LIETUVOS RESPUBLIKOS
VYRIAUSYBĖS KANCELIARIJA
Teisės akto projektas
2024-05-21 Nr. TAP-24-668(2)
TAIS Nr. 24-6889(3)

Projektas

LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMO NR. XII-1428 PAKEITIMO ĮSTATYMAS

2024 m. d. Nr.
Vilnius

1 straipsnis. Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 nauja redakcija

Pakeisti Lietuvos Respublikos kibernetinio saugumo įstatymą Nr. XII-1428 ir jį išdėstyti taip:

„LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMAS

I SKYRIUS BENDROSIOS NUOSTATOS

1 straipsnis. Įstatymo paskirtis ir taikymas

1. Šis įstatymas nustato kibernetinio saugumo principus, kibernetinio saugumo politiką formuojančias ir ją įgyvendinančias institucijas, jų funkcijas ir įgaliojimus, kibernetinio saugumo subjektų identifikavimo pagrindus ir šių subjektų pareigas, keitimąsi informacija ir tarpinstitucinį bendradarbiavimą, kibernetinio saugumo subjektų atitikties šio įstatymo reikalavimams patikrinimus ir vykdymo užtikrinimo priemones, nacionalinės kibernetinio saugumo sertifikavimo institucijos įgaliojimus, Saugiojo valstybinio duomenų perdavimo tinklo naudojimo pagrindus.

2. Šis įstatymas, išskyrus šio įstatymo VII skyrių, netaikomas žvalgybos institucijoms ir kredito unijoms, išskyrus kredito unijas, kurios paslaugoms teikti ar veiklai vykdyti valdo ir (ar) tvarko tinklų ir informacines sistemas nepriklausomai nuo centrinių kredito unijų.

3. Šio įstatymo 14 straipsnio, 15 straipsnio ir 18 straipsnio 1 dalies 1 punkto nuostatos netaikomos kibernetinio saugumo subjektams, jeigu jiems atskirai taikomuose Europos Sąjungos teisės aktuose keliami reikalavimai įgyvendinti kibernetinio saugumo rizikos valdymo priemones, pranešti apie didelius kibernetinius incidentus ar skirti atsakingus už kibernetinį saugumą asmenis, kurių poveikis yra bent lygiavertis šio įstatymo 14 straipsnyje ar jo pagrindu priimtuose įgyvendinamuosiuose teisės aktuose, 15 straipsnyje, 18 straipsnio 1 dalies 1 punkte ir 4 dalyje ir (ar) 18 straipsnio 1 dalies 2 punkte ir 5 dalyje nustatytų reikalavimų poveikiui.

4. Šio straipsnio 3 dalyje nurodytų reikalavimų poveikis yra laikomas lygiaverčiu:

1) šio įstatymo 14 straipsnyje ar jo pagrindu priimtuose įgyvendinamuosiuose teisės aktuose nustatytų reikalavimų poveikiui, jeigu nustatytos kibernetinio saugumo rizikos valdymo priemonės apima priemones, kuriomis siekiama užtikrinti tinklų ir informacinių sistemų saugumą prieinamumo, autentiškumo, vientisumo ir konfidencialumo atžvilgiu, be to, yra grindžiamos visus pavojus apimančiu požiūriu, įskaitant tinklų ir informacinių sistemų fizinį ir aplinkos saugumą;

2) šio įstatymo 15 straipsnyje nustatytų reikalavimų poveikiui, jeigu yra numatytos atsakingų už kibernetinį saugumą asmenų skyrimo pareigos, kurių poveikis yra bent lygiavertis šio įstatymo 15 straipsnyje nustatytiems reikalavimams;

3) šio įstatymo 18 straipsnio 1 dalies 1 punkte ir 4 dalyje nustatytų reikalavimų poveikiui, jeigu yra numatyta reagavimo į kibernetinius incidentus tarnybos neatidėliotina prieiga, kai tinkama, automatinė ir tiesioginė, prie pateiktų pranešimų apie incidentus, o nustatyti reikalavimai pranešti

apie didelius incidentus pagal poveikį yra bent lygiaverčiai šio įstatymo 18 straipsnio 1 dalies 1 punkte ir 4 dalyje nustatytiems reikalavimams;

4) šio įstatymo 18 straipsnio 1 dalies 2 punkte ir 5 dalyje nustatytų reikalavimų poveikiui, jeigu yra numatyta reagavimo į kibernetinius incidentus tarnybos neatidėliotina prieiga, kai tinkama, automatinė ir tiesioginė, prie pateiktų pranešimų apie incidentus, o nustatyti reikalavimai pranešti apie didelius incidentus pagal poveikį yra bent lygiaverčiai šio įstatymo 18 straipsnio 1 dalies 2 punkte ir 5 dalyje nustatytiems reikalavimams.

5. Lietuvos Respublikos Vyriausybė šio įstatymo 1 ir 2 prieduose nurodytuose atskiruose sektoriuose politiką formuojančių ministerijų teikimu patvirtina konkrečių šio įstatymo 1 ir 2 prieduose nurodytiems sektoriams taikomų Europos Sąjungos teisės aktų, atitinkančių šio straipsnio 4 dalyje nurodytus kriterijus, sąrašą. Šiame sąraše nustatomi šio įstatymo 1 ir 2 prieduose nurodytiems sektoriams taikomi Europos Sąjungos teisės aktai, atitinkantys bent vieną šio straipsnio 4 dalyje nurodytą kriterijų.

6. Šio įstatymo nuostatos suderintos su Europos Sąjungos teisės aktais, nurodytais šio įstatymo 3 priede.

2 straipsnis. Pagrindinės šio įstatymo sąvokos

1. **Aukščiausio lygio domenų vardų registro paslaugas teikiantis subjektas** – subjektas, atsakingas už aukščiausio lygio domeno administravimą, apimantį domenų vardų registraciją aukščiausio lygio domene ir techninį to aukščiausio lygio domeno veikimą, įskaitant jo vardų serverių veikimą, duomenų bazių techninę priežiūrą ir aukščiausio lygio domenų zonos rinkmenų paskirstymą tarp vardų serverių, neatsižvelgiant į tai, ar bet kurias iš tų operacijų atlieka pats subjektas, ar tai yra užsakomosios paslaugos, neįskaitant atvejų, kai registras aukščiausio lygio domenų vardus naudoja tik savo reikmėms.

2. **Debesijos kompiuterijos paslauga** – informacinės visuomenės paslauga, kuri pagal poreikį suteikia administravimo paslaugas ir plataus masto nuotolinę prieigą prie kintamo masto pritaikomos bendrų ir paskirstytų kompiuterijos išteklių bazės, įskaitant atvejus, kai tokie ištekliai yra paskirstyti per kelias vietas.

3. **Didelė kibernetinė grėsmė** – kibernetinė grėsmė, dėl kurios techninių charakteristikų galima daryti prielaidą, kad ji gali padaryti didelį neigiamą poveikį subjekto arba subjekto paslaugų naudotojų tinklų ir informacinėms sistemoms, sukeldama didelę turtinę arba neturtinę žalą.

4. **Domenų vardų registravimo paslaugas teikiantis subjektas** – registratorius arba registratorių vardu veikiantis subjektas, įskaitant privatumo ar įgaliotojo tarpininkavimo registravimo paslaugų teikėją arba perpardavėją.

5. **Domenų vardų sistema** – hierarchiškai paskirstyta vardų sistema, kurioje galima identifikuoti interneto paslaugas ir išteklius ir kurioje sudaromos sąlygos galutiniams naudotojams naudotis interneto maršruto parinkimo ir junglumo paslaugomis ir gauti tas paslaugas bei išteklius.

6. **Domenų vardų sistemos paslaugų teikėjas** – subjektas, kuris teikia viešai prieinamas rekursinio domenų vardų keitimo paslaugas galutiniams interneto naudotojams arba patikimo domenų vardų keitimo paslaugas trečiųjų šalių reikmėms, išskyrus šakninių vardų serverius.

7. **Duomenų centro paslauga** – paslauga, kuri apima struktūras arba struktūrų grupes, skirtas informacinių technologijų ir tinklo įrangos centralizuotam pritaikymui, tarpusavio junglumui ir eksploatavimui, teikiant duomenų saugojimo, tvarkymo ir perdavimo paslaugas kartu su visa energijos paskirstymo ir aplinkos kontrolės įranga ir infrastruktūra.

8. **Elektroninės informacijos prieglobos paslaugos** – paslaugos, kurias sudaro paslaugos gavėjo pateiktos informacijos saugojimas jo prašymu.

9. **Interneto duomenų srautų mainų taškas** – tinklo įrenginys, kuris sudaro sąlygas sujungti daugiau nei du nepriklausomus tinklus (autonomines sistemas), visų pirma siekiant palengvinti

interneto duomenų srautų mainus, kuris sujungia tik autonomines sistemas ir nereikalauja, kad interneto duomenų srautai, perduodami tarp bet kurių naudojamų autonominių sistemų porų, būtų perduodami per bet kurią trečią autonominę sistemą, ir nekeičia tokių srautų ar kitokiu būdu jų netrikdo.

10. **Kibernetinė erdvė** – aplinka, kurią sudaro kompiuteriai ir kita tinklų ir informacinių technologijų įranga ir juose sukuriami ir (ar) jais perduodami skaitmeniniai duomenys.

11. **Kibernetinio incidento valdymas** – visi veiksmai ir procedūros, kuriais siekiama užkirsti kibernetiniam incidentui kelią, atskleisti, išanalizuoti ir sustabdyti kibernetinį incidentą arba į jį reaguoti ir atkurti veiklą po kibernetinio incidento.

12. **Kibernetinis incidentas** – įvykis, kuriuo sukeliamas pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui.

13. **Kibernetinio saugumo rizika** – potencialus praradimas arba sutrikimas, kurį sukėlė kibernetinis incidentas, ir kuri turi būti išreikšta kaip tokio praradimo arba sutrikimo masto ir kibernetinio incidento tikimybės derinys.

14. **Kibernetinio saugumo subjektas** – subjektas, registruotas Kibernetinio saugumo subjektų registre.

15. **Nacionalinė kibernetinio saugumo strategija** – nuosekli sistema, kurioje nustatyti Lietuvos Respublikos kibernetinio saugumo srities strateginiai tikslai ir prioritetai ir jų įgyvendinimo valdymas.

16. **Saugusis valstybinis duomenų perdavimo tinklas** – valstybės valdomas specialiuosius organizacinius ir techninius reikalavimus atitinkantis ir nuo viešųjų elektroninių ryšių tinklų nepriklausomas elektroninių ryšių tinklas.

17. **Socialinių tinklų paslaugų platforma** – interneto platforma, kuri sudaro galimybę galutiniams naudotojams naudojantis įvairiais įrenginiais prisijungti, dalytis turiniu, rasti vienas kitą ir skelbiamą turinį, visų pirma per pokalbius, įrašus, vaizdo įrašus ir rekomendacijas.

18. **Subjektas** – fizinis asmuo arba juridinis asmuo, įsteigtas ir tokiu pripažintas pagal jo įsteigimo vietos nacionalinę teisę, kuris, veikdamas savo vardu, naudojasi teisėmis ir kuriam gali būti taikomos pareigos.

19. **Šakninis vardų serveris** – vardų serveris, esantis aukščiausio lygio domenų vardų sistemos struktūroje, kuris atsako į užklausas grąžindamas atitinkamo aukščiausio lygio domeno vardų serverių sąrašą.

20. **Tinklų ir informacinė sistema** – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami šiomis nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais.

21. **Tinklų ir informacinės sistemos spraga** – tinklų ir informacinės sistemos trūkumas, įskaitant informacinių ir ryšių technologijų produktų arba informacinių ir ryšių technologijų paslaugų trūkumus, dėl kurio gali įvykti kibernetinis incidentas ar kuriuo gali būti pasinaudota kibernetinei grėsmei kelti.

22. **Tinklų ir informacinių sistemų saugumas** – tinklų ir informacinių sistemų pajėgumas tam tikru patikimumo lygiu išlikti atspariems bet kokiam įvykiui, galinčiam sukelti pavojų saugomų, perduodamų ar tvarkomų duomenų arba teikiamų ar per tas tinklų ir informacines sistemas gaunamų paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui.

23. **Turinio teikimo tinklas** – geografiškai paskirstytų serverių tinklas, kurio paskirtis yra turinio ir paslaugų teikėjų vardu užtikrinti interneto naudotojams didelę skaitmeninio turinio ir paslaugų pasiūlą, prieinamumą arba greitą teikimą.

24. **Valdomų paslaugų teikėjas** – subjektas, teikiantis paslaugas, susijusias su informacinių ir ryšių technologijų produktų, tinklų, infrastruktūros, taikomųjų programų ar bet kurių kitų tinklų ir informacinių sistemų diegimu, valdymu, naudojimu ar technine priežiūra, teikiantis pagalbą arba aktyvaus administravimo paslaugas klientų patalpose arba nuotoliniu būdu.

25. **Valdomų saugumo paslaugų teikėjas** – valdomų paslaugų teikėjas, vykdantis veiklą, susijusią su kibernetinio saugumo rizikos valdymu, arba teikiantis pagalbą tokiai veiklai vykdyti.

26. **Vos neįvykęs kibernetinis incidentas –** įvykis, kuriuo galėjo būti sukeltas pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui, bet kuriam įvykti buvo sėkmingai užkirstas kelias arba kuris neįvyko.

27. Šiame įstatyme vartojamos sąvokos „Europos kibernetinio saugumo sertifikavimo schema“, „Europos kibernetinio saugumo sertifikatas“, „akreditavimas“ ir „atitikties vertinimo įstaiga“, „informacinių ir ryšių technologijų produktas“, „informacinių ir ryšių technologijų paslauga“, „informacinių ir ryšių technologijų procesas“, „kibernetinė grėsmė“, „kibernetinis saugumas“ suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2019/881. Sąvokos „Kibernetinio saugumo kompetencijos bendruomenė“, „Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras“, „Nacionalinių koordinavimo centrų tinklas“ šiame įstatyme suprantamos taip, kaip jos vartojamos Reglamente (ES) 2021/887. Sąvokos „patikimumo užtikrinimo paslauga“, „patikimumo užtikrinimo paslaugų teikėjas“, „kvalifikuota patikimumo užtikrinimo paslauga“, „kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas“ šiame įstatyme suprantamos taip, kaip jos apibrėžtos Reglamente (ES) Nr. 910/2014. Sąvoka „interneto paieškos sistema“ šiame įstatyme suprantama taip, kaip ji apibrėžta Reglamente (ES) 2019/1150. Sąvokos „standartas“, „techninė specifikacija“ šiame įstatyme suprantamos taip, kaip jos apibrėžtos Reglamente (ES) Nr. 1025/2012. Sąvoka „duomenys“ suprantama taip, kaip apibrėžta Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.

28. Kitos šiame įstatyme vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos elektroninių ryšių įstatyme, Lietuvos Respublikos viešojo administravimo įstatyme, Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatyme, Lietuvos Respublikos nesąžiningos komercinės veiklos vartotojams draudimo įstatyme, Lietuvos Respublikos smulkiojo ir vidutinio verslo plėtros įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos žvalgybos įstatyme, Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatyme, Lietuvos Respublikos informacinės visuomenės įstatyme, Lietuvos Respublikos elektros energetikos įstatyme, Lietuvos Respublikos alternatyviųjų degalų įstatyme, Lietuvos Respublikos atsinaujinančių išteklių energetikos įstatyme, Lietuvos Respublikos naftos produktų ir naftos valstybės atsargų įstatyme, Lietuvos Respublikos gamtinių dujų įstatyme, Lietuvos Respublikos geležinkelių transporto kodekse, Lietuvos Respublikos saugios laivybos įstatyme, Lietuvos Respublikos transporto veiklos pagrindų įstatyme, Lietuvos Respublikos finansinių priemonių rinkų įstatyme, Lietuvos Respublikos farmacijos įstatyme, Lietuvos Respublikos geriamojo vandens įstatyme, Lietuvos Respublikos geriamojo vandens tiekimo ir nuotekų tvarkymo įstatyme, Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatyme, Lietuvos Respublikos pašto įstatyme, Lietuvos Respublikos atliekų tvarkymo įstatyme, Lietuvos Respublikos mokslo ir studijų įstatyme, Lietuvos Respublikos civiliniame kodekse, Lietuvos Respublikos informacinės visuomenės paslaugų įstatyme.

