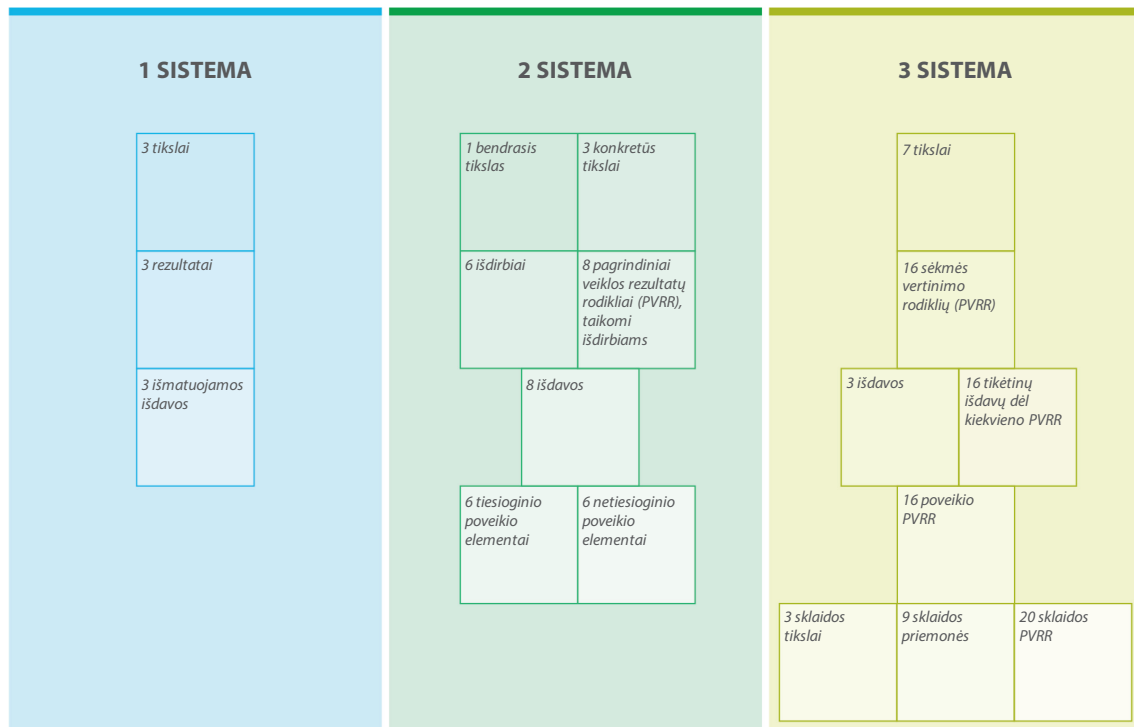
8 diagrama | Skaitmeninės Europos programos projektų tarpinės reikšmės, teikiniai ir veiklos rezultatų rodikliai

	 Tarpinės reikšmės	 Teikiniai	 Veiklos rezultatų rodikliai
Kas tai	viso projekto kontrolės punktai, padedantys įvertinti pažangą	projekto pažangai parodyti teikiami projekto išdirbiai	naudojami rezultatams vertinti
Kaip nustatyti	siejama tik su pagrindiniais išdirbiais (ribotas skaičius)	tik pagrindiniai išdirbiai (ne daugiau kaip 10–15 vienam projektui)	konkretūs, išmatuojami, pasiekiami, aktualūs ir per nustatytą laiką įvykdytini
Pavyzdžiai	„platformos bandomojo etapo pradžia“	„platformos naudojimo vadovas“	„30 % sutrumpėjęs reagavimo į incidentus laikas“
	 Struktūrizuotas metodas, internetinės dotacijų valdymo sistemos dalis		 Nestrukūrizuotas metodas

Šaltinis: Audito Rūmai, remiantis [dotacijos paraiškos forma](#).

- 98** Projekto pasiūlyme naudos gavėjai pagal pareiškėjams skirtuose nurodymuose pateiktą struktūrizuotą metodą turi nustatyti tarpines reikšmes ir teikinius. Visos tarpinės reikšmės ir teikiniai nurodomi internetinėje dotacijų valdymo sistemoje, kad būtų lengviau stebėti su jais susijusią pažangą. Paprastai ECCC kiekvieną projektą peržiūri du kartus: vieną kartą – projektui įpusėjus, kitą kartą – jį užbaigus. Per šias peržiūras išorės ekspertai tikrina, ar pasiektos tarpinės reikšmės ir teikiniai, o ECCC juos patvirtina. Todėl tarpinės reikšmės ir teikiniai yra esminiai projektų stebėsenos elementai ir turėtų būti tinkamai nustatyti.
- 99** Nustatėme, kad beveik nė viename mūsų imties projekte nesilaikyta nurodymų dėl tarpinių reikšmių ir teikinių skaičiaus: kiekvienam projektui nustatyta nuo 8 iki 39 tarpinių reikšmių ir nuo 8 iki 45 teikinių. Daugelis tarpinių reikšmių ir teikinių nustatyti nesilaikant atitinkamų nurodymų, todėl nėra tinkami pažangai stebėti (pavyzdžiui, „susitikimas, skirtas pradėti rengti kvietimą teikti mokslinių tyrimų pasiūlymus“ arba „oficialus susitikimo dėl projekto protokolas“). Trijuose projektuose vertinimo komitetas šias problemas buvo nustatęs dar prieš pasirašant dotacijos susitarimą. Dviem atvejais naudos gavėjai pasiūlė tik nedidelius pakeitimus (pavyzdžiui, pakeisti terminus), tačiau esminių problemų nesprendė, o trečiuoju atveju jokių pakeitimų nepadaryta. Atlikę analizę nustatėme, kad kitų šešių į mūsų imtį įtrauktų projektų tarpinės reikšmės arba teikiniai parengti nesilaikant nurodymų ir jie ne visada yra tinkami. Manome, kad dėl prastai nustatytų teikinių ar tarpinių reikšmių arba per didelio jų skaičiaus stebėti pažangą sudėtinga.
- 100** Veiklos rezultatų rodikliams, kitaip nei tarpinėms reikšmėms ir teikiniams, struktūrizuotas metodas netaikomas ir jie nėra suvesti į dotacijų valdymo sistemos lentelę – juos galima rasti įvairiuose pasiūlymo skirsniuose. Dėl to naudos gavėjai pasiūlė daugybę skirtingų veiklos rezultatų sistemų. Kai kurie nustatė tik projekto tikslus, susietus su veiklos rezultatų rodikliais, o kiti parengė kur kas sudėtingesnes veiklos rezultatų sistemas. Keletą pavyzdžių pateikiame [9 diagramoje](#).