3 straipsnis. Kibernetinio saugumo principai

1. Kibernetinis saugumas grindžiamas šiais kibernetinio saugumo principais:

1) kibernetinės erdvės nediskriminavimo – teisės aktų nuostatos yra taikomos, o teisės aktų saugomų gėrių apsauga yra užtikrinama vienodai tiek fizinėje, tiek kibernetinėje erdvėje;

2) kibernetinio saugumo rizikos valdymo – taikomos kibernetinio saugumo rizikos valdymo priemonės turi užtikrinti kibernetinio saugumo subjektų reguliariai įvertinamos rizikos suvaldymą;

3) kibernetinio saugumo proporcingumo – taikomos kibernetinio saugumo rizikos valdymo priemonės neturi apriboti kibernetinio saugumo subjektų veiklos labiau, negu tai būtina kibernetiniam saugumui užtikrinti;

4) viešojo intereso viršenybės – taikomos kibernetinio saugumo rizikos valdymo priemonės pirmiausia turi užtikrinti viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų, kibernetinio saugumo subjektų teisių ir teisėtų interesų ar neproporcingai apriboti jų laisvės;

5) standartizacijos ir technologinio neutralumo – įgyvendinant kibernetinio saugumo rizikos valdymo priemones, kibernetinio saugumo subjektai skatinami vadovautis nacionaliniais, Europos Sąjungos ir kitais tarptautiniais tinklų ir informacinių sistemų saugumo standartais ir techninėmis specifikacijomis, nereikalaujant taikyti kokios nors konkrečios rūšies technologijos ir nesuteikiant jai pirmenybės;

6) subsidiarumo – už tinklų ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinį saugumą yra atsakingi šias sistemas valdantys ir paslaugas jomis teikiantys kibernetinio saugumo subjektai. Srityse, kurios priklauso išimtinei kibernetinio saugumo subjektų kompetencijai, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos veiksmų imasi tik tada, kai tinklų ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinio saugumo neužtikrina šias sistemas valdantys ir paslaugas jomis teikiantys kibernetinio saugumo subjektai.

2. Taikant kibernetinį saugumą reglamentuojančias teisės normas, turi būti atsižvelgiama į visus šio straipsnio 1 dalyje nurodytus principus. Šie principai turi būti derinami tarpusavyje, nė vienam iš jų iš anksto nesuteikiama pirmenybė.

II SKYRIUS
KIBERNETINIO SAUGUMO POLITIKOS FORMAVIMAS IR ĮGYVENDINIMAS

4 straipsnis. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos

1. Kibernetinio saugumo politika formuojama, atsižvelgiant į Lietuvos Respublikos Seimo tvirtinamoje Nacionalinio saugumo strategijoje nustatytus ilgojo laikotarpio nacionalinio saugumo politikos prioritetus ir uždavinius, Vyriausybės tvirtinamame Nacionaliniame pažangos plane nustatytus strateginius tikslus ir uždavinius, Seimo tvirtinamoje Krašto apsaugos sistemos stiprinimo ir plėtros bei Vyriausybės tvirtinamoje Nacionalinės kibernetinio saugumo plėtros programose numatytus uždavinių įgyvendinimo prioritetus ir kryptis. Šioje dalyje nurodyti strateginio planavimo dokumentai ar jų dalys kartu su šiuo įstatymu ir jį įgyvendinančiais teisės aktais sudaro nacionalinę kibernetinio saugumo strategiją.

2. Kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija. Lietuvos Respublikos užsienio reikalų ministerija formuojant kibernetinio saugumo politiką dalyvauja tiek, kiek reikia nustatyti diplomatinių priemonių taikymo reaguojant į kibernetines grėsmes ir kibernetinius incidentus teisinį reguliavimą. Nacionalinis kibernetinio saugumo centras formuojant kibernetinio saugumo politiką dalyvauja tiek, kiek šiame įstatyme nustatytoms funkcijoms atlikti reikia nustatyti kibernetinio saugumo subjektų veiklos ir priežiūros teisinį reguliavimą.

3. Kibernetinio saugumo politiką įgyvendina Nacionalinis kibernetinio saugumo centras, Lietuvos policija ir Valstybinė duomenų apsaugos inspekcija.

5 straipsnis. Krašto apsaugos ministerijos įgaliojimai kibernetinio saugumo srityje

Krašto apsaugos ministerija, be šio įstatymo 4 straipsnio 2 dalyje numatyto kibernetinio saugumo politikos formavimo ir kitų šio įstatymo nustatytų funkcijų vykdymo, taip pat

bendradarbiauja su atitinkamomis Šiaurės Atlanto sutarties organizacijos (toliau – NATO) bei Europos Sąjungos ir NATO bei Europos Sąjungos valstybių institucijomis, tarptautinėmis institucijomis kibernetinio saugumo klausimais.

6 straipsnis. Kibernetinio saugumo taryba

1. Kibernetinio saugumo taryba (toliau – Taryba) yra nuolatinė kolegiali nepriklausoma visuomeniniais pagrindais veikianti patariamoji institucija, besikeičianti su Tarybos atstovais gerąja praktika ir žiniomis kibernetinio saugumo srityje bei teikianti pasiūlymus Krašto apsaugos ministerijai dėl:

1) kibernetinio saugumo politikos prioritetų, plėtros krypčių, siektinų rezultatų ir jų įgyvendinimo būdų;

2) viešojo sektoriaus, verslo ir mokslo bendradarbiavimo galimybių kibernetinio saugumo užtikrinimo srityje;

3) kibernetinio saugumo rizikos valdymo priemonių, kibernetinių incidentų valdymo ir kibernetinio saugumo stiprinimo krypčių.

2. Tarybą sudaro kibernetinio saugumo politiką formuojančių, dalyvaujančių formuojant ir ją įgyvendinančių institucijų atstovai, šio įstatymo 1 ir 2 prieduose nurodytų institucijų, atsakingų už kibernetinio saugumo subjektų identifikavimą, atstovai, kibernetinio saugumo subjektams atstovaujančių asociacijų, mokslo ir studijų institucijų atstovai ir šio įstatymo 23 straipsnyje nurodyti Kibernetinio saugumo bendruomenės nariai.

3. Tarybai vadovauja Krašto apsaugos ministerijos atstovas.

4. Tarybą sudaro, jos narių skaičių tvirtina, institucinę ir personalinę sudėtį nustato ir jos darbo reglamentą tvirtina krašto apsaugos ministras.

5. Tarybą ūkiškai ir techniškai aptarnauja Krašto apsaugos ministerija ar ministro įgaliota institucija.

6. Taryba, siekdama jai nustatytų veiklos tikslų, turi šias teises:

1) gauti iš valstybės ir savivaldybių institucijų, įstaigų bei kitų juridinių asmenų reikalingą informaciją Tarybos kompetencijai priskirtiems klausimams spręsti;

2) organizuoti pasitarimus, konferencijas ir kitus renginius.

7 straipsnis. Nacionalinis kibernetinio saugumo centras

1. Nacionalinis kibernetinio saugumo centras yra įstaiga prie Krašto apsaugos ministerijos.

2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:

1) taiko kibernetinių grėsmių paieškos priemones kibernetinėje erdvėje, siekdamas įvertinti tinklų ir informacinių sistemų atsparumą kibernetiniams incidentams;

2) stebi, renka ir analizuoja informaciją apie kibernetines grėsmes, tinklų ir informacinių sistemų spragas (toliau – spraga), kibernetinius incidentus ir vos neįvykusius kibernetinius incidentus;

3) valdo kibernetinius incidentus nacionalinio kibernetinių incidentų valdymo plano, tvirtinamo Vyriausybės, nustatyta tvarka;

4) kibernetinio saugumo subjektams ir suinteresuotiesiems subjektams teikia ankstyvuosius perspėjimus, įspėjimus, pranešimus ir keičiasi informacija apie kibernetines grėsmes, spragas, kibernetinius incidentus ir vos neįvykusius kibernetinius incidentus;

5) kibernetinio saugumo subjektams teikia pagalbą, susijusią su jų tinklų ir informacinių sistemų stebėjimu;

6) siekdamas stabdyti kibernetinio incidento poveikį kibernetinio saugumo subjektų tinklų ir informacinių sistemų saugumui, duoda nurodymą viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjams, elektroninių prekyviečių, interneto paieškos sistemų, debesijos kompiuterijos paslaugų teikėjams, elektroninės informacijos prieglobos paslaugų teikėjams ne ilgiau

negu 48 valandoms apriboti viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų, elektroninių prekyviečių, interneto paieškos sistemų, debesijos kompiuterijos paslaugų, elektroninės informacijos prieglobos paslaugų teikimą. Nacionalinis kibernetinio saugumo centras apie viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjams pagal šį punktą duotus nurodymus ne vėliau kaip kitą darbo dieną praneša Lietuvos Respublikos ryšių reguliavimo tarnybai;

7) siekdamas pašalinti kibernetines grėsmes ar stabdyti jų plitimą, duoda nurodymą viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjams ir (ar) domenų vardų paslaugų teikėjams blokuoti interneto svetainių, platinančių kenkimo kodus, apgaulės būdu renkančius prisijungimus prie tinklų ir informacinių sistemų ir (ar) naudojamus siekiant koordinuoti ir vykdyti kibernetinius incidentus, domenų vardus, taip pat kitus domenų vardus, sukurtus minėtoms interneto svetainių veikloms vykdyti. Dėl Nacionalinio kibernetinio saugumo centro nurodymo blokuoti interneto svetainės domeno vardą jos savininkas turi teisę kreiptis į teismą Lietuvos Respublikos civilinio proceso kodekso nustatyta tvarka;

8) kibernetinio incidento metu taiko būtinas kibernetinio saugumo priemones;

9) tikrina kibernetinio saugumo subjektų valdomas ir (ar) tvarkomas tinklų ir informacines sistemas, siekdamas nustatyti spragas;

10) koordinuoja spragų atskleidimą;

11) renka ir analizuoja kibernetinio incidento tyrimo duomenis ir vykdo kibernetinio saugumo rizikų bei kibernetinių incidentų analizę, taip pat užtikrina kibernetinio saugumo politiką formuojančių ir įgyvendinančių institucijų, taip pat kibernetinio saugumo subjektų informavimą apie padėtį kibernetinio saugumo srityje;

12) kai būtina informuoti visuomenę siekiant išvengti kibernetinio incidento arba valdyti vykstantį kibernetinį incidentą arba iškilusią kibernetinę grėsmę, prieš tai pasikonsultavęs su kibernetinio saugumo subjektu, pranešusiu apie kibernetinį incidentą, informuoja visuomenę apie kibernetinį incidentą ir (ar) kibernetinę grėsmę, jeigu įmanoma, nurodydamas veiksmus, kurių būtina imtis reaguojant į tą kibernetinį incidentą ir (ar) kibernetinę grėsmę, arba reikalauja, kad tai padarytų informaciją pateikęs kibernetinio saugumo subjektas;

13) dalyvauja valdant krizes, susijusias su kibernetiniais incidentais, Krizių valdymo ir civilinės saugos įstatymo nustatyta tvarka;

14) koordinuojant Nacionaliniam krizių valdymo centrui praneša Europos Sąjungos institucijoms apie šio straipsnio 2 dalies 13 punkte nurodytas krizes, kurių viena Lietuvos Respublika nepajėgia suvaldyti;

15) dalyvauja Europos Sąjungos ir NATO įsteigtų reagavimo į kibernetinius incidentus tinklų veikloje ir teikia savitarpio pagalbą pagal savo pajėgumus ir kompetenciją kitiems šių tinklų nariams jų prašymu;

16) atlieka kibernetinio saugumo subjektų atitikties kibernetinio saugumo rizikos valdymo priemonėms stebėseną;

17) konsultuoja kibernetinio saugumo subjektus kibernetinio saugumo rizikos valdymo priemonių parinkimo ir taikymo klausimais;

18) bendradarbiauja su Europos Sąjungos, NATO ir kitų valstybių institucijomis ir organizacijomis, įgyvendinančiomis kibernetinio saugumo politiką, tarptautinėmis organizacijomis, turi teisę jas pasitelkti kartu atliekant šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje;

19) kartu su verslo subjektais, mokslo ir studijų institucijomis, nacionalinėmis, Europos Sąjungos, NATO ir kitų valstybių institucijomis ir organizacijomis, tarptautinėmis organizacijomis, nevyriausybinėmis organizacijomis bei kibernetinio saugumo subjektais plėtoja nacionalinį kibernetinį saugumą stiprinančius projektus;

20) atlieka kitas šiame įstatyme nustatytas funkcijas.

3. Nacionalinis kibernetinio saugumo centras, atlikdamas šio straipsnio 2 dalies 16 punkte nurodytas funkcijas, kibernetinio saugumo auditui atlikti turi teisę pasitelkti nepriklausomą auditorių, audito įmonę ar kitą instituciją, kuri atitinka Nacionalinio kibernetinio saugumo centro nustatytus nepriklausomumo, nešališkumo ir nepriekaištingos reputacijos reikalavimus. Atliekant kibernetinio saugumo auditą turi būti užtikrinamas kibernetinio saugumo subjekto valdomų ir (ar) tvarkomų tinklų ir informacinės sistemos kibernetinis saugumas.

4. Nacionalinio kibernetinio saugumo centro pritaikytas priemones ir nurodymus kibernetinio saugumo subjektai ir kiti subjektai turi teisę skųsti teismui Administracinių bylų teisenos įstatymo nustatyta tvarka, išskyrus šiame įstatyme nurodytus atvejus, kai taikoma kita apskundimo tvarka.

5. Nacionalinis kibernetinio saugumo centras turi atitikti šiuos reikalavimus:

1) Nacionalinio kibernetinio saugumo centro ryšio kanalai turi būti lengvai prieinami išvengiant kritinių funkcionavimo trikties taškų;

2) turi būti nustatoma keletas būdų, kaip bet kuriuo metu susisiekti su Nacionaliniu kibernetinio saugumo centru ir su kitais subjektais, apie šiuos būdus ir ryšių kanalus informuojant kibernetinio saugumo subjektus ir kitas šio įstatymo 20 straipsnyje nurodytas institucijas;

3) Nacionalinio kibernetinio saugumo centro patalpos ir pagalbinės informacinės sistemos turi būti saugiose vietose;

4) Nacionalinis kibernetinio saugumo centras turi turėti prašymų valdymo ir perdavimo sistemą, užtikrinančią veiksmingą ir efektyvų prašymų perdavimą;

5) Nacionalinis kibernetinio saugumo centras privalo užtikrinti savo veiklos konfidencialumą ir patikimumą;

6) Nacionalinis kibernetinio saugumo centras privalo turėti pakankamai darbuotojų, kad būtų užtikrintas Nacionalinio kibernetinio saugumo centro pasiekiamumas bet kuriuo metu,

7) Nacionalinio kibernetinio saugumo centro darbuotojai turi būti tinkamai apmokyti vykdyti funkcijas;

8) Nacionalinis kibernetinio saugumo centras turi turėti antrines sistemas ir atsarginę darbo erdvę, kad būtų užtikrintas Nacionalinio kibernetinio saugumo centro funkcijų tęstinumas.

6. Krašto apsaugos ministerija privalo užtikrinti, kad Nacionalinis kibernetinio saugumo centras turėtų pakankamai pajėgumų ir išteklių, reikalingų šio straipsnio 2 dalyje nustatytoms funkcijoms vykdyti, atitiktų šio straipsnio 5 dalyje nustatytus reikalavimus, ir plėtoti Nacionalinio kibernetinio saugumo centro techninius pajėgumus.

8 straipsnis. Pagalba valdant kibernetinius incidentus

1. Nacionalinis kibernetinio saugumo centras tvarko duomenis apie kibernetinio saugumo subjektus, kitas įstaigas ir ūkio subjektus, kuriems, įvykus ekstremaliajam įvykiui kibernetinėje erdvėje, būtų pavedamos būtinosios užduotys valdant kibernetinius incidentus.

2. Nacionalinis kibernetinio saugumo centras šio straipsnio 1 dalyje nurodytiems kibernetinio saugumo subjektams, kitoms įstaigoms ir ūkio subjektams organizuoja kibernetinio saugumo pratybas ir mokymus, siekdamas užtikrinti pasirengimą krizėms, ekstremaliosioms situacijoms kibernetinio saugumo srityje, tvirtina pratybų planą.

9 straipsnis. Valstybinės duomenų apsaugos inspekcijos įgaliojimai kibernetinio saugumo srityje

Valstybinė duomenų apsaugos inspekcija įgyvendina kibernetinio saugumo politiką asmens duomenų apsaugos srityje ir atlieka Reglamente (ES) 2016/679 nustatytas priežiūros institucijos užduotis.