9 diagrama | Projektams parengtų veiklos rezultatų sistemų įvairovės pavyzdys



Šaltinis: Audito Rūmai.

- 101** Atlikę analizę padarėme išvadą, kad daugelis projektams taikomų veiklos rezultatų rodiklių nėra aktualūs ar išmatuojami ir nenustatytos jų siektinos ar pradinės reikšmės (žr. [5 langelį](#)). Be to, septyniuose projektuose nustatyta po 20 ar daugiau rodiklių, o viename projekte – 52 rodikliai. Šio vertinimo rezultatus pateikiame [IV priede](#).

5 langelis

Netinkamų veiklos rezultatų rodiklių pavyzdžiai

Neišmatuojami:

- „užvaldymo rodiklis ir kitos teikiamos paslaugos stiprina MVĮ kibernetinio saugumo pajėgumus“;
- „reagavimo į incidentus priemonių ir metodų, kuriais sudaromos sąlygos integracijai į EU-CyCLONe ryšių kanalus, teikimas“.

Nenurodyta pradinė arba siektina reikšmė:

- „≥20 % geresnė darbuotojų parengtis“;
- „≥20 % sumažėjęs pastangų, reikalingų siekiant prisitaikyti prie atitinkamų ES kibernetinio saugumo iniciatyvų ir laikytis jų reikalavimų, poreikis“.

Nesusiję su veiklos rezultatais:

- „galutinė projekto ataskaita finansavimo etapo pabaigoje“;
- „stažuotojų, dalyvausiančių visuose mokymuose, skaičius“.

Šaltinis: Audito Rūmai, remiantis projektų dokumentais.

102 Apskritai, manome, kad didelė veiklos rezultatų sistemų įvairovė, netinkamai nustatyti rodikliai ir per didelis jų skaičius labai apsunkina veiklos rezultatų stebėseną. Todėl neįmanoma tinkamai įvertinti projektų veiklos rezultatų. Papildomų sunkumų kelia tai, kad ataskaitos šablone nėra atskiro skirsnio projektų veiklos rezultatų rodikliams, todėl daugumoje mūsų imties projektų informacija apie juos nebuvo pateikta.

Duomenys apie Skaitmeninės Europos programos kibernetinio saugumo komponento veiklos rezultatus yra netikslūs

- 103** Skaitmeninės Europos programos pasiekimams stebėti reglamente nustatyti programos rodikliai, apie kuriuos turi būti pranešama įgyvendinant visus projektus, kaip išsamiau aprašyta [6 langelyje](#).

6 langelis

Skaitmeninės Europos programos kibernetinio saugumo rodikliai

1. a) Bendrai įsigytų, be kita ko, Europos kibernetinio saugumo įspėjimų sistemos kontekste, kibernetinės infrastruktūros objektų arba priemonių ar tiek objektų, tiek priemonių skaičius.
1. b) Įdiegtų kibernetinės infrastruktūros objektų arba priemonių ar tiek objektų, tiek priemonių, skaičius.
2. Naudotojų ir naudotojų bendruomenių, kurie gauna prieigą prie Europos kibernetinio saugumo įrenginių, skaičius.
3. Pagal Reagavimo į kibernetinio saugumo krizes mechanizmą vykdomų veiksmų, kuriais remiamas pasirengimas kibernetinio saugumo incidentams ir reagavimas į juos, skaičius.

Šaltinis: [Reglamento \(ES\) 2021/694, kuriuo nustatoma Skaitmeninės Europos programa](#), II priedas; Skaitmeninės Europos programos stebėsenos ir vertinimo sistema ([SWD\(2024\) 37](#)).

- 104** Vertiname, ar įgyvendinant mūsų imties projektus, buvo teikiama informacija apie šiuos rodiklius, ir nagrinėjome, kaip ECCC šiuos duomenis renka ir tikrina.
- 105** Prieš atliekant visų projektų laikotarpio vidurio ir galutines peržiūras, dotacijų valdymo sistemoje prašoma pateikti informaciją apie Skaitmeninės Europos programos rodiklius. Nustatėme, kad iš septynių projektų, kurių įgyvendinimo laikotarpis mūsų audito metu buvo įpusėjęs ir todėl turėjo būti pateikta informacija apie šiuos rodiklius, tai buvo padaryta tik dėl trijų projektų. Iš šių trijų projektų dėl dviejų projektų pateikta informacija nebuvo tiksli: dėl vieno projekto pateikta informacija apie netinkamą rodiklį, o dėl kito vietoj pasiektų rezultatų pateiktos siektinos reikšmės.

106 Kasmēt Komisija apie šiuos rodiklius praneša [programos veiklos rezultatų ataskaitose](#). Taip suinteresuotieji subjektai gali įvertinti, ar įgyvendinant programą pasiekiami jos tikslai. Remiantis 2024 m. programos veiklos rezultatų ataskaitomis, Skaitmeninės Europos programos kibernetinio saugumo rodikliai rodo pagal planą daromą pažangą. ECCC mums paaiškino, kad šiems rodikliams apskaičiuoti jis naudojo projektų naudos gavėjams siūstas apklausas, o ne dotacijų valdymo sistemos duomenis. Peržiūrėjome ECCC pateiktus išskaidytus duomenis ir nustatėme daug problemų, susijusių su duomenų rinkimo būdu ir bendra jų kokybe. Nustatėme, kad surinkti duomenys neatitinka programos veiklos rezultatų ataskaitoje pateiktų reikšmių, todėl neaišku, kaip nurodytos reikšmės buvo apskaičiuotos. Neradome jokių įrodymų, kad ECCC būtų patikrinęs, ar pateikti duomenys tikslūs. Atlikę į mūsų imtį įtrauktų projektų patikras, manome, kad pateikti duomenys tinkamai neparodo pasiektų rezultatų, nes daugumos reikšmių trūksta arba jos yra netikslios.

Šią ataskaitą priėmė III kolegija, vadovaujama Audito Rūmų nario
George'o Mariaus Hyzlerio, 2026 m. birželio 16 d. Liuksemburge įvykusiame posėdyje.

Audito Rūmų vardu

Pirmininkas
Tony Murphy

Priedai

I priedas. Apie auditą

- 01** Kibernetinis saugumas apibrėžiamas kaip „veikla, būtina tinklų ir informacinėms sistemoms, tokių sistemų naudotojams ir kitiems susijusiems asmenims apsaugoti nuo kibernetinių grėsmių“¹. Kibernetinė grėsmė – tai „galima aplinkybė, įvykis arba veiksmas, kuris galėtų pažeisti, sutrikdyti arba kitaip neigiamai paveikti tinklų ir informacines sistemas, tokių sistemų naudotojus ir kitus asmenis“². Kibernetiniam saugumui užtikrinti būtinas visapusiškas požiūris, apimantis įvairią tarpusavyje susijusią veiklą, kuria siekiama užkirsti kelią kibernetinėms grėsmėms, jas aptikti, į jas reaguoti ir po jų atkurti veiklą, kaip parodyta [1 diagramoje](#).

¹ Reglamentas (ES) 2019/881 ([Kibernetinio saugumo aktas](#)).

² [Kibernetinio saugumo akto](#) 2 straipsnis.

1 diagrama | Kibernetinio saugumo veiklos pavyzdžiai

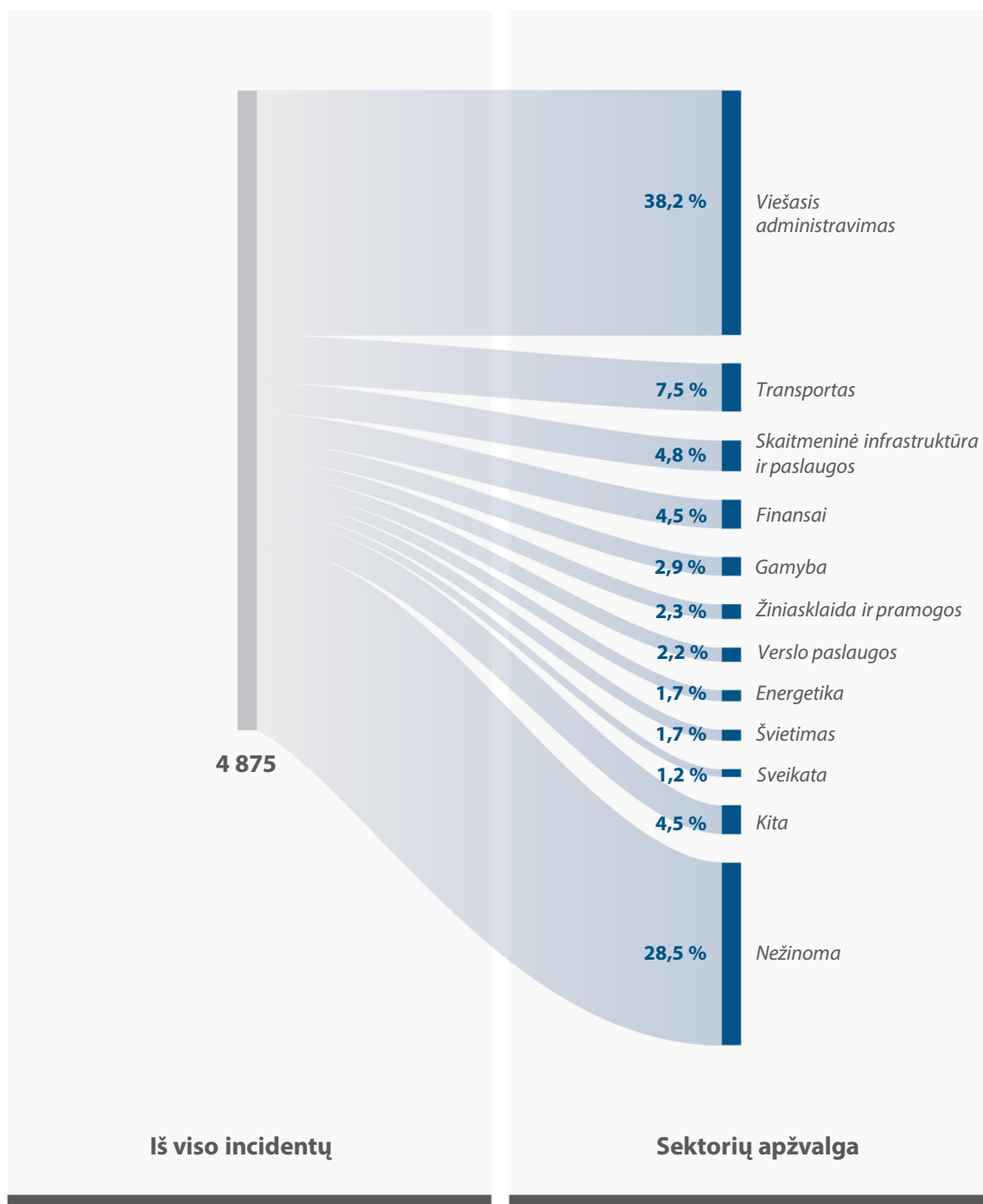
Prevencija 	Kibernetinio saugumo incidentų rizikos mažinimas ir galimo jų poveikio švelninimas <i>Pavyzdžiai: antivirusinės programos, užkardos, šifravimas, dvielementis tapatumo nustatymas, programinės įrangos atnaujinimo valdymas, darbuotojams skirti pažintiniai saugumo mokymai</i>
Aptikimas 	Kenkimo veiklos aptikimas <i>Pavyzdžiai: tinklo stebėsena, informuotumas apie padėtį</i>
Reagavimas 	Kibernetinio saugumo incidento valdymas ir poveikio mažinimas sustabdant grėsmės plitimą ir užkertant kelią tolesnei žalai <i>Pavyzdžiai: grėsmės pašalinimas, suvaldymas izoliuojant serverius, išjungiant užvaldytas paskyras ir iš naujo nustatant slaptažodžius</i>
Atsigavimas 	Paveiktų sistemų, duomenų ir paslaugų saugios ir tinkamos naudoti būklės atkūrimas <i>Pavyzdžiai: paveiktų serverių operacinių sistemų diegimas iš naujo, duomenų atkūrimas iš atsarginių kopijų, įgytos patirties analizė, tvarkų atnaujinimas</i>

Šaltinis: Audito Rūmai, remiantis Direktyvos (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui užtikrinti (TIS 2 direktyva) 78 konstatuojamąja dalimi.