10 straipsnis. Policijos įgaliojimai kibernetinio saugumo srityje

1. Policija, įgyvendindama kibernetinio saugumo politiką:

1) gauna ir tvarko duomenis ir (ar) informaciją apie kibernetinius incidentus nusikalstamų veikų prevencijos, analizės, tyrimo ar atskleidimo tikslais;

2) turi teisę iš kibernetinio saugumo subjektų gauti informaciją, reikalingą kibernetinių incidentų analizei ir vertinimui, ar kibernetinis incidentas turi galimų nusikalstamos veikos požymių, atlikti. Kibernetinio saugumo subjektai privalo policijos prašymu teikti šiame punkte nurodytą informaciją;

3) turi teisę, kai paslaugų gavėjas galimai dalyvauja ar jo naudojama tinklų ir informacinių technologijų įranga galimai yra naudojama nusikalstamai veikai, be teismo sankcijos duoti nurodymą viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjui, elektroninės informacijos prieglobos paslaugų teikėjui, elektroninių prekyviečių, interneto paieškos sistemų, debesijos kompiuterijos paslaugų teikėjams ne ilgiau kaip 48 valandoms, o ilgesniam laikui – su apylinkės teismo sankcija apriboti viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų, elektroninių prekyviečių, interneto paieškos sistemų, debesijos kompiuterijos paslaugų teikimą paslaugų gavėjui ir (ar) nurodyti taikyti priemones nusikalstamų veikų kibernetinėje erdvėje priežastims šalinti. Šiais atvejais teisėjui pateikiamas teikimas dėl veiksmų teisėtumo ar pagrįstumo patvirtinimo motyvuota nutartimi. Jeigu šiame punkte nurodytas paslaugų teikimo apribojimo terminas baigiasi poilsio ar švenčių dieną, teikimas pateikiamas ne vėliau kaip kitą darbo dieną po poilsio ar švenčių dienos. Teisėjas turi išnagrinėti teikimą ir priimti nutartį dėl teikime nurodytų veiksmų teisėtumo ar pagrįstumo ne vėliau kaip per 3 darbo dienas nuo prašymo pateikimo dienos. Jeigu teisėjas motyvuota nutartimi nepatvirtina teikime nurodytų veiksmų teisėtumo ar pagrįstumo, nurodymas nedelsiant stabdomas;

4) turi teisę duoti nurodymą viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjui, elektroninės informacijos prieglobos paslaugų teikėjui, elektroninių prekyviečių, interneto paieškos sistemų, debesijos kompiuterijos paslaugų teikėjams išsaugoti su jų teikiamomis paslaugomis susijusią informaciją, iš kurios galima nustatyti naudotos ryšio paslaugos tipą, taikytas priemones ir naudojimo laiką, paslaugos gavėjo tapatybę, pašto, geografinės padėties adresą, ryšio numerį, informaciją apie sąskaitas ir atliktus mokėjimus paslaugos sutarties arba susitarimo pagrindu ir kitą informaciją ryšių aparatūros įrengimo vietoje, turimą pagal paslaugos sutartį arba susitarimą, šią informaciją gauti, o kai yra motyvuota teismo nutartis, gauti paslaugų gavėjo srauto duomenis ir kontroliuoti šiame punkte nurodytos perduodamos informacijos turinį.

2. Policijos nurodymus dėl paslaugų teikimo jų gavėjui apribojimo ar (ir) taikyti priemones nusikalstamų veikų kibernetinėje erdvėje priežastims šalinti, ar (ir) nurodymus paslaugų teikėjams išsaugoti su jų teikiamomis paslaugomis susijusią informaciją privaloma įvykdyti ne vėliau kaip per 8 valandas nuo policijos nurodymo įteikimo, o pagrįstais skubos atvejais kaip įmanoma greičiau, ir bet kuriuo atveju ne vėliau kaip per vieną valandą nuo nurodymo gavimo.

III SKYRIUS
KIBERNETINIO SAUGUMO SUBJEKTŲ IDENTIFIKAVIMAS IR ŠIŲ SUBJEKTŲ PAREIGOS

11 straipsnis. Kibernetinio saugumo subjektai

1. Kibernetinio saugumo subjekto statusą įgyja ir Kibernetinio saugumo subjektų registre registruojami subjektai, atitinkantys bent vieną iš šio straipsnio 3–5 dalyse nurodytų bendrųjų ar specialiųjų kibernetinio saugumo subjektų identifikavimo kriterijų ir šiuose kriterijuose nurodytoms paslaugoms teikti ar veiklai vykdyti valdantys ir (ar) tvarkantys tinklų ir informacines sistemas. Atsižvelgiant į galimą neigiamą poveikį, kurį kibernetinis incidentas gali padaryti kibernetinio saugumo subjektų valdomoms ir (ar) tvarkomoms tinklų ir informacinėms sistemoms, kibernetinio

saugumo subjektai skirstomi į esminius kibernetinio saugumo subjektus (toliau – esminiai subjektai) ir svarbius kibernetinio saugumo subjektus (toliau – svarbūs subjektai).

2. Kibernetinio saugumo subjektai įgyja pareigas, numatytas kibernetinio saugumo subjektams, tik nuo jų įregistravimo Kibernetinio saugumo subjektų registre.

3. Bendrieji esminių subjektų identifikavimo kriterijai:

1) subjektas teikia paslaugas ir (ar) vykdo veiklą šio įstatymo 1 priede nurodytuose sektoriuose ir viršija vidutinių įmonių darbuotojų skaičių ir finansinius duomenis apibrėžiančias ribas, nustatytas Smulkiojo ir vidutinio verslo plėtros įstatyme;

2) subjektas šio įstatymo 1 priede nurodytame skaitmeninės infrastruktūros sektoriuje teikia kvalifikuotas patikimumo užtikrinimo paslaugas, aukščiausio lygio domeno vardų registro paslaugas ar domenų vardų sistemos (toliau – DNS) paslaugas, išskyrus šakninių vardų serverių operatorius;

3) subjektas šio įstatymo 1 priede nurodytame skaitmeninės infrastruktūros sektoriuje teikia viešąsias elektroninių ryšių tinklų ar viešąsias elektroninių ryšių paslaugas ir yra laikomas vidutine įmone pagal Smulkiojo ir vidutinio verslo plėtros įstatymą;

4) subjektas Krizių valdymo ir civilinės saugos įstatymo nustatyta tvarka yra pripažintas ypatingos svarbos subjektu;

5) subjektas šio įstatymo 1 priede nurodytame viešojo administravimo sektoriuje teikia paslaugas ir (ar) vykdo veiklą ir yra laikomas centriniu valstybinio administravimo, regioninio administravimo subjektu ir savivaldybių administravimo subjektu pagal Viešojo administravimo įstatymą;

6) subjektas Valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka valdo ir (ar) tvarko ypatingos svarbos ir (ar) svarbius valstybės informacinius išteklius;

7) subjektas yra laikomas nacionaliniam saugumui užtikrinti svarbia įmone arba subjekto valdoma ir (ar) tvarkoma tinklų ir informacinė sistema yra įrašyta į nacionaliniam saugumui užtikrinti svarbių įrenginių ir turto sąrašą.

4. Bendrieji svarbių subjektų identifikavimo kriterijai:

1) subjektas teikia paslaugas ir (ar) vykdo veiklą šio įstatymo 2 priede nurodytuose sektoriuose ir viršija mažų įmonių darbuotojų skaičių ir finansinius duomenis apibrėžiančias ribas, nustatytas Smulkiojo ir vidutinio verslo plėtros įstatyme;

2) subjektas teikia paslaugas ir (ar) vykdo veiklą šio įstatymo 1 priede nurodytuose sektoriuose ir viršija mažų įmonių darbuotojų skaičių ir finansinius duomenis apibrėžiančias ribas, tačiau neviršija vidutinių įmonių darbuotojų skaičių ir finansinius duomenis apibrėžiančių ribų, nustatytų Smulkiojo ir vidutinio verslo plėtros įstatyme;

3) subjektas teikia nekvalifikuotas patikimumo užtikrinimo paslaugas šio įstatymo 1 priede nurodytame skaitmeninės infrastruktūros sektoriuje ir yra laikomas vidutine, maža ar labai maža įmone pagal Smulkiojo ir vidutinio verslo plėtros įstatymą;

4) subjektas teikia viešąsias elektroninių ryšių tinklų ar viešąsias elektroninių ryšių paslaugas šio įstatymo 1 priede nurodytame skaitmeninės infrastruktūros sektoriuje ir yra laikomas maža ar labai maža įmone pagal Smulkiojo ir vidutinio verslo plėtros įstatymą;

5) subjektas valdo ir (ar) tvarko valstybės informacinius išteklius;

6) subjektas teikia domenų vardų registravimo paslaugas;

7) subjektas teikia elektroninės informacijos prieglobos paslaugas.

5. Specialieji kibernetinio saugumo subjektų identifikavimo kriterijai:

1) subjektas yra vienintelis paslaugos, kuri yra būtina siekiant užtikrinti ypatingos svarbos visuomeninės ar ekonominės veiklos vykdymą Lietuvos Respublikoje, teikėjas;

2) paslaugos, kurią teikia subjektas, sutrikimas galėtų daryti didelį poveikį viešajam saugumui, visuomenės saugumui arba visuomenės sveikatai;

3) paslaugos, kurią teikia subjektas, sutrikimas galėtų kelti didelę sisteminę riziką sektoriuose, kuriuose toks sutrikimas galėtų daryti tarpvalstybinį poveikį;

4) subjektas yra ypatingos svarbos atsižvelgiant į jo konkrečią svarbą konkrečiam sektoriui ar paslaugos rūšiai arba kitiems tarpusavyje priklausomiems sektoriams nacionaliniu ar regioniniu lygmeniu;

5) subjektas šio įstatymo 1 priede nurodytame viešojo administravimo sektoriuje teikia paslaugas ir (ar) vykdo veiklą, kuriai sutrikus galėtų būti didelis poveikis valstybei, institucijoms ar gyventojams, ir yra laikomas teritoriniu valstybinio administravimo subjektu ar regioniniu administravimo subjektu, ar savivaldybių administravimo subjektu pagal Viešojo administravimo įstatymą;

6) paslaugos, kurią teikia subjektas, sutrikimas galėtų daryti didelį poveikį esminio subjekto teikiamai paslaugai ir (ar) vykdomai veiklai;

7) subjektas yra paslaugos, kuri yra būtina gyvybiškai svarbioms valstybės funkcijoms atlikti ir valstybinėms mobilizacinėms užduotims vykdyti, teikėjas;

8) subjektas šio įstatymo 1 priede nurodytame mokslinių tyrimų sektoriuje vykdo ypatingos svarbos mokslinių tyrimų ir eksperimentinės plėtros veiklą.

6. Vyriausybė nustato identifikavimo pagal specialiuosius kriterijus metodiką, pagal kurią subjektas priskiriamas esminiams arba svarbiems subjektams. Pagal šio straipsnio 5 dalies 5 punkte nurodytą kriterijų identifikuojami tik esminiai subjektai, o pagal šio straipsnio 5 dalies 8 punkte nurodytą kriterijų identifikuojami tik svarbūs subjektai.

7. Jeigu subjektas atitinka bent vieną šio straipsnio 4 ar 5 dalyse nurodytą kriterijų, kuriuo identifikuojamas esminis subjektas, laikoma, kad subjektas yra esminis subjektas nepriklausomai nuo jo atitikties svarbaus subjekto kriterijams.

12 straipsnis. Jurisdikcija ir teritoriškumas

1. Identifikuojant kibernetinio saugumo subjektus laikoma, kad Lietuvos Respublikos jurisdikcijai priklauso:

1) subjektai, registruoti ar įsisteigę Lietuvos Respublikoje, išskyrus:

a) viešojo administravimo subjektus, kurie yra įsteigti kitos valstybės;

b) šios dalies 3 punkte nurodyti subjektai, kurių pagrindinė buveinė yra ne Lietuvos Respublikoje;

2) viešojo administravimo subjektai, kuriuos Lietuvos Respublika įsteigė kitose valstybėse;

3) DNS paslaugų teikėjai, aukščiausio lygio domenų vardų registro paslaugas teikiantys subjektai, domenų vardų registravimo paslaugas teikiantys subjektai, debesijos kompiuterijos paslaugų teikėjai, duomenų centrų paslaugų teikėjai, turinio teikimo tinklo paslaugų teikėjai, valdomų paslaugų teikėjai, valdomų saugumo paslaugų teikėjai, elektroninių prekyviečių, interneto paieškos sistemų ar socialinio tinklo paslaugų platformų paslaugų teikėjai, kurių pagrindinė buveinė yra Lietuvos Respublikoje;

4) viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjai, teikiantys šias paslaugas Lietuvos Respublikoje.

2. Laikoma, kad šio straipsnio 1 dalies 3 punkte nurodyta pagrindinė buveinė yra Lietuvos Respublikoje, jeigu šio straipsnio 1 dalies 3 punkte nurodyti subjektai yra registruoti ar įsisteigę Lietuvos Respublikoje. Laikoma, kad šio straipsnio 1 dalies 3 punkte nurodyta pagrindinė buveinė yra Lietuvos Respublikoje, jeigu su kibernetinio saugumo rizikos valdymo priemonėmis susiję sprendimai yra priimami Lietuvos Respublikoje. Jeigu Europos Sąjungos valstybė, kurioje priimami tokie sprendimai, nenustatoma arba tokie sprendimai Europos Sąjungoje nepriimami, laikoma, kad pagrindinė buveinė yra Lietuvos Respublikoje, kai Lietuvos Respublikoje įgyvendinamos kibernetinio saugumo rizikos valdymo priemonės. Jeigu nenustatoma Europos Sąjungos valstybė,

kurioje įgyvendinamos kibernetinio saugumo rizikos valdymo priemonės, laikoma, kad pagrindinė buveinė yra Lietuvos Respublikoje, jeigu subjektas Lietuvos Respublikoje turi padalinį, kuriame dirba daugiausia jo darbuotojų Europos Sąjungoje.

3. Jei šio straipsnio 1 dalies 3 punkte nurodytas subjektas nėra įsisteigęs Europos Sąjungoje, bet teikia paslaugas Lietuvos Respublikoje, jis privalo paskirti Europos Sąjungoje įsisteigusį fizinį arba juridinį asmenį veikti tik DNS paslaugų teikėjo, aukščiausio lygio domenų vardų registro paslaugas teikiančio subjekto, domenų vardų registravimo paslaugas teikiančio subjekto, debesijos kompiuterijos paslaugų teikėjo, duomenų centro paslaugų teikėjo, turinio teikimo tinklo paslaugų teikėjo, valdomų paslaugų teikėjo, valdomų saugumo paslaugų teikėjo, elektroninės prekyvietės paslaugų teikėjo, interneto paieškos sistemos paslaugų teikėjo arba socialinio tinklo paslaugų platformų paslaugų teikėjo, kuris nėra įsisteigęs Europos Sąjungoje, vardu, į kurį Nacionalinis kibernetinio saugumo centras gali kreiptis vietoj subjekto dėl to subjekto pareigų pagal šį įstatymą (toliau – atstovas) Europos Sąjungoje. Šioje dalyje nurodytas atstovas turi būti įsisteigęs vienoje iš tų valstybių narių, kuriose siūlomos paslaugos. Jei šio straipsnio 1 dalies 3 punkte nurodytas subjektas skiria atstovą Lietuvos Respublikoje arba jo nepaskiria, bet teikia paslaugas Lietuvos Respublikoje, laikoma, kad toks subjektas priklauso Lietuvos Respublikos jurisdikcijai.

13 straipsnis. Kibernetinio saugumo subjektų registras

1. Kibernetinio saugumo subjektų registro objektas yra kibernetinio saugumo subjektai.

2. Kibernetinio saugumo subjektų registro objektas ir jį apibūdinantys duomenys tvarkomi Kibernetinio saugumo informaciniame tinkle.

3. Kibernetinio saugumo subjektų registrą sudaro šie pagrindiniai duomenys apie kibernetinio saugumo subjektus:

1) jeigu kibernetinio saugumo subjektas yra juridinis asmuo – kibernetinio saugumo subjekto pavadinimas, juridinio asmens kodas, teisinis statusas, ekonominės veiklos forma, pagrindinės buveinės adresas (jeigu kibernetinio saugumo subjektas nėra įsisteigęs Europos Sąjungoje – pagal šio įstatymo 12 straipsnio 3 dalį paskirto atstovo pavadinimas, teisinis statusas, ekonominės veiklos forma, registracijos numeris, kontaktiniai duomenys (elektroninio pašto adresas, ryšio numeris ir adresas) ir kitų juridinių padalinių Europos Sąjungoje adresai, jei kibernetinio saugumo subjektas yra DNS paslaugų teikėjas, aukščiausio lygio domenų vardų registro paslaugas teikiantis subjektas, debesijos kompiuterijos paslaugų teikėjas, duomenų centrų paslaugų teikėjas, turinio teikimo tinklo paslaugų teikėjas, valdomų paslaugų teikėjas, valdomų saugumo paslaugų teikėjas, internetines prekyvietes, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų paslaugų teikėjas (toliau – specialusis subjektas) ar yra domenų vardų registravimo paslaugas teikiantis subjektas;

2) jeigu kibernetinio saugumo subjektas yra fizinis asmuo – kibernetinio saugumo subjekto vardas, pavardė, asmens kodas, veiklos vykdymo adresas;

3) kibernetinio saugumo subjekto kontaktiniai duomenys (elektroninio pašto adresas, ryšio numeris);

4) kibernetinio saugumo subjekto teikiamos paslaugos ir (ar) vykdomos veiklos, atitinkančios šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus;

5) kibernetinio saugumo subjekto naudojami interneto protokolo (IP) adresų rėžiai;

6) valstybės, kuriose kibernetinio saugumo subjektas teikia paslaugas ir (ar) vykdo veiklą, nurodytą šio įstatymo 1 ir 2 prieduose nurodytuose sektoriuose ir subsektoriuose;

7) kibernetinio saugumo subjekto paslaugų teikimui ar veiklai reikšmingos tinklų ir informacinės sistemos;

8) šio įstatymo 1 ir 2 prieduose nurodytas sektorius, kuriame kibernetinio saugumo subjektas veikia ar teikia paslaugas, subsektorius, subjekto rūšis kibernetinio saugumo subjekto sektorius, subsektorius, subjekto rūšis.