02 Europos Sąjungos kibernetinio saugumo agentūra (ENISA) vertina, kad kibernetinio saugumo grėsmių lygis yra aukštas, tačiau pažymi, kad kibernetinio saugumo grėsmių padėtis tapo ir tebėra gerokai sudėtingesnė³. Šios grėsmės rodo, kad, ekonomikai ir visuomenei vis labiau skaitmenėjant, kibernetinis saugumas yra gyvybiškai svarbus. 2025 m. grėsmių padėties ataskaitoje ENISA nurodė, kad pačią didžiausią grėsmę Europos Sąjungoje kelia išpirkos reikalavimo programinė įranga. 2 diagramoje parodyti sektoriai, į kuriuos buvo nukreipti kibernetiniai išpuoliai.

³ ENISA 2024 m. ataskaita dėl kibernetinio saugumo padėties Sąjungoje.

2 diagrama | Sektoriai, į kuriuos nukreipti kibernetiniai išpuoliai



Šaltinis: Audito Rūmai, remiantis ENISA.

Reikšmingi ir didelio masto kibernetinio saugumo incidentai

- 03** Kibernetinio saugumo incidentai, kurie apima kibernetines grėsmes ir netyčinius įvykius (pavyzdžiui, nurodytus [3 diagramoje](#) ir [40 dalyje](#)), „gali trukdyti teikti viešąsias paslaugas [ir] vykdyti ekonominę veiklą, [...] sukelti didelių finansinių nuostolių, pakenkti naudotojų pasitikėjimui, padaryti didelę žalą Sąjungos ekonomikai ir demokratinėms sistemoms, o jų padariniai gali būti pavojingi net žmonių sveikatai ar gyvybei“⁴. Kibernetinio saugumo incidentas laikomas⁵:
- **reikšmingu**, jeigu dėl jo atitinkamas subjektas patyrė arba galėtų patirti didelių paslaugų teikimo sutrikimų arba finansinių nuostolių arba jeigu jis paveikė arba galėtų paveikti kitus fizinius ar juridinius asmenis sukeldamas didelę turtinę ar neturtinę žalą;
 - **didelio masto**, jeigu į jo sukeltą sutrikimą viena valstybė narė nepajėgia reaguoti arba jis daro didelį poveikį bent ne mažiau kaip dviem valstybėms narėms.
- 04** Didelio masto kibernetinio saugumo incidentas gali peraugti į plataus masto **ES kibernetinę krizę**, jeigu dėl jo vidaus rinka negali tinkamai veikti arba jis kelia rimtą pavojų visuomenės saugumui ir subjektų ar piliečių saugai keliose valstybėse narėse arba visoje ES⁶.

⁴ Reglamento (ES) 2025/38 ([Kibernetinio solidarumo akto](#)) 2 konstatuojamoji dalis.

⁵ [TIS 2 direktyvos](#) 6 ir 23 straipsniai, dėl kai kurių skaitmeninės infrastruktūros sektoriaus paslaugų teikėjų išsamiau paaiškinti [Komisijos įgyvendinimo reglamente \(ES\) 2024/2690](#).

⁶ [TIS 2 direktyvos](#) 69 konstatuojamoji dalis.

ES politikos sistema

- 05** ES kibernetinio saugumo sistema yra sudėtinga ir daugiasluoksnė, apimanti įvairias vidaus politikos sritis, pavyzdžiui, teisingumo ir vidaus reikalų, bendrosios skaitmeninės rinkos ir mokslinių tyrimų politikos sritis⁷. Išorės politikoje kibernetinis saugumas priklauso diplomatijos sričiai ir tampa vis svarbesne besiformuojančios ES gynybos politikos dalimi⁸.
- 06** Pastaraisiais metais ES sustiprino savo kibernetinio saugumo reguliavimo sistemą. Toliau pateiktoje **3 diagramoje** nurodyti aktualūs ES lygmens teisės aktai ir politikos priemonės. Atsižvelgdami į savo audito apimtį (žr. **13** ir **14** dalis), daugiausia dėmesio skyrėme priemonėms, susijusioms su reikšmingų ir didelio masto kibernetinio saugumo incidentų aptikimu ir reagavimu į juos.

⁷ Audito Rūmų apžvalginis pranešimas „Veiksmingos ES kibernetinio saugumo politikos iššūkiai“, p. 12.

⁸ Pavyzdžiui, Europos Sąjungos pozicija kibernetiniais klausimais (2022 m.), pagrindas koordinuotam ES atsakui į hibridines kampanijas (2022 m.), ES kibernetinės gynybos politika (2023 m.) ir peržiūrėtas Kibernetinio saugumo diplomatijos priemonių rinkinys (2023 m.).

3 diagrama | Aktualūs ES teisės aktai ir politikos priemonės



Šaltinis: Audito Rūmai.

Vaidmenys ir atsakomybės sritys

- 07** ES kibernetinio saugumo aplinkoje yra daug viešųjų ir privačiųjų subjektų, veikiančių regioniniu, nacionaliniu ir ES lygmenimis civilinėje srityje, įskaitant teisėsaugą. Kibernetinis saugumas taip pat yra vienas iš esminių nacionalinio saugumo ir gynybos elementų⁹. Dabartinę ES aplinką pavaizduojame **II priede**.
- 08** Valstybėms narėms tenka pagrindinė atsakomybė už joms poveikį darančių kibernetinio saugumo incidentų ir krizių prevenciją, pasirengimą jiems ir reagavimą į juos. Pagal **Europos Sąjungos sutarties 4 straipsnio 2 dalį**, atsakomybė už nacionalinį saugumą ir toliau išimtinai tenka kiekvienai valstybei narei. Kadangi kibernetinio saugumo incidentai gali sutrikdyti ar pažeisti ypatingos svarbos informacinę infrastruktūrą, nuo kurios priklauso sklandus vidaus rinkos veikimas, reikšmingo incidento ar krizės atveju svarbus vaidmuo taip pat tenka ES¹⁰. Pagrindiniai ES lygmens subjektai nurodyti toliau pateiktoje **4 diagramoje**.

⁹ Nuomonė 02/2023 dėl siūlomo Kibernetinio solidarumo akto.

¹⁰ ES kibernetinių krizių valdymo planas.

4 diagrama | Pagrindinį vaidmenį kibernetinio saugumo srityje atliekantys ES lygmens subjektai



Šaltinis: Audito Rūmai.