4. Subjektas, atitinkantis šio įstatymo 11 straipsnio 3–5 dalyse nustatytus kibernetinio saugumo subjektų identifikavimo kriterijus, Kibernetinio saugumo informacinio tinklo duomenų tvarkytojui pateikia duomenis, nurodytus Kibernetinio saugumo informacinio tinklo nuostatuose, tvirtinamuose Krašto apsaugos ministerijos. Duomenys teikiami šiuose nuostatuose nustatyta tvarka.

5. Kibernetinio saugumo subjektus registruoja ir išregistruoja Kibernetinio saugumo informacinio tinklo duomenų tvarkytojas Kibernetinio saugumo informacinio tinklo nuostatuose nustatyta tvarka.

6. Šio įstatymo 1 ir 2 prieduose nurodytos institucijos, atsakingos už kibernetinio saugumo subjektų identifikavimą, dalyvauja kibernetinio saugumo subjektų registravimo procese Kibernetinio saugumo informacinio tinklo nuostatuose nustatyta tvarka.

7. Kibernetinio saugumo informacinio tinklo duomenų tvarkytojas Kibernetinio saugumo informacinio tinklo nuostatuose nustatytais atvejais ir tvarka identifikuodamas ir registruodamas kibernetinio saugumo subjektus turi teisę neatlygintinai gauti iš identifikuojamų subjektų, kitų valstybės institucijų, valstybės įstaigų, valstybės valdomų įmonių, viešųjų įstaigų, savivaldybių valdomų įmonių ir savivaldybių įstaigų šio straipsnio 3 dalyje nurodytus duomenis ir kitą šiuos duomenis apibūdinančią informaciją, reikalingą kibernetinio saugumo subjektams registruoti.

8. Subjektai turi teisę skųsti sprendimą juos registruoti Kibernetinio saugumo subjektų registre Lietuvos Respublikos administracinių bylų teisenos įstatymo nustatyta tvarka.

9. Jei kibernetinio saugumo subjektas neatitinka šio įstatymo 11 straipsnio 3–5 dalyse nurodytų kriterijų, jis išregistruojamas iš Kibernetinio saugumo subjektų registro. Kibernetinio saugumo subjektas išregistruojamas iš Kibernetinio saugumo subjektų registro per 20 darbo dienų nuo momento, kai Kibernetinio saugumo informacinio tinklo duomenų tvarkytojas gauna informacijos, kad kibernetinio saugumo subjektas nebeatitinka šio įstatymo 11 straipsnio 3–5 dalyse nurodytų kriterijų. Kibernetinio saugumo subjektas netenka šiame įstatyme nurodytų kibernetinio saugumo subjektams taikomų pareigų nuo jo išregistravimo iš Kibernetinio saugumo subjektų registro.

10. Kibernetinio saugumo subjektai šio įstatymo 1 ir 2 prieduose nurodytiems sektoriams, subsektoriams ir subjekto rūšiai priskiriami pagal Ekonominės veiklos rūšių klasifikatorių Kibernetinio saugumo informacinio tinklo nuostatuose nustatyta tvarka.

14 straipsnis. Kibernetinio saugumo rizikos valdymo priemonės

1. Kibernetinio saugumo subjektai privalo užtikrinti šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus atitinkančiai veiklai vykdyti ar paslaugoms teikti naudojamų tinklų ir informacinių sistemų atitiktį kibernetinio saugumo rizikos valdymo priemonėms:

1) kibernetinio saugumo reikalavimams, tvirtinamiems Vyriausybės, išskyrus šio straipsnio 2 dalyje nurodytus atvejus;

2) Europos Komisijos priimtiems įgyvendinimo aktams, pagal šio straipsnio 3 dalyje nurodytas priemones nustatantiems techninius ir metodinius reikalavimus.

2. Kibernetinio saugumo subjektai privalo šio straipsnio 1 dalies 1 punkte nurodytus kibernetinio saugumo reikalavimus įgyvendinti per Vyriausybės nustatytą ne trumpesnį nei 12 mėn. terminą nuo jų įtraukimo į Kibernetinio saugumo subjektų registrą. Nustatydama terminą Vyriausybė privalo atsižvelgti į kibernetinio saugumo reikalavimams įgyvendinti reikalingus žmogiškuosius ir finansinius išteklius.

3. Kibernetinio saugumo subjektai privalo Nacionaliniam kibernetinio saugumo centrui pateikti duomenis apie kibernetinio saugumo rizikos valdymo priemonių įgyvendinimą. Kibernetinio saugumo informacinio tinklo nuostatuose nurodyti duomenys apie kibernetinio saugumo rizikos valdymo priemonių įgyvendinimą teikiami šiuose nuostatuose nustatyta tvarka.

4. Specialusis subjektas privalo užtikrinti jų naudojamų tinklų ir informacinių sistemų atitiktį tik šio straipsnio 1 dalies 2 punkte nurodytiems teisės aktams.

5. Kibernetinio saugumo reikalavimai apima šiuos elementus:

1) kibernetinio saugumo rizikos analizės, tinklų ir informacinių sistemų kibernetinio saugumo politiką;

2) už kibernetinį saugumą atsakingų asmenų, nurodytų šio įstatymo 15 straipsnyje, ir kibernetinio saugumo subjekto vadovo ar jo įgalioto asmens pareigas;

3) kibernetinių incidentų valdymą;

4) veiklos tęstinumą;

5) tiekimo grandinės saugumą, įskaitant aspektus, susijusius su kiekvieno kibernetinio saugumo subjekto ir jo tiesioginių tiekėjų ar paslaugų teikėjų santykius;

6) tinklų ir informacinių sistemų įsigijimą, plėtojimą ir priežiūros saugumą, įskaitant spragų valdymą ir atskleidimą;

7) politiką ir procedūras, skirtas kibernetinio saugumo reikalavimų veiksmingumui įvertinti;

8) kibernetinės higienos praktiką ir reguliarius kibernetinio saugumo mokymus;

9) kriptografijos ir šifravimo naudojimo politiką ir procedūras;

10) žmogiškųjų išteklių saugumą, prieigos kontrolės politiką ir turto valdymą;

11) kelių veiksnių tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių ryšių sistemų subjekto viduje naudojimą;

12) kibernetinio saugumo subjektų naudotojų, administratorių, tiekėjų, jų subtiekėjų ir kitų ūkio subjektų teisių ir prieigos prie kibernetinio saugumo subjektų valdomų ir (ar) tvarkomų tinklų ir informacinių sistemų ir (ar) skaitmeninių duomenų suteikimo ir valdymo politiką;

13) kitus atskiriems sektoriams arba atskiroms kibernetinio saugumo subjektų grupėms taikomus kibernetinio saugumo reikalavimus, nustatytus atsižvelgiant į atskiruose sektoriuose identifikuotas kibernetinio saugumo rizikas.

6. Kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo privalo užtikrinti, kad kibernetinio saugumo subjektas laikytųsi šiame įstatyme jam nustatytų pareigų, ir prižiūrėti jų laikymąsi. Kibernetinio saugumo subjekto vadovas, įgaliodamas šioje dalyje nurodytą asmenį, užtikrina, kad jis turėtų būtinų priemonių, reikalingų nurodytam įgaliojimui vykdyti.

7. Kibernetinio saugumo subjekto valdymo organų nariai, vadovas ir jo įgaliotas asmuo, jeigu toks yra, ar kibernetinio saugumo subjektas, jei jis yra fizinis asmuo, privalo ne rečiau kaip kartą per 2 metus Nacionalinio kibernetinio saugumo centro vadovo nustatyta tvarka išklausyti kibernetinio saugumo mokymus bei užtikrinti kibernetinio saugumo subjekto darbuotojų nuolatinį švietimą kibernetinio saugumo srityje.

8. Kibernetinio saugumo subjektai ne rečiau kaip kartą per 3 metus atlieka kibernetinio saugumo auditą pagal Nacionalinio kibernetinio saugumo centro patvirtintą metodiką. Kibernetinio saugumo auditą atlieka nepriklausomi visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų saugumo atitikties auditoriai, audito įmonės ar kitos institucijos, kurios atitinka Nacionalinio kibernetinio saugumo centro metodikoje nustatytus nepriklausomumo, nešališkumo ir nepriekaištingos reputacijos reikalavimus, ar asmenys, Nacionalinio kibernetinio saugumo centro vadovo nustatyta tvarka išklausę mokymus ir išlaikę kvalifikacinius žinių ir praktinių įgūdžių patikrinimo egzaminą toliau kartu – auditoriai). Auditoriams negali būti pavedama vertinti tinklų ir informacinių sistemų, kurias valdo ir (ar) tvarko subjektas, kuriame dirba auditorius, saugos.

15 straipsnis. Už kibernetinį saugumą atsakingi asmenys

1. Kibernetinio saugumo subjekto vadovas ar jo įgaliotas asmuo privalo paskirti kibernetinio saugumo vadovą, tiesiogiai atskaitingą kibernetinio saugumo subjekto vadovui, atsakingą už atitikties

šio įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantį kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas.

2. Kibernetinio saugumo subjekto vadovas ar jo įgaliotas asmuo privalo paskirti saugos įgaliotinį, atsakingą už konkrečios tinklų ir informacinės sistemos atitiktį šio įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams ir atliekantį kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas.

3. Kibernetinio saugumo vadovas gali vykdyti saugos įgaliotinio funkcijas. Kibernetinio saugumo vadovas gali būti paskirtas atsakingas už šio įstatymo 14 ir 18 straipsniuose nustatytų reikalavimų, taikomų keliems kibernetinio saugumo subjektams, gyvendinimą. Saugos įgaliotinis gali būti paskirtas atsakingas už kelių tinklų ir informacinių sistemų atitiktį šio įstatymo 14 straipsnyje nustatytiems reikalavimams. Tinklų ir informacinės sistemos valdytojas turi teisę pavesti šios tinklų ir informacinės sistemos tvarkytojui paskirti saugos įgaliotinį. Sprendimą dėl šioje dalyje numatytų už kibernetinį saugumą atsakingų asmenų skyrimo priima kibernetinio saugumo subjekto vadovas, atsižvelgdamas į kibernetinio saugumo subjekto organizacinę struktūrą ir dydį.

4. Kibernetinio saugumo subjektui leidžiama iš tiekėjo įsigyti paslaugas, kurių metu būtų vykdomos už kibernetinį saugumą atsakingų asmenų funkcijos. Įsigyjant šioje dalyje numatytas paslaugas, turi būti užtikrinamas šio įstatymo 14 ir 18 straipsniuose nustatytų reikalavimų įgyvendinimas.

5. Už kibernetinį saugumą atsakingi asmenys:

1) turi atitikti Lietuvos Respublikos valstybės tarnybos įstatyme nustatytus nepriekaištingos reputacijos reikalavimus, keliamus asmeniui, einančiam valstybės tarnautojo pareigas;

2) negali turėti paskirtos administracinės nuobaudos už teisės aktų pažeidimus tinklų ir informacinių sistemų ir asmens duomenų tvarkymo ir privatumo apsaugos srityse arba nuo nuobaudos paskyrimo turi būti praėję ne mažiau kaip vieni metai;

3) gali būti skiriami, jeigu turi ne mažiau kaip 2 metų patirtį informacinių technologijų, kibernetinio saugumo ar tinklų ir informacinių sistemų srityje arba turi žinias šiose srityse patvirtinantį aukštojo mokslo diplomą, tarptautiniu lygmeniu pripažįstamą kvalifikacijos sertifikatą ar Nacionalinio kibernetinio saugumo centro vadovo nustatyta tvarka yra išklausę mokymus ir išlaikę kibernetinio saugumo vadovo egzaminą.

6. Jei kibernetinio saugumo subjektas yra fizinis asmuo, jam netaikomi šiame straipsnyje nustatyti reikalavimai.

16 straipsnis. Techninės kibernetinio saugumo priemonės

1. Vykdydamas esminių subjektų valdomų ir (ar) tvarkomų tinklų ir informacinių sistemų stebėseną, siekdamas identifikuoti kibernetines grėsmes ir kibernetinius incidentus, Nacionalinis kibernetinio saugumo centras esminių subjektų tinklų ir informacinėse sistemose diegia ir valdo technines kibernetinio saugumo priemones. Svarbių subjektų valdomose ir (ar) tvarkomose tinklų ir informacinėse sistemose techninės kibernetinio saugumo priemonės gali būti diegiamos jų prašymu, siekiant suvaldyti kibernetinius incidentus. Šioje dalyje numatytų priemonių diegimas ir naudojimas atliekamas taip, kad būtų užtikrinamas kibernetinio saugumo subjektų valdomų ir (ar) tvarkomų tinklų ir informacinės sistemos saugumas, nepertraukiamas veikimas, kibernetinio saugumo subjekto duomenų ir informacijos slaptumas, konfidencialumas, prieinamumas bei atsparumas, tinkama kibernetinio saugumo subjektų, kitų subjektų teisių ir teisėtų interesų apsauga.

2. Krašto apsaugos ministras nustato techninių kibernetinio saugumo priemonių diegimo ir valdymo kibernetinio saugumo subjektų valdomose ir (ar) tvarkomose tinklų ir informacinėse sistemose tvarką, tvirtina techninių kibernetinio saugumo priemonių diegimo planą, kuriame nustato technines kibernetinio saugumo priemones, šiomis priemonėmis tvarkomus duomenis (jeigu jie yra tvarkomi).

3. Nacionalinio kibernetinio saugumo centro lėšomis įdiegtos techninės kibernetinio saugumo priemonės prižiūrimos, jų diegimas, naudojimas, remontas ir aptaranavimas atliekamas Nacionalinio kibernetinio saugumo centro lėšomis.

4. Esminiai subjektai privalo sudaryti sąlygas Nacionaliniam kibernetinio saugumo centrui diegti ir valdyti technines kibernetinio saugumo priemones.

17 straipsnis. Reikalavimai aukščiausio lygio domenų vardų registro ir domenų vardų registravimo paslaugų teikimui

Kibernetinio saugumo subjektai, kurie yra aukščiausio lygio domenų vardų registro paslaugas teikiantys subjektai ir domenų vardų registravimo paslaugas teikiantys subjektai, privalo:

1) siekdami prisidėti prie DNS saugumo, stabilumo ir atsparumo, kaupti informaciją, pagal kurią būtų galima nustatyti domenų vardų turėtojus ir kontaktinius asmenis, administruojančius aukščiausio lygio domenų vardais pažymėtus domenų vardus, ir su jais susisiekti, laikydamiesi Reglamento (ES) 2016/679 reikalavimų, kai tvarkomi asmens duomenys. Tokia informacija apima:

a) domeno vardą;

b) registracijos datą;

c) domeno vardo turėtojo juridinio asmens pavadinimą ar fizinio asmens vardą ir pavardę, kontaktinius duomenis (elektroninio pašto adresas, ryšio numeris);

d) domeno vardą administruojančio kontaktinio asmens elektroninio pašto adresą ir ryšio numerį, jei jie skiriasi nuo domeno vardo turėtojo duomenų;

2) taikyti politiką ir procedūras, įskaitant tikrinimo procedūras, kuriomis užtikrinama, kad domenų vardų registracijos duomenų bazėje būtų pateikiama tiksli ir išsami informacija;

3) skelbti šio straipsnio 2 ir 5 punktuose nurodytą politiką ir procedūras viešai savo interneto svetainėse ar, jeigu jie interneto svetainės neturi, kitomis visuomenės informavimo priemonėmis;

4) nepagrįstai nedelsdami po domeno vardo užregistravimo paskelbti viešai jų interneto svetainėse ar, jeigu jie interneto svetainės neturi, kitomis visuomenės informavimo priemonėmis domeno vardo registracijos duomenis, kurie nėra asmens duomenys;

5) gavę teisėtus ir pagrįstus teisėtos prieigos prie domenų vardų registracijos duomenų, kurie yra asmens duomenys, prašančių subjektų prašymus, pagal taikomą duomenų atskleidimo politiką ir procedūras suteikti prieigą prie konkrečių domenų vardų registracijos duomenų, laikydamiesi Reglamento (ES) 2016/679 nustatytos tvarkos. Atsakymai prašančiam subjektui turi būti teikiami nepagrįstai nedelsiant ir bet kuriuo atveju ne vėliau kaip per 72 valandas nuo tada, kai gaunamas prašymas suteikti prieigą;

6) siekdami nedubliuoti domenų vardų registracijos duomenų rinkimo, bendradarbiauti tarpusavyje.