ES finansavimas

- 09** Pagal dabartinę 2021–2027 m. daugiamečią finansinę programą, pagrindinis kibernetinio saugumo finansavimo šaltinis yra [Skaitmeninės Europos programa \(DIGITAL\)](#). 2021 m. pradėta įgyvendinti programa yra pirmoji ES programa, kuria konkrečiai siekiama skatinti ES skaitmeninę transformaciją; jos bendras biudžetas – 8,1 milijardo eurų¹¹.
- 10** Kibernetinio saugumo veiksmai finansuojami pagal Skaitmeninės Europos programos 3 konkretų tikslą „Kibernetinis saugumas ir pasitikėjimas“. Konkrečiau, 1,4 milijardo eurų biudžetas skirtas:
- valstybių narių priemonių ir duomenų infrastruktūros koordinavimui kibernetinio saugumo srityje stiprinti;
 - plačiam kibernetinio saugumo sprendinių diegimui visose ekonomikos srityse remti.
- 11** Skaitmeninės Europos programos finansavimas kibernetiniam saugumui daugiausia skiriamas pagal kvietimus teikti pasiūlymus – nuo 2021 m. lapkričio mėn. iki 2025 m. gruodžio mėn. paskelbta 12 kvietimų. Šiems kvietimams numatytas ES finansavimas sudaro 825 milijonus eurų. 2026 ir 2027 m. planuojama paskelbti naujų kvietimų, pagal kuriuos dotacijoms bus skirta dar 212 milijonų eurų.
- 12** Kita svarbi ES programa, kuria remiamas kibernetinis saugumas, yra programa „[Europos horizontas](#)“. Kibernetinio saugumo projektai iš esmės finansuojami pagal [3 veiksmų grupę](#) „Civilinė visuomenės sauga“ ir paprastai yra ankstyvame brandos etape, nes programoje „Europos horizontas“ daugiausia dėmesio skiriama moksliniams tyrimams ir inovacijoms. Kibernetinio saugumo priemonės taip pat finansuojamos pagal [Ekonomikos gaivinimo ir atsparumo didinimo priemonę](#).

¹¹ [Skaitmeninės Europos programa](#).

Audito apimtis ir metodas

13 Padaugėjus kibernetinių grėsmių ir išaugus galimam jų poveikiui išryškėjo poreikis stiprinti mūsų kolektyvinį kibernetinį atsparumą. Mūsų audito tikslas buvo įvertinti, ar ES veiksmai rezultatyviai padeda aptikti reikšmingus ir didelio masto kibernetinio saugumo incidentus ir į juos reaguoti. Visų pirma šiuo tikslu vertinome:

- ES lygmens tinklus ir mechanizmus (t. y. CSIRT tinklą, EU-CyCLONe, Europos kibernetinio saugumo įspėjimų sistemą, Kibernetinės padėties centrą ir ES kibernetinio saugumo rezervą);
- pagal Skaitmeninės Europos programą finansuojamus veiksmus.

Nenagrinėjome ES lygmens teisėsaugos bendradarbiavimo ir kibernetinio atgrasymo veiksmų, kurių ES lygmeniu imtasi taikant diplomatines priemones ar vykdant gynybos veiklą.

14 Auditas apima 2022–2025 m. laikotarpį. Jis grindžiamas dokumentų peržiūra ir atitinkamų dokumentų analize, audito vizitais trijose valstybės narėse (Airijoje, Graikijoje ir Italijoje), taip pat rašytiniais klausimynais ir interviu su atitinkamais suinteresuotaisiais subjektais.

[5 diagramoje](#) parodyta, kaip gavome įrodymų savo pastaboms pagrįsti.