18 straipsnis. Pranešimai apie kibernetinius incidentus

1. Kibernetinio saugumo subjektai privalo pranešti Nacionaliniam kibernetinio saugumo centrui apie:

1) didelį kibernetinį incidentą, darantį poveikį jų šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus atitinkančiai vykdomai veiklai ir (ar) teikiamoms paslaugoms;

2) šios dalies 1 punkte nenurodytus kibernetinius incidentus, darančius poveikį jų šio įstatymo 11 straipsnio 3–5 dalyse nurodytus kriterijus atitinkančiai vykdomai veiklai ir (ar) teikiamoms paslaugoms, nacionalinio kibernetinių incidentų valdymo plano, tvirtinamo Vyriausybės, nustatytais terminais ir pateikti Vyriausybės nustatytą informaciją.

2. Kibernetinis incidentas laikomas dideliu bent vienu iš šių atvejų:

1) jeigu dėl kibernetinio incidento atitinkamas subjektas patyrė arba gali patirti didelių paslaugų teikimo sutrikimų arba finansinių nuostolių;

2) jeigu kibernetinis incidentas paveikė arba gali paveikti kitus fizinius ar juridinius asmenis, sukeldamas didelę turtinę arba neturtinę žalą.

3. Atvejai, kai kibernetinis incidentas laikomas dideliu, išsamiau apibrėžiami Europos Komisijos priimamuose įgyvendinimo aktuose.

4. Pranešant apie didelį kibernetinį incidentą pateikiama:

1) nedelsiant, bet ne vėliau kaip per 24 valandas nuo sužinojimo apie didelį kibernetinį incidentą – ankstyvasis perspėjimas, kuriame pagal galimybes nurodoma, ar didelį kibernetinį incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai ir ar jis galėtų daryti tarpvalstybinį poveikį;

2) nedelsiant, bet ne vėliau kaip per 72 valandas nuo sužinojimo apie didelį kibernetinį incidentą – pranešimas apie kibernetinį incidentą, kuriame pagal galimybes atnaujinama šios dalies 1 punkte nurodyta informacija ir nurodomas didelio kibernetinio incidento, įskaitant jo sunkumą ir poveikį, pradinis vertinimas, taip pat nurodomi įsilaužimo įrodymai, jei tokių yra;

3) Nacionalinio kibernetinio saugumo centro prašymu – tarpinė atitinkamų atnaujintų padėties duomenų ataskaita per Nacionalinio kibernetinio saugumo centro nurodytą pateikimo terminą;

4) ne vėliau kaip per vieną mėnesį nuo šios dalies 1 punkte nurodyto pranešimo apie kibernetinį incidentą – galutinė ataskaita, kurioje pateikiama ši informacija:

a) išsamus kibernetinio incidento, įskaitant jo sunkumą ir poveikį, aprašymas;

b) grėsmės arba pagrindinės priežasties, dėl kurios kibernetinis incidentas galėjo būti sukeltas, rūšis;

c) taikomos ir įgyvendinamos kibernetinio incidento poveikio mažinimo priemonės;

d) tarpvalstybinis kibernetinio incidento poveikis, jeigu toks buvo;

5) tuo atveju, jei šios dalies 4 punkte nurodytos galutinės ataskaitos pateikimo metu kibernetinis incidentas tebevyksta, pateikiama pažangos ataskaita, o galutinė ataskaita – per vieną mėnesį nuo tada, kai kibernetinis incidentas suvaldomas.

5. Kibernetinio saugumo subjektai privalo pranešti apie kibernetinį incidentą ir kibernetinę grėsmę nacionalinio kibernetinių incidentų valdymo plano, tvirtinamo Vyriausybės, nustatyta tvarka.

6. Nacionaliniame kibernetinių incidentų valdymo plane nustatoma:

1) terminai per kuriuos turi būti pranešama apie šio straipsnio 1 dalies 1 punkte nenurodytus kibernetinius incidentus;

2) informacija, kuri turi būti perduodama pranešant apie šio straipsnio 1 dalies 1 punkte nenurodytus kibernetinius incidentus;

3) informacijos apie kibernetinius incidentus pateikimo būdai ir priemonės;

4) institucijų veiksmai, gavus informacijos apie kibernetinius incidentus;

5) išsamesni atvejai, kada kibernetinis incidentas laikomas dideliu, jeigu išsamesni atvejai nenustatomi Europos Komisijos įgyvendinimo aktuose.

IV SKYRIUS
KEITIMASIS INFORMACIJA IR TARPINSTITUCINIS BENDRADARBIAVIMAS

19 straipsnis. Kibernetinio saugumo informacinis tinklas

1. Kibernetinio saugumo informacinis tinklas yra valstybės informacinė sistema, kurios paskirtis:

1) registruoti Kibernetinio saugumo subjektų registro objektus ir tvarkyti jų duomenis;

2) tvarkyti duomenis, surinktus techninėmis kibernetinio saugumo priemonėmis, siekiant užkardyti ir valdyti kibernetinius incidentus;

3) tvarkyti duomenis, susijusius su kibernetinio saugumo rizikos valdymo priemonių įgyvendinimo stebėsena;

4) tvarkyti duomenis apie kibernetinio saugumo subjektus, kitas įstaigas ir ūkio subjektus, kuriems, įvykus ekstremaliajam įvykiui kibernetinėje erdvėje, būtų pavedamos būtinosios užduotys valdant kibernetinius incidentus;

5) keistis su Kibernetinio saugumo informacinio tinklo naudotojais duomenimis, susijusiais su kibernetiniais incidentais, kibernetinėmis grėsmėmis, vos neįvykusiais kibernetiniais incidentais, taip pat kita su kibernetinio saugumo užtikrinimu susijusia informacija;

6) tvarkyti duomenis apie privalomus nurodymus blokuoti domeno vardą, identifikuojantį interneto svetainę ir juos viešai skelbti;

7) teikti kibernetinio saugumo paslaugas ir priemones, įskaitant mokymų ir pratybų paslaugas ir įrankius.

2. Kibernetinio saugumo informacinio tinklo valdytoja ir duomenų valdytoja – Krašto apsaugos ministerija, tvarkytojas ir duomenų tvarkytojas – Nacionalinis kibernetinio saugumo centras.

3. Kibernetinio saugumo informacinio tinklo naudotojai yra subjektai, kurie atitinka Kibernetinio saugumo informacinio tinklo nuostatuose nurodytus reikalavimus. Šio straipsnio 1 dalies 6 punkte nustatytus nurodymus duodančios institucijos ir juos įgyvendinantys kibernetinio saugumo subjektai privalo naudotis Kibernetinio saugumo informacinio tinklo dalimi, kurioje tvarkomi duomenys apie privalomus nurodymus blokuoti domeno vardą, identifikuojantį interneto svetainę, nepriklausomai nuo kibernetinio saugumo subjektų atitikties Kibernetinio saugumo informacinio tinklo nuostatuose nurodytiems reikalavimams.

4. Kibernetinio saugumo subjektai turi teisę tapti Kibernetinio saugumo informacinio tinklo naudotojais, įgyvendindami tarpusavio dalijimosi kibernetinio saugumo informacija susitarimus. Nepriklausomai nuo to, ar naudojamasi Kibernetinio saugumo informaciniu tinklu, kibernetinio saugumo subjektai privalo pranešti Nacionaliniam kibernetinio saugumo centrui apie tokių susitarimų sudarymą, taip pat apie pasitraukimą iš tokių susitarimų per 20 darbo dienų nuo šių aplinkybių atsiradimo.

5. Kibernetinio saugumo informacinio tinklo duomenys yra konfidencialūs ir teikiami tik šiais atvejais:

1) Kibernetinio saugumo informacinio tinklo naudotojams tiek, kiek tai susiję su jų valdomomis ir (ar) tvarkomomis tinklų ir informacinėmis sistemomis;

2) Nacionaliniam kibernetinio saugumo centrui atliekant šio įstatymo 7 straipsnio 2 dalies 12 punkte nustatytą funkciją;

3) valdant ir (ar) tiriant kibernetinius incidentus tiek, kiek tai būtina šio įstatymo 20 straipsnio 1 dalyje nustatytoms institucijų funkcijoms atlikti;

4) identifikuojant ir registruojant kibernetinio saugumo subjektus Kibernetinio saugumo subjektų registre šio įstatymo 13 straipsnyje nustatytoms institucijų funkcijoms atlikti;

5) viešai skelbiant duomenis apie privalomus nurodymus blokuoti domeno vardą, identifikuojantį interneto svetainę;

6) Policijai atliekant šio įstatymo 10 straipsnio 1 dalies 1 punkte nustatytą funkciją;

7) jeigu teisė gauti šią informaciją yra nustatyta įstatymuose ar jų pagrindu priimtuose įgyvendinamuosiuose teisės aktuose.

20 straipsnis. Tarpinstitucinis bendradarbiavimas

1. Kibernetinio saugumo politiką formuojančios ir įgyvendinančios institucijos bendradarbiauja tarpusavyje bei su kitomis valstybės institucijomis, įskaitant Ryšių reguliavimo tarnybą, kompetentingas institucijas pagal Reglamentą (ES) Nr. 910/2014 ir Reglamentą (ES) 2022/2554, taip pat Krizių valdymo centru, įgyvendindamos šiame įstatyme nustatytus tikslus,

įskaitant keitimąsi informacija ir duomenimis apie kibernetinius incidentus, kibernetines grėsmes ir vos neįvykusius kibernetinius incidentus, taip pat informacijos perdavimą pagal šio straipsnio 2 dalį.

2. Nacionalinis kibernetinio saugumo centras:

1) ne vėliau kaip per 20 darbo dienų nuo sprendimo taikyti šio įstatymo 28 straipsnio 1 dalyje nurodytą vykdymo užtikrinimo priemonę priėmimo apie tai informuoja Nacionalinį krizių valdymo centrą, jeigu vykdymo užtikrinimo priemonė taikoma siekiant užtikrinti, kad esminis subjektas laikytųsi šio įstatymo reikalavimų;

2) ne vėliau kaip per 20 darbo dienų nuo sprendimo taikyti šio įstatymo 28 straipsnio 1 dalyje vykdymo užtikrinimo priemonę priėmimo apie tai informuoja kompetentingą instituciją pagal Reglamentą (ES) 2022/2554, jeigu vykdymo užtikrinimo priemonė taikoma siekiant užtikrinti, kad esminis subjektas, kuris paskirtas ypatingai svarbiu trečiųjų šalių informacinių ir ryšių technologijų paslaugų teikėju pagal Reglamento (ES) 2022/2554 31 straipsnį, laikytųsi šio įstatymo reikalavimų;

3) teikia technines ir kitokias konsultacijas, pagalbą kompetentingai institucijai pagal Reglamentą (ES) 2022/2554 ir turi teisę su kompetentinga institucija pagal Reglamentą (ES) 2022/2554 sudaryti bendradarbiavimo susitarimą, nurodytą Reglamento (ES) 2022/2554 47 straipsnio 3 dalyje;

4) nustatęs, kad esminis ar svarbus subjektas gali būti padaręs asmens duomenų saugumo pažeidimą, apie tai nepagrįstai nedelsiant, bet ne vėliau kaip per 36 valandas nuo šios aplinkybės nustatymo informuoja Valstybinę duomenų apsaugos inspekciją, nurodydamas turimą informaciją apie Reglamento (ES) 2016/679 33 straipsnio 3 dalyje nurodytas aplinkybes;

5) bendradarbiauja su Ryšių reguliavimo tarnyba patikimumo užtikrinimo paslaugų teikėjų kibernetinio saugumo audito srityje, taip pat nedelsdamas, bet ne vėliau kaip per 24 val. informuoja Ryšių reguliavimo tarnybą apie patikimumo užtikrinimo paslaugų teikėjų praneštus kibernetinius incidentus;

6) ne vėliau kaip per 20 darbo dienų nuo sprendimo taikyti šio įstatymo 28 straipsnio 1 dalyje vykdymo užtikrinimo priemonę priėmimo apie tai informuoja kitos valstybės narės kompetentingą instituciją, atsakingą už kibernetinio saugumo reikalavimų vykdymo užtikrinimą, jeigu kibernetinio saugumo subjektas teikia paslaugas arba jo tinklų ir informacinės sistemos yra toje valstybėje narėje;

7) bendradarbiauja su kitų valstybių narių kompetentingomis institucijomis, atsakingomis už kibernetinio saugumo reikalavimų vykdymo užtikrinimą, kai kibernetinio saugumo subjektas teikia paslaugas daugiau nei vienoje valstybėje narėje arba teikia paslaugas vienoje ar daugiau valstybių narių, o jo tinklų ir informacinės sistemos yra vienoje ar daugiau kitų valstybių narių, vykdydamos savitarpio pagalbos prašymus šios įstatymo 21 straipsnio nustatyta tvarka

8) prieš vykdydamas šio įstatymo 26 straipsnyje numatytus patikrinimus ar taikydamas šio įstatymo 28 straipsnyje numatytas vykdymo užtikrinimo priemones Lietuvos banko atžvilgiu konsultuojasi su Europos Centriniu banku.

21 straipsnis. Savitarpio pagalba

1. Nacionalinis kibernetinio saugumo centras, gavęs kitos valstybės narės kompetentingos institucijos pagrįstą savitarpio prašymą, vykdo šio įstatymo 26 ir 28 straipsniuose numatytus kibernetinio saugumo subjektų patikrinimo ir (ar) vykdymo užtikrinimo priemonių veiksmus, taip pat kitus prašomus veiksmus, kuriuos vykdyti suteikia teisę šis įstatymas. Teikdamas savitarpio pagalbą dėl šio įstatymo 12 straipsnio 1 dalies 3 punkte nurodyto subjekto, kurio pagrindinė buveinė yra ne Lietuvos Respublikoje, Nacionalinis kibernetinio saugumo centras negali imtis daugiau veiksmų, nei nurodyta savitarpio pagalbos prašyme.

2. Nacionalinis kibernetinio saugumo centras kitos valstybės narės kompetentingos institucijos savitarpio pagalbos prašymą gali atmesti tik tais atvejais, kai:

1) Nacionalinis kibernetinio saugumo centras neturi kompetencijos teikti prašomą pagalbą;

2) prašoma pagalba nėra proporcinga Nacionalinio kibernetinio saugumo centro turimiems žmogiškiesiems ar finansiniams ištekliams;

3) prašymas yra susijęs su informacija arba apima veiklą, kurios atskleidimas arba atlikimas prieštarautų Lietuvos Respublikos nacionaliniam saugumui, visuomenės saugumui ar gynybai.

3. Jeigu Nacionalinis kibernetinio saugumo centras pagal kompetenciją negali įgyvendinti pateikto savitarpio pagalbos prašymo, tačiau nustatęs, kad prašymą turėtų vykdyti kita valstybės institucija, prašymo nenagrinėja, persiunčia jį kitai valstybės institucijai ir apie tai praneša prašymą pateikusiai kitos valstybės kompetentingai institucijai.

4. Nacionalinis kibernetinio saugumo centras, negalėdamas įvykdyti kitos valstybės narės kompetentingos institucijos savitarpio pagalbos prašymo, apie tai privalo ją informuoti, nurodydamas negalėjimo įgyvendinti prašymo priežastis, ir, jeigu yra kitos valstybės narės prašymas, prieš atmesdamas tokį prašymą, konsultuojasi su Europos Komisija ir (ar) Europos Sąjungos kibernetinio saugumo agentūra.

22 straipsnis. Informacijos, tvarkomos tarpinstitucinio bendradarbiavimo metu, apsauga

1. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos šio įstatymo tikslais gauta informacija, įskaitant asmens duomenis ir konfidencialią informaciją, turi teisę keistis tarpusavyje, su kitų valstybių institucijomis, NATO ir Europos Sąjungos institucijomis ir tarptautinėmis organizacijomis tik tiek, kiek tai yra būtina šių institucijų funkcijoms pagal kompetenciją atlikti, atsižvelgiant į keitimosi informacija tikslą ir proporcingumą.

2. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos, tvarkydamos šio įstatymo tikslais gautą informaciją, saugo įslaptintą informaciją, asmenų saugumo ir komercinius interesus, taip pat pateiktos informacijos konfidencialumą. Šioje dalyje nurodyta informacija teikiama tik tais atvejais, jeigu teisė gauti šią informaciją yra nustatyta įstatymuose ar jų pagrindu priimtuose kituose įgyvendinamuosiuose norminiuose teisės aktuose.

3. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos šio įstatymo tikslais tvarkomus asmens duomenis tvarko laikydamosi Asmens duomenų teisinės apsaugos įstatymo, Reglamento (ES) 2016/679 ir Asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymu.

23 straipsnis. Kibernetinio saugumo kompetencijos bendruomenė

1. Bent vienoje iš Reglamento (ES) 2021/887 8 straipsnio 3 dalyje nurodytų sričių kibernetinio saugumo ekspertinių žinių turintys Lietuvos Respublikoje registruoti juridiniai asmenys, galintys prisidėti prie Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro ir Nacionalinių koordinavimo centrų tinklo misijos, turi teisę tapti Kibernetinio saugumo kompetencijos bendruomenės (toliau – Bendruomenė), sudaromos Reglamento (ES) 2021/887 8 straipsnio pagrindu, nariais. Bendruomenės nariais negali būti nacionalinio saugumo interesams grėsmę keliantys asmenys.

2. Kaip Bendruomenės narius juridinius asmenis registruoja Reglamento (ES) 2021/887 6 straipsnyje nustatyta tvarka paskirtas Nacionalinis koordinavimo centras, atlikęs vertinimą, patvirtinantį, kad šie juridiniai asmenys atitinka šio straipsnio 1 dalyje nustatytus reikalavimus. Nacionalinis koordinavimo centras neregistruoja juridinių asmenų kaip Bendruomenės narių, jei jie kelia grėsmę nacionalinio saugumo interesams. Informaciją, ar šie asmenys galėtų kelti grėsmę nacionalinio saugumo interesams, pagal Nacionalinio koordinavimo centro kreipimąsi teikia institucijos, nurodytos Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų

apsaugos įstatymo 12 straipsnio 7 dalyje vadovaudamosi Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatyme nurodytais investuotojų patikros dėl atitikties nacionalinio saugumo interesams vertinimo kriterijais.

3. Lietuvos Respublikoje registruotas juridinis asmuo, reiškiantis norą tapti Bendruomenės nariu (toliau – pareiškėjas), Nacionaliniam koordinavimo centrui pateikia prašymą, kuriame turi būti nurodyta:

1) juridinio asmens pavadinimas, juridinio asmens kodas, organizacijos buveinės adresas ir kontaktiniai duomenys (elektroninio pašto adresas, ryšio numeris);

2) juridinio asmens atstovo kontaktiniai duomenys (elektroninio pašto adresas, ryšio numeris);

3) patvirtinimas, kad pareiškėjui netaikomas nė vienas iš Reglamento (ES, Euratomas) 2018/1046 136 straipsnyje nustatytų pašalinimo kriterijų;

4) informacija apie pareiškėjo turimas kibernetinio saugumo ekspertines žinias bent vienoje iš Reglamento (ES) 2021/887 8 straipsnio 3 dalyje nurodytų sričių.

4. Nacionalinis koordinavimo centras įvertina pareiškėją ir jo pateiktą informaciją, taip pat atsižvelgia į kompetentingų institucijų informaciją, pateiktą pagal šio straipsnio 2 dalį, ir per du mėnesius nuo pareiškėjo prašymo gavimo dienos priima sprendimą:

1) įregistruoti pareiškėją kaip Bendruomenės narį;

2) atsisakyti įregistruoti pareiškėją kaip Bendruomenės narį.

5. Nacionalinis koordinavimo centras išbraukia Bendruomenės narį iš Bendruomenės:

1) jeigu Bendruomenės narys pateikia prašymą išbraukti iš Bendruomenės narių;

2) jeigu Bendruomenės narys nebeatitinka šio straipsnio 1 dalies nuostatų.

6. Sprendimą išbraukti iš Bendruomenės narių Nacionalinis koordinavimo centras priima per 10 darbo dienų nuo Bendruomenės nario prašymo būti išbrauktam gavimo arba nuo to momento, kai paaiškėja kitos aplinkybės, nurodytos šio straipsnio 5 dalies 2 punkte.

7. Nacionaliniam koordinavimo centrui atsisakius registruoti pareiškėją kaip Bendruomenės narį, pareiškėjas turi teisę dar kartą pateikti prašymą tapti Bendruomenės nariu. Nacionalinis koordinavimo centras turi teisę nenagrinėti pakartotinai pateikto prašymo, jeigu:

1) nepraėjo du mėnesiai nuo anksčiau priimto sprendimo atsisakyti registruoti pareiškėją kaip Bendruomenės nariu;

2) nepasikeitė faktinės aplinkybės, kurios buvo pagrindas priimti sprendimą atsisakyti registruoti pareiškėją kaip Bendruomenės narį.

8. Pareiškėjas turi teisę skųsti teismui Administracinių bylų teisenos įstatymo nustatyta tvarka šio straipsnio 4 dalies 2 punkte, 5 dalies 2 punkte ir 7 dalyje nurodytus Nacionalinio koordinavimo centro sprendimus.

24 straipsnis. Savanoriškas pranešimas

1. Subjektai, kuriems šio įstatymo 18 straipsnio 1 dalyje nėra nustatytos pareigos pranešti apie kibernetinius incidentus, kibernetines grėsmes, vos neįvykusius kibernetinius incidentus ir (ar) taikytas kibernetinių incidentų valdymo priemones, turi teisę savanoriškai apie juos pranešti Nacionaliniam kibernetinio saugumo centrui. Nacionalinis kibernetinio saugumo centras tokius pranešimus tvarko Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka.

2. Subjektui, savanoriškai pranešusiam apie kibernetinį incidentą, kibernetinę grėsmę, vos neįvykusį kibernetinį incidentą ir (ar) taikytas kibernetinių incidentų valdymo priemones, nenustatoma pareigų, susijusių su pranešimo pateikimu.

25 straipsnis. Spragų paieška ir atskleidimas

1. Spragų paieška ir atskleidimas laikomi teisėtais ir tokius veiksmus atlikusiam subjektui neužtraukia teisinės atsakomybės tik tais atvejais, kai spragų paieška atliekama kibernetinio saugumo subjektų valdomuose ir tvarkomuose tinkluose ir informacinėse sistemose laikantis šio straipsnio 2 dalyje, nacionalinės spragų atskleidimo tvarkos apraše, tvirtinamame krašto apsaugos ministro, ir (ar) kibernetinio saugumo subjekto nustatytos spragų atskleidimo tvarkos apraše, taip pat šio straipsnio 6 dalyje numatytų apribojimų.

2. Atliekant spragų paiešką laikomasi šių apribojimų:

1) negali būti trikdomas ar keičiamas tinklų ir informacinės sistemos darbas, funkcionalumas, teikiamos paslaugos bei duomenų prieinamumas ar vientisumas;

2) įsitikinus, kad spraga yra, nutraukiama spragos paieškos veikla, susijusi su aptikta spraga;

3) subjektas, atlikęs spragų paiešką, ne vėliau kaip per 24 valandas nuo spragų paieškos pradžios (paiešką tęsiant ilgiau kaip 24 valandas – kas 24 valandas) turi parengti nacionalinės spragų atskleidimo tvarkos apraše ar kibernetinio saugumo subjekto nustatytos spragų atskleidimo tvarkos apraše nustatyto turinio informaciją apie spragų paieškos rezultatus ir ją pateikti Nacionaliniam kibernetinio saugumo centrui nacionalinės spragų atskleidimo tvarkos apraše nustatyta tvarka ir (ar) kibernetinio saugumo subjektui, kurio tinklų ir informacinėje sistemoje atlikta spragų paieška, šio kibernetinio saugumo subjekto nustatytos spragų atskleidimo tvarkos apraše nustatyta tvarka;

4) nesiekiama be reikalo, daugiau, negu reikia spragai patvirtinti, stebėti, fiksuoti, perimti, įgyti, laikyti, atskleisti, kopijuoti, keisti, naikinti, gadinti, šalinti, naikinti kibernetinio saugumo subjekto valdomų ir (ar) tvarkomų duomenų;

5) atskleidžiant spragą nenaudojami pastebėti, užfiksuoti, perimti, atskleisti asmens duomenys;

6) nebandoma atspėti slaptažodžių, nenaudojami neteisėtu būdu gauti slaptažodžiai ir nėra manipuliuojama kibernetinio saugumo subjekto darbuotojais ar kitais subjektais, turinčiais teisę naudotis viešai neskelbtina informacija, reikšminga spragų paieškai;

7) nesidalijama informacija apie aptiktą spragą, išskyrus šios dalies 3 punkte ir šio straipsnio 6 dalyje nustatytus atvejus, taip pat kai informacija apie aptiktą spragą yra registruojama Europos pažeidžiamumų duomenų bazėje.

3. Subjektas, surinkęs informaciją apie spragą, turi teisę šią informaciją anonimiškai pateikti Nacionaliniam kibernetinio saugumo centrui, išsaugodamas nacionalinės spragų atskleidimo tvarkos apraše nurodytą informaciją apie spragų paieškos rezultatų pateikimą. Nacionalinis kibernetinio saugumo centras užtikrina apie spragą pranešusio subjekto anonimiškumą. Šioje dalyje nurodytą informaciją apie spragų paieškos rezultatų pateikimą subjektas, surinkęs informaciją apie spragą ir ją pateikęs anonimiškai, privalo saugoti 12 metų nuo pranešimo Nacionaliniam kibernetinio saugumo centrui pateikimo dienos.

4. Spragų atskleidimo Nacionaliniam kibernetinio saugumo centrui tvarka, Nacionaliniam kibernetinio saugumo centrui teikiamos informacijos apie spragas turinys, trumpesnio negu 90 kalendorinių dienų informacijos apie aptiktą spragą atskleidimo kitiems, negu nurodyti šio straipsnio 2 dalies 3 punkte, subjektams termino nustatymo tvarka nustatomi nacionalinės spragų atkleidimo tvarkos apraše.

5. Kibernetinio saugumo subjektas turi teisę nustatyti spragų jo valdomose ir (ar) tvarkomose tinklų ir informacinėse sistemose atskleidimo tvarką ir nustatyti kitus spragų paieškos apribojimus, negu numatyta šio straipsnio 2 dalyje, arba jų atsisakyti. Kibernetinio saugumo subjekto nustatytame spragų atskleidimo tvarkos apraše numatyti spragų paieškos apribojimai negali būti griežtesni, negu nurodyti šio straipsnio 2 dalyje. Kibernetinio saugumo subjekto nustatytame spragų atskleidimo tvarkos apraše negali būti nustatoma informacijos apie spragas pateikimo Nacionalinio kibernetinio saugumo centro tvarka ir numatomos šio straipsnio 6 dalyje nustatyto reguliavimo išimtys.

6. Subjektas, nustatęs spragą, laikydamasis šio straipsnio 1 dalyje nurodytų apribojimų, turi teisę informaciją apie aptiktą spragą, tačiau ne daugiau, negu buvo pateikta Nacionaliniam kibernetinio saugumo centrui ir (ar) kibernetinio saugumo subjektui, atskleisti kitiems, negu nurodyti šio straipsnio 2 dalies 3 punkte, subjektams ne anksčiau kaip po 90 kalendorinių dienų nuo informacijos apie spragą pateikimo Nacionaliniam kibernetinio saugumo centrui ir (ar) kibernetinio saugumo subjektui. Nacionalinis kibernetinio saugumo centras, įvertinęs spragos sudėtingumą ir jos ištaisymo galimybes, nacionalinės spragų atskleidimo tvarkos apraše nustatyta tvarka turi teisę nustatyti trumpesnį informacijos apie aptiktą spragą atskleidimo kitiems, negu nurodyti šio straipsnio 2 dalies 3 punkte, subjektams terminą, tačiau ne trumpesnį kaip 3 kalendorinės dienos.

V SKYRIUS
PATIKRINIMAI IR VYKDYMO UŽTIKRINIMO PRIEMONĖS

26 straipsnis. Kibernetinio saugumo subjektų patikrinimai

1. Nacionalinis kibernetinio saugumo centras atlieka kibernetinio saugumo subjektų atitikties šio įstatymo reikalavimams, išskyrus nustatytus šio įstatymo VI ir VII skyriuose, patikrinimus.

2. Nacionalinis kibernetinio saugumo centras turi teisę pradėti šio straipsnio 1 dalyje nurodytą kibernetinio saugumo subjekto patikrinimą bet kokiu klausimu, susijusiu su šio įstatymo reikalavimais, nustatytais kibernetinio saugumo subjektams, kurių nevykdymas laikomas pažeidimu, savo iniciatyva, gavęs skundą ar kitų šaltinių pagrindu, išskyrus šio straipsnio 3 dalyje nurodytus atvejus.

3. Šio straipsnio 1 dalyje nurodyti svarbių subjektų patikrinimai atliekami tik gavus duomenų ar informacijos, kad svarbus subjektas, kaip įtariama, padarė šio įstatymo reikalavimų pažeidimą.

4. Šio straipsnio 1 dalyje nurodyti patikrinimai atliekami šio įstatymo 27 straipsnyje ir Nacionalinio kibernetinio saugumo centro nustatyta tvarka. Nacionalinio kibernetinio saugumo centro nustatytame patikrinimų atlikimo tvarkos apraše turi būti numatoma kibernetinio saugumo rizikos požiūriu prioritetinių patikrinimų nustatymo tvarka.

27 straipsnis. Bendrieji kibernetinio saugumo subjektų patikrinimų atlikimo pagrindai

1. Patikrinimas turi būti atliktas per kuo trumpesnį terminą, bet ne vėliau kaip per 4 mėnesius nuo šio įstatymo 26 straipsnio 2 dalyje nurodyto skundo gavimo dienos arba Nacionalinio kibernetinio saugumo centro direktoriaus ar jo įgalioto asmens sprendimo atlikti patikrinimą savo iniciatyva arba kitų šaltinių pagrindu priėmimo dienos.

2. Atsižvelgiant į patikrinimo sudėtingumą, mastą, kibernetinio saugumo subjektų veiklos pobūdį bei vengimą vykdyti Nacionalinio kibernetinio saugumo centro reikalavimus, patikrinimo metu paaiškėjusias naujas aplinkybes arba kitas objektyvias priežastis, šio straipsnio 1 dalyje nustatytas terminas Nacionalinio kibernetinio saugumo centro sprendimu gali būti pratęstas, bet ne ilgiau kaip 2 mėnesiams. Bendras patikrinimo atlikimo terminas negali būti ilgesnis kaip 6 mėnesiai nuo šio įstatymo 26 straipsnio 2 dalyje nurodyto skundo gavimo dienos arba sprendimo atlikti patikrinimą savo iniciatyva ar kitų šaltinių pagrindu priėmimo dienos. Apie patikrinimo termino pratęsimą ir priežastis, dėl kurių šis terminas pratęstas, Nacionalinis kibernetinio saugumo centras privalo nedelsdamas, bet ne vėliau kaip iki šio straipsnio 1 dalyje nurodyto termino pabaigos pranešti tikrinamam subjektui.

3. Atlikdamas šio įstatymo 26 straipsnio 1 dalyje nurodytus patikrinimus, Nacionalinis kibernetinio saugumo centras turi teisę:

1) įeiti į tikrinamų kibernetinio saugumo subjektų patalpas (tarp jų ir nuomojamas ar naudojamas kitais pagrindais), ne ilgesniam kaip 30 kalendorinių dienų terminui paimti dokumentų kopijas ir nuorašus, duomenų kopijas bei kitus daiktus, reikalingus patikrinimams atlikti. Įeiti į juridinio asmens patalpas (tarp jų ir nuomojamas ar naudojamas kitais pagrindais) galima tik juridinio

asmens darbo laiku, pateikus tarnybinį pažymėjimą ir Nacionalinio kibernetinio saugumo centro sprendimą atlikti patikrinimą liudijantį dokumentą ar kitą Nacionalinio kibernetinio saugumo centro vadovo suteiktą įgaliojimą. Įeiti į fiziniam asmeniui priklausančias patalpas (tarp jų ir nuomojamas ar naudojamas kitais pagrindais) galima tik pateikus teismo nutartį dėl leidimo įeiti į fiziniam asmeniui priklausančias patalpas;

2) duoti nurodymus tikrinamiems kibernetinio saugumo subjektams savo lėšomis atlikti nepriklausomą tinklų ir informacinių sistemų arba jomis vykdomos veiklos ar teikiamų paslaugų tikslinį kibernetinio saugumo auditą ir pateikti šio audito rezultatus, jeigu remiantis kibernetinio saugumo rizikos analizės rezultatais nustatytas aukštas rizikos lygis;

3) duoti nurodymus pateikti visą reikalingą informaciją, dokumentų kopijas ir išrašus, duomenų kopijas, taip pat susipažinti su visais duomenimis ir dokumentais, reikalingais kibernetinio saugumo subjektų tinklų ir informacinių sistemų atitikčiai šio įstatymo 14 straipsnio 1 dalyje nurodytiems reikalavimams įvertinti, įskaitant atliktų kibernetinio saugumo auditų rezultatus, įrodančius tinklų ir informacinių sistemų atitiktį nurodytiems reikalavimams;

4) duoti nurodymus subjektams, turintiems patikrinimams reikšmingos informacijos, pateikti žodinius ir rašytinius paaiškinimus, reikalauti, kad jie atvyktų į Nacionalinio kibernetinio saugumo centro patalpas duoti paaiškinimų;

5) savo lėšomis pasitelkti nepriklausomus, nešališkus ir atitinkančius Valstybės tarnybos įstatyme nustatytus nepriekaištingos reputacijos kriterijus bei atitinkamą kvalifikaciją ir patirtį turinčius subjektus;

6) sudaryti sutartis su audito įmonėmis, kitais subjektais, kurių paslaugomis Nacionalinis kibernetinio saugumo centras naudosis atlikdamas patikrinimą. Sudarant šiame punkte nurodytas sutartis taikomi šio įstatymo 7 straipsnio 3 dalyje nurodyti reikalavimai;

7) naudoti visą Nacionalinio kibernetinio saugumo centro turimą informaciją, įskaitant ir informaciją, gautą kitų patikrinimų metu;

8) naudotis kitomis įstatymų suteiktomis teisėmis.