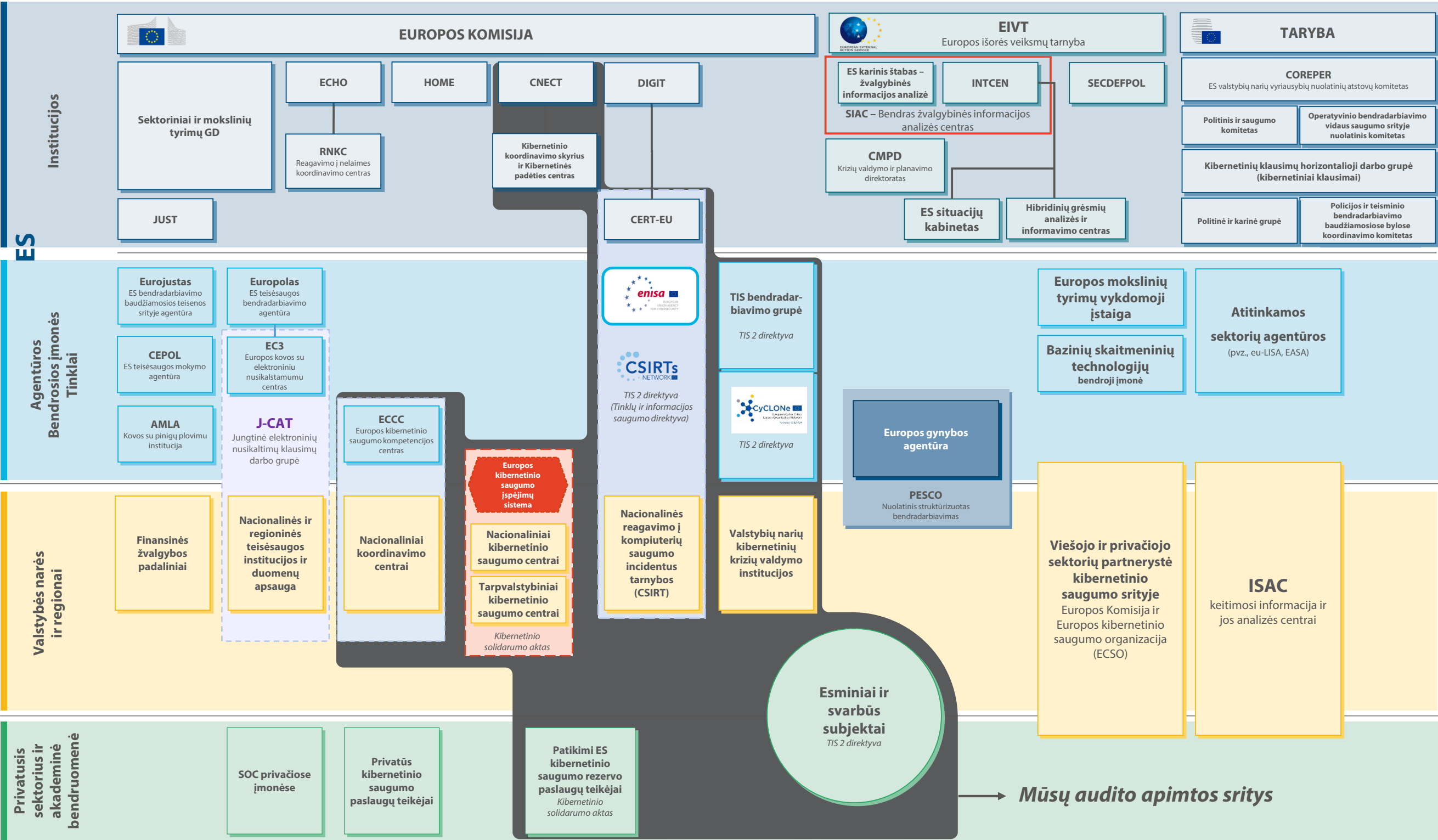
5 diagrama | Atliktas audito darbas

Tikrinome	• reikšmingų ir didelio masto kibernetinio saugumo incidentų aptikimui ir reagavimui į juos taikomą teisinę sistemą; • ES lygmeniu sukurtų tinklų ir struktūrų vaidmenis ir atsakomybės sritis.
Analizavome	• CSIRT tinklo ir EU-CyCLONe veikimo dokumentus; • Skaitmeninės Europos programos programavimo ir veiklos rezultatų stebėsenos sistemos dokumentus; • 13 atrinktų ES finansuojamų veiksmų dokumentus (11 dotacijų ir 2 sutartis; išsamus sąrašas pateiktas III priede). * Atrinkome ES finansuojamus veiksmus, įgyvendinamus trijose valstybėse narėse (Airijoje, Graikijoje ir Italijoje), kuriose atitinkamas Skaitmeninės Europos programos finansavimas buvo didesnis. 11 dotacijų atrinktos iš 137 ES finansuojamų projektų, susijusių su grėsmių aptikimu ir reagavimu į jas, sąrašo, siekiant apimti įvairaus pobūdžio projektus.
Surengėme interviu su	• 11-os į imtį įtrauktų ES finansuojamų dotacijų gavėjais; • trijų valstybių narių (Airijos, Graikijos ir Italijos) nacionalinių kibernetinio saugumo institucijų atstovais; • Europos Komisijos (CNECT GD), ENISA ir ECCC atstovais.

Šaltinis: Audito Rūmai.

- 15** Tikimės, kad mūsų nustatyti faktai padės rezultatyviau ir efektyviau ES lygmeniu aptikti reikšmingus ir didelio masto kibernetinio saugumo incidentus ir į juos reaguoti, taip pat pagerinti ES finansuotinių veiksmų atranką ir stebėseną. Mūsų [audito metodika](#) atitinka [Tarptautinės aukščiausiųjų audito institucijų organizacijos \(INTOSAI\)](#) paskelbtus tarptautinius audito standartus.

II priedas. ES kibernetinio saugumo aplinka



CNECT GD – Ryšių tinklų, turinio ir technologijų generalinis direktoratas
ECHO GD – Europos civilinės saugos ir humanitarinės pagalbos operacijų generalinis direktoratas
HOME GD – Migracijos ir vidaus reikalų generalinis direktoratas
JUST GD – Teisingumas ir vartotojų reikalų generalinis direktoratas
DIGIT GD – Skaitmeninių paslaugų generalinis direktoratas
EASA – Europos Sąjungos aviacijos saugos agentūra

EU-CyCLONe – Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas
eu-LISA – Europos Sąjungos didelės apimties IT sistemų laisvės, saugumo ir teisingumo erdvėje operacijų valdymo agentūra
INTNEN – Europos Sąjungos žvalgybos ir situacijų centras

SECDEFPOL – Saugumo ir gynybos politikos direktoratas
SOC – saugumo operacijų centras

III priedas. Atrinkti kibernetinio saugumo veiksmai

Nr.	Pavadinimas	Valstybės	Pradžios data	Pabaigos data	Visos išlaidos (mln. EUR) ir ES įnašas (%)	Nuoroda į ES finansavimo ir konkursų portalą
Dotacijos tarpvalstybiniam kibernetinio saugumo centrui, priklausantiems Europos kibernetinio saugumo įspėjimų sistemai						
1	Tarpvalstybinių SOC steigimas (ATHENA)	Bulgarija, Graikija, Kipras, Malta	2024 01 01	2028 03 31	4,7 (50 %)	🔗
2	Tarpvalstybinė ENSOC platforma (ENSOC)	Ispanija, Italija, Liuksemburgas, Nyderlandai, Austrija, Portugalija, Rumunija	2024 01 01	2028 06 30	10,4 (50 %)	🔗
Dotacijos nacionalinių koordinavimo centrų (NKC) tinklui valstybėse narėse diegti						
3	Airijos nacionalinio kibernetinio saugumo koordinavimo ir plėtros centro (NCC-IE) kūrimas ir įgyvendinimas	Airija	2023 10 02	2026 10 01	4,2 (47 %)	🔗
4	Italijos nacionalinis koordinavimo centras (NCC-IT)	Italija	2023 11 01	2025 10 31	2,0 (50 %)	🔗
Dotacijos saugumo operacijų centrų (SOC) pajėgumams stiprinti, SOC skirtoms naujoviškoms DI ir kitų didelio poveikio technologijų taikmenoms skatinti, parengties paramai ir savitarpio pagalbai teikti						
5	Graikijos konsoliduoto saugumo operacijų centro (EL-SOC) pajėgumų stiprinimas	Graikija, Kipras	2024 01 01	2026 12 31	9,7 (50 %)	🔗
6	Graikijos mažųjų ir vidutinių įmonių saugumo operacijų centras (GR-SME-SOC)	Graikija	2024 01 01	2026 12 31	12,1 (50 %)	🔗