4. Nacionalinis kibernetinio saugumo centras, užtikrindamas jam pavestų uždavinių ir funkcijų vykdymą atliekant patikrinimus, turi teisę:

1) atlikti veiksmus, nurodytus šio straipsnio 3 dalies 1 punkte;

2) užfiksuoti faktines aplinkybes;

3) patikrinimo metu savo lėšomis naudoti technines priemones;

4) tikrinti asmenų tapatybę patvirtinančius dokumentus.

5. Taikydamas šio straipsnio 3 dalies 3 punktą, Nacionalinis kibernetinio saugumo centras privalo nurodyti konkretų prašymo tikslą, pagrindą ir tiksliai apibrėžti prašomą informaciją.

6. Nacionalinis kibernetinio saugumo centras, baigęs patikrinimą, priima bent vieną iš šių sprendimų:

1) konstatuoti, kad pažeidimų nenustatyta;

2) nustatęs šio įstatymo pažeidimą, taikyti šio įstatymo 28 straipsnyje nurodytas vykdymo užtikrinimo priemones.

7. Nustačius šio įstatymo pažeidimą, šio įstatymo 28 straipsnyje numatytos vykdymo užtikrinimo priemonės, išskyrus nurodytas 28 straipsnio 1 dalies 9–11 punktuose, atsižvelgiant į patikrinimo sudėtingumą, mastą, kibernetinio saugumo subjektų veiklos pobūdį bei vengimą vykdyti Nacionalinio kibernetinio saugumo centro reikalavimus, patikrinimo metu paaiškėjusias naujas aplinkybes arba kitas objektyvias priežastis, gali būti taikomos ir nebaigus patikrinimo.

8. Prieš priimdamas sprendimą taikyti šio įstatymo 28 straipsnio 1 dalyje nurodytą vykdymo užtikrinimo priemonę (priemones), Nacionalinis kibernetinio saugumo centras privalo apie tai informuoti kibernetinio saugumo subjektą, kuriam ketinama taikyti vykdymo užtikrinimo priemonę (priemones), pateikdamas esminę informaciją apie teisės aktų nuostatas ir nustatytus faktinius

duomenis, kurie sudaro vykdymo užtikrinimo priemonės (priemonių) taikymo pagrindus, ir nustatyti ne trumpesnį kaip 20 darbo dienų terminą nuo pranešimo įteikimo dienos paaiškinimams pateikti, išskyrus atvejus, kai tai trukdytų imtis neatidėliotinų kibernetinių incidentų prevencijos arba reagavimo į juos veiksmų. Skiriant šio įstatymo 28 straipsnio 1 dalies 9–11 punktuose numatytas poveikio priemones šioje dalyje nurodytas 20 darbo dienų terminas paaiškinimams teikti turi būti nustatomas.

28 straipsnis. Vykdymo užtikrinimo priemonės

1. Nacionalinis kibernetinio saugumo centras, šio įstatymo 26 straipsnio 1 dalyje nurodyto patikrinimo metu nustatęs šio įstatymo pažeidimą, taiko vykdymo užtikrinimo priemonę ar jų grupę:

1) teikia įspėjimus, kad kibernetinio saugumo subjektai pažeidžia šio įstatymo nustatytus reikalavimus;

2) duoda nurodymus esminiams subjektams dėl priemonių, kurių reikia siekiant užkirsti kelią kibernetiniam incidentui arba jam suvaldyti, ir tokių priemonių įgyvendinimo bei jų įgyvendinimo ataskaitų pateikimo terminų, nurodymus kibernetinio saugumo subjektams, kad atitinkami subjektai pašalintų nustatytus trūkumus arba ištaisytų šio įstatymo reikalavimų pažeidimus;

3) duoda nurodymus kibernetinio saugumo subjektams nutraukti veiksmus, kurie pažeidžia šio įstatymo nustatytus reikalavimus, ir tokių veiksmų nebekartoti;

4) duoda nurodymus kibernetinio saugumo subjektams konkrečiu būdu ir per nustatytą laikotarpį užtikrinti, kad jų naudojamos kibernetinio saugumo rizikos valdymo priemonės atitiktų šio įstatymo 14 straipsnio 1 dalyje nurodytus teisės aktus arba kad jie įvykdytų šio įstatymo 18 straipsnio 1 dalyje nustatytą pareigą pranešti apie kibernetinius incidentus;

5) duoda nurodymus kibernetinio saugumo subjektams informuoti subjektus, kuriems jie teikia paslaugas arba vykdo jiems aktualią veiklą ir kuriuos didelė kibernetinė grėsmė gali paveikti, apie grėsmės pobūdį, taip pat apie visus galimus veiksmus, kurių gali imtis tie subjektai, reaguodami į tą grėsmę;

6) duoda nurodymus kibernetinio saugumo subjektams per pagrįstą terminą įgyvendinti kibernetinio saugumo audito metu pateiktas rekomendacijas;

7) paskiria stebėsenos pareigūną, kuriam per nustatytą laikotarpį pavestos aiškiai apibrėžtos užduotys, prižiūrėti, kaip esminiai subjektai laikosi šio įstatymo 14 ir 18 straipsnių reikalavimų;

8) duoda nurodymus kibernetinio saugumo subjektams konkrečiu būdu viešai paskelbti šio įstatymo pažeidimo aspektus;

9) skiria kibernetinio saugumo subjektams baudą šio įstatymo 30 ir 31 straipsniuose nustatyta tvarka, kartu su bet kuriomis šios dalies 1–8, 10 ir 11 punktuose nurodytomis priemonėmis;

10) inicijuoja šio įstatymo 32 straipsnyje nustatytą laikiną teisės užsiimti dalimi ar visa esminio subjekto vykdoma veikla ar teikti paslaugas sustabdymą;

11) inicijuoja šio įstatymo 33 straipsnyje nustatytą esminio subjekto vadovo, išskyrus Lietuvos Respublikos Seimo, Vyriausybės ir Prezidento sprendimu skiriamus viešojo administravimo subjektų vadovus, laikiną nušalinimą nuo pareigų.

2. Vykdymo užtikrinimo priemonės pritaikymas neatleidžia kibernetinio saugumo subjekto nuo pareigos, už kurios nevykdymą pritaikyta vykdymo užtikrinimo priemonė, atlikimo. Vykdymo užtikrinimo priemonės taikymas juridiniams asmenims neatleidžia jų vadovų ir darbuotojų nuo įstatymuose nustatytos civilinės, administracinės ar baudžiamosios atsakomybės.

3. Taikydamas bet kurią iš šio straipsnio 1 dalyje nurodytų vykdymo užtikrinimo priemonių, Nacionalinis kibernetinio saugumo centras atsižvelgia į kiekvieno konkretaus atvejo aplinkybes, taip pat į:

1) atsakomybę lengvinančias aplinkybes, nustatytas šio straipsnio 4 dalyje, atsakomybę sunkinančias aplinkybės, nustatytas šio straipsnio 5 dalyje, ir pažeistų nuostatų pavojingumą, nurodytą šio įstatymo 29 straipsnyje;

2) pažeidimo trukmę;

3) subjekto įvykdytus ankstesnius šio įstatymo pažeidimus per pastaruosius 2 metus;

4) padarytą turtinę arba neturtinę žalą, kuri vertinama apskaičiuojant finansinius ar ekonominius nuostolius, poveikį kitoms paslaugoms ir paveiktų naudotojų skaičių, nuostolių atlyginimą ar padaryto neigiamo poveikio panaikinimą;

5) priemones, kurių subjektas ėmėsi siekdamas užkirsti kelią turtinei ar neturtinei žalai arba ją sumažinti;

6) patvirtintų elgesio kodeksų arba patvirtintų sertifikavimo mechanizmų laikymąsi;

7) bendradarbiavimą su Nacionaliniu kibernetinio saugumo centru;

8) pažeidimo mastą.

4. Šio straipsnio 3 dalies 1 punkte nurodytomis atsakomybę lengvinančiomis aplinkybėmis laikoma:

1) subjektas savo noru užkirto kelią turtinei ar neturtinei žalai;

2) subjektas atlygino padarytą žalą;

3) subjektas pripažino pažeidimą ir padėjo Nacionaliniam kibernetinio saugumo centrui patikrinimo metu;

4) subjektas savo valia nutraukė pažeidimą;

5) pažeidimas padarytas dėl neatsargumo.

5. Šio straipsnio 3 dalies 1 punkte nurodytomis atsakomybę sunkinančiomis aplinkybėmis laikoma:

1) pažeidimas padarytas pakartotinai. Laikoma, kad pažeidimas padarytas pakartotinai, jeigu subjektas, įtariamas pažeidimo padarymu, per paskutinius 12 mėnesių nuo sprendimo, kuriuo buvo paskirta vykdymo užtikrinimo priemonė, įsigaliojimo dienos padarė tokį patį pažeidimą. Padarius pakartotinį pažeidimą, šioje dalyje nustatytas terminas skaičiuojamas iš naujo;

2) padarytas pavojingas pažeidimas, kaip jis suprantamas pagal šio įstatymo 29 straipsnio 2 dalį;

3) subjektas neištaisė trūkumų pagal Nacionalinio kibernetinio saugumo centro pateiktus nurodymus;

4) subjektas trukdė vykdyti kibernetinio saugumo audito ar stebėsenos pareigūno veiklą, kurią įpareigojo atlikti Nacionalinis kibernetinio saugumo centras, nustatęs pažeidimą;

5) subjektas pateikė neteisingą informaciją, susijusią su šio įstatymo reikalavimais;

6) subjektas slėpė padarytą pažeidimą ar pažeidimą tęsė nepaisydamas to, kad Nacionalinis kibernetinio saugumo centras buvo atkreipęs dėmesį į pažeidimus ar veiklos trūkumus;

7) pažeidimas padarytas tyčia.

6. Šio straipsnio 1 dalyje nurodytos vykdymo užtikrinimo priemonės taikomos Vyriausybės nustatyta vykdymo užtikrinimo priemonių taikymo tvarka.

7. Sprendimas dėl vykdymo užtikrinimo priemonės skyrimo gali būti priimtas, jeigu praėjo ne daugiau kaip 2 metai nuo pažeidimo dienos (išskyrus atvejus, kai sprendimo dėl vykdymo užtikrinimo priemonės skyrimo metu pažeidimas ar trūkumas jau yra ištaisytas), o kai pažeidimas trunkamasis – nuo jo paaiškėjimo dienos.

29 straipsnis. Pažeidimai, dėl kurių taikomos vykdymo užtikrinimo priemonės

1. Pažeidimais yra laikomi šiame įstatyme ir jį įgyvendinančiuose teisės aktuose nustatytų reikalavimų nesilaikymas ar trukdymas šio įstatymo 4 straipsnio 2 ir 3 dalyse nurodytoms

institucijoms, įskaitant jų pasitelktus subjektus, atlikti joms priskirtas funkcijas. Pažeidimai skirstomi į: pavojingus, vidutinio pavojingumo, nedidelio pavojingumo.

2. Pažeidimais, priskiriamais pavojingiems pažeidimams, yra laikomi šio įstatymo 14 straipsnio 1 dalyje, 18 straipsnio 1 dalies 1 punkte nustatytų reikalavimų pažeidimai.

3. Pažeidimais, priskiriamais vidutinio pavojingumo pažeidimams, yra laikomi šio įstatymo 7 straipsnio 2 dalies 6 ir 7 dalyse, 14 straipsnio 6 ir 8 dalyse, 15 straipsnio 1, 2 ir 3 dalyse nustatytų reikalavimų pažeidimai ar trukdymas institucijoms atlikti šio įstatymo 27 straipsnio 3 dalyje joms priskirtas funkcijas, taip pat šio įstatymo 17 straipsnyje nustatytų reikalavimų pažeidimai, jeigu juos atliko aukščiausio lygio domenų vardų registro paslaugas teikiantis subjektai.

4. Pažeidimais, priskiriamais nedidelio pavojingumo pažeidimams, yra laikomi šio įstatymo 14 straipsnio 3 ir 7 dalyse, 18 straipsnio 1 dalies 2 punkte, 19 straipsnio 4 dalyje nustatytų reikalavimų pažeidimai, taip pat šio įstatymo 17 straipsnyje nustatytų reikalavimų pažeidimai, jeigu juos atliko domenų vardų registro paslaugas teikiantis subjektai.

30 straipsnis. Baudos

1. Baudas skiria Nacionalinio kibernetinio saugumo centro vadovas ar jo įgaliotas asmuo pagal vykdymo užtikrinimo priemonių taikymo esminiams ir svarbiems subjektams tvarką, tvirtinamą Vyriausybės.

2. Už 29 straipsnyje nurodytus pažeidimus skiriamų baudų dydžiai:

1) esminiam subjektui – iki 10 000 000 Eur arba iki 2 proc. juridinio asmens bendros pasaulinės metinės apyvartos per praėjusį finansinį laikotarpį, atsižvelgiant į tai, kuri suma didesnė;

2) svarbiam subjektui – iki 7 000 000 Eur arba iki 1,4 proc. juridinio asmens bendros pasaulinės metinės apyvartos per praėjusį finansinį laikotarpį, atsižvelgiant į tai, kuri suma didesnė;

3) biudžetinei įstaigai, kuri yra esminis subjektas, – iki 1 procento biudžetinės įstaigos einamųjų metų biudžeto ir kitų praėjusiais metais gautų bendrųjų metinių pajamų dydžio, bet ne didesnė negu 60 000 Eur;

4) biudžetinei įstaigai, kuri yra svarbus subjektas, – iki 0,5 procento biudžetinės įstaigos einamųjų metų biudžeto ir kitų praėjusiais metais gautų bendrųjų metinių pajamų dydžio, bet ne didesnė negu 30 000 Eur.

3. Nustatomos šios baudos:

1) iki 100 proc. šio straipsnio 2 dalyje nustatytos maksimalios baudos, jei pažeidimas yra laikomas pavojingu pažeidimu pagal šio įstatymo 29 straipsnio 2 dalį;

2) iki 50 proc. šio straipsnio 2 dalyje nustatytos maksimalios baudos, jei pažeidimas yra laikomas vidutinio pavojingumo pažeidimu pagal šio įstatymo 29 straipsnio 3 dalį;

3) iki 10 proc. šio straipsnio 2 dalyje nustatytos maksimalios baudos, jei pažeidimas yra laikomas nedidelio pavojingumo pažeidimu pagal šio įstatymo 29 straipsnio 4 dalį.

4. Nustatomas konkretus baudos dydis turi būti veiksmingas, proporcingas padarytam pažeidimui ir atgrasantis nuo pažeidimų darymo ateityje. Nustatant konkretų baudos dydį atsižvelgiama į 28 straipsnio 3 dalyje nurodytas aplinkybes, išskyrus 28 straipsnio 5 dalies 2 punkte nurodytą aplinkybę.

31 straipsnis. Baudų skyrimo tvarka

1. Nacionalinis kibernetinio saugumo centras baudos skyrimo klausimą paprastai nagrinėja rašytinės procedūros tvarka pagal jam pateiktus paaiškinimus, gautus šio įstatymo 27 straipsnio 8 dalyje nustatyta tvarka. Baudos skyrimą svarstant rašytinės procedūros tvarka, posėdis nerengiamas.