Nr.	Pavadinimas	Valstybės	Pradžios data	Pabaigos data	Visos išlaidos (mln. EUR) ir ES įnašas (%)	Nuoroda į ES finansavimo ir konkursų portalą
7	Naujos kartos saugumo operacijų centrai (NG-SOC)	Graikija, Ispanija, Kipras, Liuksemburgas, Slovėnija, Norvegija	2024 01 01	2026 12 31	4,8 (50 %)	
8	Airijos vietos valdžios saugumo operacijų centras (ILG-SOC)	Airija	2023 10 01	2026 09 30	8,3 (50 %)	
9	Tarpusavyje sujungta kibernetinio saugumo koordinavimo ir reagavimo tinklų ekosistema („Cyber-CORE-Network“)	Airija	2024 01 01	2026 12 31	3,6 (50 %)	
10	Žmonių, procesų ir technologijų suderinimas siekiant patikimo kibernetinio saugumo („CyberSynchrony“)	Belgija, Graikija, Italija, Kipras, Nyderlandai	2024 06 01	2027 05 31	7,0 (100 %)	
11	Pažangūs bendradarbiavimui pritaikyti saugumo operacijų centrai (ACSOC)	Graikija, Italija, Rumunija	2025 01 01	2027 12 31	3,0 (50 %)	
Preliminarioji sutartis dėl ENISA kibernetinio saugumo paramos veiksmų						
12	Parama ENISA dėl paslaugų teikimo pagal Kibernetinio saugumo paramos veiksmų programą (28 pirkimo dalys)	27 valstybėms narėms skirtos pirkimo dalys 1 Europos masto pirkimo dalis	2022 12 01 ¹	2025 12 31	28,3 (100 %)	
CNECT GD Kibernetinės padėties centro paslaugų sutartis						
13	Specializuota paslauga Europos Komisijos Kibernetinės padėties ir analizės centrui remti	-	2022 12 30	2026 12 30	18,0 (100 %)	

Šaltinis: Audito Rūmai.

¹ Kelios sutartys pasirašytos 2022 m. gruodžio mėn.

IV priedas. Audito Rūmų atliktas ES finansuojamų kibernetinio saugumo projektų vertinimas

Nr. Projektas		Projektu tenkinama dauguma kvietime nurodytų poreikių	Iki šiol pasiekti planuoti projekto išdirbiai ir rezultatai	Projekto išdirbiai pateikti iki nustatyto termino	Projekto veiklos rezultatų rodikliai yra aktualūs, išmatuojami, nustatytos jų pradinės ir siektinos reikšmės
Patenkinamai Yra trūkumų Nepatenkinamai Negalima padaryti išvados (vertinti dar per anksti)					
1	Tarpvalstybinių SOC steigimas (ATHENA)				
2	Tarpvalstybinė ENSOC platforma (ENSOC)				
3	Airijos nacionalinio kibernetinio saugumo koordinavimo ir plėtros centro (NCC-IE) kūrimas ir įgyvendinimas				
4	Italijos nacionalinis koordinavimo centras (NCC-IT)				
5	Graikijos konsoliduoto saugumo operacijų centro (EL-SOC) pajėgumų stiprinimas				
6	Graikijos mažųjų ir vidutinių įmonių saugumo operacijų centras (GR-SME-SOC)				
7	Naujos kartos saugumo operacijų centrai (NG-SOC)				
8	Airijos vietos valdžios saugumo operacijų centras (ILG-SOC)				
9	Tarpusavyje sujungta kibernetinio saugumo koordinavimo ir reagavimo tinklų ekosistema („Cyber-CORE-Network“)				
10	Žmonių, procesų ir technologijų suderinimas siekiant patikimo kibernetinio saugumo („CyberSynchrony“)				
11	Pažangūs bendradarbiavimui pritaikyti saugumo operacijų centrai (ACSOC)				

Santrumpos

Santrumpa	Reikšmė (paaiškinimas)
CNECT GD	Ryšių tinklų, turinio ir technologijų generalinis direktoratas
CSIRT	Reagavimo į kompiuterių saugumo incidentus tarnyba
DIGITAL	Skaitmeninės Europos programa
ECCC	Europos kibernetinio saugumo kompetencijos centras
ENISA	Europos Sąjungos kibernetinio saugumo agentūra
EU-CyCLONe	Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas
MVĮ	mažoji ar vidutinė įmonė
NKC	nacionalinis koordinavimo centras
SOC	saugumo operacijų centras
SPG	Strateginė patariamoji grupė
TIS	tinklų ir informacijos saugumas

Žodynėlis

Terminas	Apibrėžtis (paaiškinimas)
didelio masto kibernetinio saugumo incidentas	kibernetinio saugumo incidentas, kuris yra pernelyg trikdantis, kad valstybė narė galėtų su juo susidoroti viena, arba kuris daro didelį poveikį ne mažiau kaip dviem valstybėms narėms
išpirkos reikalavimo programinė įranga	kenkimo programinė įranga, kuri blokuoja prieigą prie kompiuterinės sistemos arba užšifruoja failus taip, kad jų nebūtų galima perskaityti, paprastai taip versdama auką sumokėti išpirką už prieigos atkūrimą
kibernetinė grėsmė	galimas kibernetinės erdvės naudojimas siekiant pakenkti duomenų ar informacinių sistemų prieinamumui, autentiškumui, vientisumui ar konfidencialumui
kibernetinio saugumo centras	centrinė platforma, kurioje sutelkiamos įvairios paslaugos, priemonės ir IT specialistai, siekiant gerinti kibernetinių grėsmių stebėseną, aptikimą ir analizę, užkirsti kelią kibernetinio saugumo incidentams ir padėti rengti kibernetinių grėsmių žvalgybos informaciją
kibernetinio saugumo incidentas	įvykis, kuriuo sukeliamas pavojus duomenų ar informacinių sistemų prieinamumui, autentiškumui, vientisumui ar konfidencialumui
priešiškasis subjektas	asmuo arba grupė, kurie, pasinaudodami IT sistemų, tinklų ar įrenginių pažeidžiamumu, tyčia daro žalą, trikdo paslaugų teikimą arba vagia duomenis
reikšmingas kibernetinio saugumo incidentas	kibernetinio saugumo incidentas, dėl kurio organizacija patyrė arba gali patirti didelių veiklos sutrikimų arba finansinių nuostolių arba dėl kurio kitiems subjektams ar asmenims padaryta arba gali būti padaryta didelė žala
saugumo operacijų centras	organizacinis padalinys, kuris siekia užkirsti kelią kibernetinėms grėsmėms ir incidentams ir renka susijusią žvalgybos informaciją
taksonomija	kibernetinio saugumo srityje tai klasifikavimo sistema, pagal kurią tvarkomos, skirstomos į kategorijas ir struktūrinamos žinios apie pagrindines sąvokas, kaip antai grėsmes ir incidentus

Komisijos atsakymai

<https://www.eca.europa.eu/lt/publications/SR-2026-19>

Europos kibernetinio saugumo kompetencijos centro (ECCC) atsakymai

<https://www.eca.europa.eu/lt/publications/SR-2026-19>

Europos Sąjungos kibernetinio saugumo agentūros (ENISA) atsakymai

<https://www.eca.europa.eu/lt/publications/SR-2026-19>

Chronologija

<https://www.eca.europa.eu/lt/publications/SR-2026-19>

Audito grupė

Audito Rūmų specialiosiose ataskaitose pateikiami Audito Rūmų atliktų auditų, susijusių su įvairių sričių ES politika ir programomis arba su konkrečių biudžeto sričių valdymo temomis, rezultatai. Audito užduotis Audito Rūmai atrenka ir parengia taip, kad jos turėtų kuo didesnį poveikį, atsižvelgdami į neveiksmingumo ar neatitikties riziką, susijusių pajamų ar išlaidų lygį, būsimus pokyčius ir politinį bei viešąjį interesą.

Šį veiklos auditą atliko Audito Rūmų nario George'o-Mariaus Hyzlerio vadovaujama III audito kolegija „Išorės veiksmai, saugumas ir teisingumas“. Auditui vadovavo Audito Rūmų narys George'as-Marius Hyzleris, jam padėjo kabineto vadovas Romualdas Kayibanda ir kabineto atašė Annette Farrugia, pagrindinis vadybininkas Cyrilas Messeinas, užduoties vadovas Frédéricas Soblet, auditoriai Jurgenas Manjé ir Flavia Di Marco. Kalbinę pagalbą teikė Zoe Amador Martínez. Diagramas parengti padėjo Dunja Weibel.



Iš kairės į dešinę: Frédéricas Soblet, Romualdas Kayibanda, George'as Marius Hyzleris, Jurgenas Manjé, Cyrilas Messeinas.

AUTORIŲ TEISĖS

© Europos Sąjunga, 2026

Europos Audito Rūmų pakartotinio naudojimo politika nustatyta [Audito Rūmų sprendime Nr. 6–2019](#) dėl atvirųjų duomenų politikos ir pakartotinio dokumentų naudojimo.

Jeigu nenurodyta kitaip (pavyzdžiui, atskiruose pranešimuose dėl autorių teisių), ES priklausantis Audito Rūmų turinys yra licencijuojamas pagal [Creative Commons Attribution 4.0 International \(CC BY 4.0\) licenciją](#). Todėl paprastai pakartotinis naudojimas yra leidžiamas, jeigu tai tinkamai pažymima ir nurodomi bet kokie padaryti pakeitimai. Asmenys, kurie pakartotinai naudoja Audito Rūmų turinį, neturi iškreipti pirminės prasmės ar minties. Audito Rūmai nėra atsakingi už pakartotinio naudojimo padarinius.

Būtina gauti papildomą leidimą, jei tam tikrame turinyje vaizduojami privatūs asmenys, kurių tapatybę galima nustatyti, pavyzdžiui, Audito Rūmų darbuotojų nuotraukose, arba s Jame pateikiami trečiųjų asmenų kūriniai.

Gavus tokį leidimą, juo panaikinamas ir pakeičiamas pirmiau minėtas bendrasis leidimas ir jame aiškiai nurodomi bet kokie naudojimo apribojimai.

Siekiant naudoti ar atgaminti turinį, kuris nepriklauso ES, gali reikėti prašyti leidimo tiesiogiai iš autorių teisių turėtojų.

Viršelio nuotrauka: © 4AXY – stock.adobe.com.

6 ir 8 diagramų piktogramos: šios diagramos parengtos naudojant [Flaticon.com](#) išteklius. © Freepik Company S.L. Visos teisės saugomos.

5 diagramos žemėlapiai: [Eurostatas](#).

Programinei įrangai ar dokumentams, kuriems taikomos pramoninės nuosavybės teisės, pavyzdžiui, patentams, prekių ženklams, registruotiesiems dizainams, logotipams ir pavadinimams, Audito Rūmų pakartotinio naudojimo politika netaikoma.

Europos Sąjungos institucijų domeno „europa.eu“ svetainėse pateikiamos nuorodos į trečiųjų asmenų svetaines. Audito Rūmai jų nekontroliuoja, todėl raginame peržiūrėti jose spateiktą privatumo ir autorių teisių politiką.

Audito Rūmų logotipo naudojimas

Audito Rūmų logotipas negali būti naudojamas be išankstinio Audito Rūmų sutikimo.

HTML	ISBN 978-92-849-7877-9	ISSN 1977-5725	doi:10.2865/2164269	QJ-01-26-032-LT-Q
PDF	ISBN 978-92-849-7878-6	ISSN 1977-5725	doi:10.2865/9536527	QJ-01-26-032-LT-N

KAIP CITUOTI

Europos Audito Rūmai, [Specialioji ataskaita 19/2026](#) „Kibernetinio saugumo incidentų aptikimas ir reagavimas į juos. ES bendradarbiavimo sistema tobulėja, tačiau dėl vėluojančio įgyvendinimo ir riboto dalijimosi informacija ji tik iš dalies rezultatyvi“, Europos Sąjungos leidinių biuras, 2026.

Pastaraisiais metais ES sustiprino savo kibernetinio saugumo reguliavimo sistemą ir sukūrė tinklus bei mechanizmus kibernetinio saugumo incidentams valdyti. ES taip pat finansuoja kibernetinio saugumo projektus pagal Skaitmeninės Europos programą.

Darome išvadą, kad ES veiksmai tik iš dalies padeda aptikti reikšmingus ir didelio masto kibernetinio saugumo incidentus ir į juos reaguoti. Nors bendradarbiavimo sistema buvo nuosekliai kuriama, vis dar dirbama siekiant užtikrinti, kad ji visapusiškai veiktų. Ribotas dalijimasis informacija, pranešimų teikimo trūkumai ir smarkiai vėluojantis įgyvendinimas neleidžia išnaudoti viso ES tinklų ir mechanizmų potencialo. Projektais siekiama aktualių tikslų, tačiau įgyvendinant kai kuriuos iš jų vėluojama ar susiduriama su veiklos sunkumais. Be to, bendra veiklos rezultatų stebėsenos sistema turi trūkumų. Teikiame rekomendacijas, kaip šiuos trūkumus pašalinti.

Audito Rūmų specialioji ataskaita pagal SESV 287 straipsnio 4 dalies antrą pastraipą.



EUROPOS
AUDITO
RŪMAI



Europos Sąjungos
leidinių biuras

EUROPOS AUDITO RŪMAI
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tel. +352 4398-1

Užklausos: eca.europa.eu/lt/contact
Interneto svetainė: eca.europa.eu
Socialiniai tinklai: @EUauditors