2. Nacionalinis kibernetinio saugumo centras kibernetinio saugumo subjekto, kuriam numatoma skirti baudą, prašymu arba savo iniciatyva dėl aplinkybių sudėtingumo ar kitų svarbių aplinkybių gali nuspręsti baudos skyrimą svarstyti žodinės procedūros tvarka, kai būtina išklausyti

žodinius pažeidimo padarymu įtariamo kibernetinio saugumo subjekto paaiškinimus ar kitais atvejais, kai baudos skyrimas gali būti geriau apsvarstytas žodinės procedūros tvarka. Nusprendus baudos skyrimą svarstyti žodinės procedūros tvarka, kibernetinio saugumo subjektui, kuriam numatoma skirti baudą, ir kitiems suinteresuotiems subjektams turi būti pranešta apie posėdžio, kuriame svarstomas baudos skyrimas, vietą, datą ir laiką ne vėliau kaip prieš 10 darbo dienų iki posėdžio dienos elektroniniu paštu.

3. Posėdyje, kuriame svarstomas baudos skyrimas, gali dalyvauti ir pateikti paaiškinimus dėl pažeidimo padarymo kibernetinio saugumo subjektas, kuriam numatoma skirti baudą, ir kiti subjektai, kurių dalyvavimas reikalingas baudos skyrimui tinkamai apsvarstyti.

4. Kibernetinio saugumo subjekto, kuriam numatoma skirti baudą, ar jo atstovo neatvykimas netrukdo svarstyti baudos skyrimo, jeigu subjektui apie bylos nagrinėjimo posėdį buvo tinkamai pranešta ir jis nepateikė įrodymų, kad negali atvykti dėl svarbių priežasčių.

5. Baudos skyrimo svarstymas yra viešas, išskyrus atvejus, kai Nacionalinis kibernetinio saugumo centras savo iniciatyva arba kibernetinio saugumo subjekto, kuriam numatoma skirti baudą, ir (ar) kito suinteresuoto subjekto prašymu nusprendžia baudos skyrimą svarstyti uždarame posėdyje siekdamas apsaugoti valstybės, tarnybos, profesines, komercines paslaptis ar kitas įstatymų saugomas paslaptis arba užtikrinti subjekto teises į privataus gyvenimo neliečiamumą ir (ar) asmens duomenų apsaugą.

6. Posėdis, kuriame svarstomas baudos skyrimas, vyksta lietuvių kalba. Asmenims, nemokantiems valstybinės kalbos, garantuojama teisė naudotis vertėjo paslaugomis.

7. Posėdžio, kuriame svarstomas baudos skyrimas, metu daromas posėdžio garso įrašas. Jis laikomas posėdžio protokolu.

8. Kai baudos skyrimas svarstomas rašytinės procedūros tvarka, Nacionalinis kibernetinio saugumo centras sprendimą dėl baudos skyrimo priima per 20 darbo dienų nuo šio įstatymo 27 straipsnio 8 dalyje nustatyto termino pabaigos. Jei baudos skyrimas svarstomas žodinės procedūros tvarka posėdyje, Nacionalinis kibernetinio saugumo centras sprendimą dėl baudos skyrimo priima per 20 darbo dienų nuo posėdžio dienos. Nacionalinis kibernetinio saugumo centras sprendimo nuorašą dėl baudos skyrimo ne vėliau kaip per 3 darbo dienas nuo priėmimo dienos išsiunčia subjektui, dėl kurio šis sprendimas priimtas, ir, jeigu bauda skiriama atlikus tyrimą, kuris pradėtas gauto skundo pagrindu, skundą pateikusiam subjektui.

9. Nacionalinio kibernetinio saugumo centro sprendimas dėl baudos skyrimo turi būti motyvuotas. Jame turi būti nurodoma Valstybės tarnybos įstatymo 10 straipsnio 5 punkte nurodyta informacija, įskaitant:

1) duomenis apie esminį ar svarbų subjektą, dėl kurio priimtas sprendimas;

2) pažeidimus, jei jie nustatyti, ir jų aplinkybes;

3) surinktus įrodymus ir jų vertinimą;

4) pažeidimo padarymu įtariamo kibernetinio saugumo subjekto ir kitų subjektų paaiškinimus (jeigu jie pateikti), jų vertinimą;

5) priimtą sprendimą – skirti baudą arba jos neskirti.

10. Nacionalinio kibernetinio saugumo centro sprendimas dėl baudos skyrimo gali būti skundžiamas teismui Administracinių bylų teisenos įstatymo nustatyta tvarka.

11. Nacionalinio kibernetinio saugumo centro sprendimas dėl baudos skyrimo turi būti įvykdytas ne vėliau kaip per 3 mėnesius nuo dienos, kurią jis buvo įteiktas subjektui, kuriam bauda paskirta. Apskundus Nacionalinio kibernetinio saugumo centro sprendimą dėl baudos skyrimo, jis turi būti įvykdytas ne vėliau kaip per 3 mėnesius nuo teismo sprendimo, kuriuo baudos skyrimas pripažįstamas pagrįstu, įsiteisėjimo dienos. Bauda turi būti sumokėta į valstybės biudžetą.

12. Nacionalinio kibernetinio saugumo centro sprendimas dėl baudos skyrimo yra vykdomasis dokumentas, vykdomas Civilinio proceso kodekso nustatyta tvarka. Jis gali būti pateiktas vykdyti ne vėliau kaip per 3 metus nuo priėmimo dienos.

13. Bauda neskiriama, jeigu kibernetinio saugumo subjektui už tą patį pažeidimą jau buvo skirta bauda vadovaujantis Reglamento (ES) 2016/679 58 straipsnio 2 dalies i punktu.

32 straipsnis. Laikinas teisės užsiimti dalimi ar visa esminio subjekto vykdoma veikla ar teikti paslaugas sustabdymas

1. Teismas, gavęs Nacionalinio kibernetinio saugumo centro prašymą, nutartimi turi teisę laikinai sustabdyti teisę užsiimti dalimi ar visa esminio subjekto vykdoma veikla, jeigu nustatoma, kad šio įstatymo 28 straipsnio 1 dalies 1–4 ir 6 punktuose numatytų vykdymo užtikrinimo priemonių taikymas yra neveiksmingas. Laikinas sustabdymas teise užsiimti dalimi ar visa esminio subjekto vykdoma veikla ar teikti paslaugas gali būti taikomas tik pavojingų pažeidimų, nurodytų šio įstatymo 29 straipsnio 2 dalyje, atveju.

2. Nacionalinis kibernetinio saugumo centras, prieš kreipdamasis į teismą su prašymu laikinai sustabdyti teisę užsiimti dalimi ar visa esminio subjekto vykdoma veikla šio straipsnio 1 dalyje nurodytu pagrindu, privalo esminį subjektą informuoti pateikdamas esminę informaciją apie teisės aktų nuostatas ir nustatytus faktinius duomenis, kurie sudaro laikino teisės užsiimti dalimi ar visa esminio subjekto vykdoma veikla sustabdymo pagrindus, ir nustatyti terminą, kuris negali būti trumpesnis kaip 10 darbo dienų nuo pranešimo įteikimo dienos, iki kurio esminis subjektas turi imtis būtinų veiksmų nustatytiems trūkumams pašalinti ar reikalavimams įvykdyti. Nacionalinis kibernetinio saugumo centras šio straipsnio 1 dalyje nustatytu pagrindu į teismą turi teisę kreiptis tik pasibaigus Nacionalinio kibernetinio saugumo centro nustatytam terminui ir esminiam subjektui nesiėmus nurodytų veiksmų.

3. Nacionalinio kibernetinio saugumo centro prašyme teismui dėl teisės laikinai sustabdyti teisę užsiimti dalimi ar visa esminio subjekto vykdoma veikla turi būti nurodyta:

1) esminio subjekto vykdoma veikla ar jos dalis ar teikiamos paslaugos, kurias prašoma stabdyti;

2) aplinkybės, įrodančios, kad šio įstatymo 28 straipsnio 1 dalies 1–4 ir 6 punktuose numatytų užtikrinimo priemonių taikymas yra neveiksmingas;

3) aplinkybės, įrodančios, kad esminiam subjektui buvo nustatytas terminas trūkumams pašalinti ar reikalavimams įvykdyti, o esminis subjektas nesiėmė nurodytų veiksmų;

4) esminio subjekto, kurio teisę užsiimti dalimi ar visa vykdoma veikla ar teikti paslaugas prašoma stabdyti, paaiškinimai, jeigu tokie buvo gauti.

4. Nutartimi laikinai sustabdyti teisę užsiimti dalimi ar visa esminio subjekto vykdoma veikla juridinis asmuo įpareigojamas laikinai nutraukti visą steigimo dokumentuose numatytą ūkinę, komercinę, finansinę, profesinę veiklą ar jos dalį ir uždaryti visus šia veikla ar jos dalimi susijusius padalinius. Nutartyje nurodomas laikino juridinio asmens veiklos sustabdymo terminas, kuris negali būti ilgesnis kaip 4 mėnesiai. Jeigu aplinkybės, kad šio įstatymo 28 straipsnio 1 dalies 1–4 ir 6 punktuose numatytų užtikrinimo priemonių taikymas yra neveiksmingas, išlieka, gavus Nacionalinio kibernetinio saugumo centro prašymą, teismo nutartimi šis terminas gali būti pratęstas, bet ne ilgiau kaip 2 mėnesiams. Pratęsimu skaičius neribojamas.

5. Nutartis, kuria laikinai sustabdoma dalis ar visa juridinio asmens veikla, nedelsiant nusiunčiama antstoliui vykyti, Nacionaliniam kibernetinio saugumo centrui ir, prireikus, atitinkamo viešo registro tvarkytojui.

6. Nutartis esminiam subjektui ar jo atstovui paskelbiama Civilinio proceso kodekso nustatyta tvarka.

7. Esminis subjektas teismo nutartį laikinai sustabdyti esminio subjekto veiklą gali apskųsti aukštesnės instancijos teismui per 7 darbo dienas nuo nutarties įteikimo dienos.

8. Teismas privalo panaikinti juridinio asmens veiklos laikiną sustabdymą, kai ši priemonė pasidaro nebereikalinga ir Nacionalinis kibernetinio saugumo centras prašo panaikinti laikiną sustabdymą. Nacionalinis kibernetinio saugumo centras, gavęs motyvuotą esminio subjekto, kurio visa ar dalis veiklos buvo sustabdyta, prašymą ir nustatęs, kad juridinio asmens veiklos laikinas sustabdymas yra nebereikalingas, ne vėliau kaip per 7 darbo dienas nuo prašymo gavimo dienos kreipiasi į teismą dėl laikino sustabdymo panaikinimo.

9. Nacionalinis kibernetinio saugumo centras informaciją apie subjektą, kuriam laikinai sustabdyta teisė užsiimti dalimi ar visa juridinio asmens vykdoma veikla ar teikti paslaugas, skelbia savo interneto svetainėje.

33 straipsnis. Esminio subjekto vadovo laikinas nušalinimas nuo pareigų

1. Teismas, gavęs Nacionalinio kibernetinio saugumo centro prašymą laikinai nušalinti esminio subjekto vadovą nuo pareigų, nutartimi turi teisę laikinai nušalinti esminio subjekto vadovą nuo pareigų, jeigu nustatoma, kad šio įstatymo 28 straipsnio 1 dalies 1–4 ir 6 punktuose numatytų vykdymo užtikrinimo priemonių taikymas yra neveiksmingas. Laikinas esminio subjekto vadovo nušalinimas nuo pareigų gali būti taikomas tik pavojingų pažeidimų, nurodytų šio įstatymo 29 straipsnio 2 dalyje, atveju.

2. Nacionalinis kibernetinio saugumo centras, prieš kreipdamasis į teismą su prašymu laikinai nušalinti esminio subjekto vadovą nuo pareigų šio straipsnio 1 dalyje nurodytu pagrindu, privalo esminį subjektą informuoti pateikdamas esminę informaciją apie teisės aktų nuostatas ir nustatytus faktinius duomenis, kurie sudaro laikino esminio subjekto vadovo nušalinimo nuo pareigų pagrindus, ir nustatyti terminą, kuris negali būti trumpesnis kaip 10 darbo dienų nuo pranešimo įteikimo dienos, per kurį esminis subjektas turi imtis būtinų veiksmų nustatytiems trūkumams pašalinti ar reikalavimams įvykdyti. Nacionalinis kibernetinio saugumo centras šio straipsnio 1 dalyje nustatytu pagrindu į teismą turi teisę kreiptis tik pasibaigus Nacionalinis kibernetinio saugumo centro nustatytam terminui ir esminiam subjektui nesiėmus nurodytų veiksmų.

3. Nacionalinio kibernetinio saugumo centro prašyme teismui dėl esminio subjekto vadovo laikino nušalinimo nuo pareigų turi būti nurodyta:

1) aplinkybės, įrodančios, kad šio įstatymo 28 straipsnio 1 dalies 1–4 ir 6 punktuose numatytų užtikrinimo priemonių taikymas yra neveiksmingas;

2) aplinkybės, įrodančios, kad esminiam subjektui buvo nustatytas terminas trūkumams pašalinti ar reikalavimams įvykdyti, o esminis subjektas nesiėmė nurodytų veiksmų;

3) esminio subjekto, kurio vadovą prašoma laikinai nušalinti nuo pareigų, paaiškinimai, jeigu tokie buvo gauti.

4. Nutartis, kuria esminio subjekto vadovas laikinai nušalinimas nuo pareigų, nedelsiant nusiunčiama jį į pareigas priimančiam subjektui ir Nacionaliniam kibernetinio saugumo centrui.

5. Nutartis esminio subjekto vadovui ar jo atstovui paskelbiama Civilinio proceso kodekso nustatyta tvarka.

6. Nuo teismo nutarties laikinai nušalinti esminio subjekto vadovą nuo pareigų paskelbimo dienos nušalintas nuo pareigų fizinis asmuo neturi teisės atlikti savo funkcijų ir visi po tokio teismo sprendimo paskelbimo dienos jo priimti sprendimai yra negaliojantys.

7. Laikinas esminio subjekto vadovo nušalinimas nuo pareigų negali trukti ilgiau kaip šešis mėnesius. Prireikus šios priemonės taikymas gali būti pratęstas dar iki trijų mėnesių. Pratęsimų skaičius neribojamas, bet visais atvejais nušalinimas nuo pareigų negali trukti ilgiau, nei to reikia, kad būtų užtikrinamas šio įstatymo nuostatų laikymasis.

8. Nutartį laikinai nušalinti esminio subjekto vadovą nuo pareigų, taip pat nutartį pratęsti šios priemonės taikymo terminą per 7 darbo dienas nuo nutarties paskelbimo esminis subjektas ar nušalintas esminio subjekto vadovas gali apskųsti aukštesnės instancijos teismui. Šio teismo priimta nutartis yra galutinė ir neskundžiama.

9. Teismas privalo panaikinti laikiną esminio subjekto vadovo nušalinimą nuo pareigų ar laikiną teisės užsiimti tam tikra veikla sustabdymą, kai Nacionalinis kibernetinio saugumo centras prašo panaikinti laikiną sustabdymą. Nacionalinis kibernetinio saugumo centras, gavęs motyvuotą nušalinto esminio subjekto vadovo prašymą ir nustatęs, kad esminio subjekto vadovo nušalinimas yra nebereikalingas, ne vėliau kaip per 7 darbo dienas nuo prašymo gavimo dienos privalo prašyti teismo panaikinti laikiną sustabdymą

10. Nacionalinis kibernetinio saugumo centras informaciją apie esminį subjektą, kurio vadovas laikinai nušalintas nuo pareigų, skelbia savo interneto svetainėje.

VI SKYRIUS
NACIONALINĖS KIBERNETINIO SAUGUMO SERTIFIKAVIMO INSTITUCIJOS ĮGALIOJIMAI

34 straipsnis. Nacionalinė kibernetinio saugumo sertifikavimo institucija

1. Nacionalinis kibernetinio saugumo centras vykdo Reglamente (ES) 2019/881 nustatytas nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas, turi nacionalinės kibernetinio saugumo sertifikavimo institucijos įgaliojimus.

2. Nacionalinis kibernetinio saugumo centras, vykdydamas nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas:

1) turi teisę neatlygintinai iš atitikties vertinimo įstaigų, Europos kibernetinio saugumo sertifikatų turėtojų, Europos Sąjungos atitikties pareiškimus išduodančių subjektų, valstybės ir savivaldybių institucijų ir įstaigų gauti visą nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijoms atlikti reikalingą informaciją, dokumentų kopijas ir nuorašus, duomenų kopijas, taip pat susipažinti su visais duomenimis ir dokumentais;

2) nustato įgaliojimų atitikties vertinimo įstaigoms pagal Reglamento (ES) 2019/881 60 straipsnio 3 dalį (toliau – papildomi įgaliojimai) suteikimo, apribojimo ir sustabdymo, papildomų įgaliojimų apribojimo ir sustabdymo panaikinimo, papildomų įgaliojimų atšaukimo tvarką, teikia papildomus įgaliojimus, juos apriboja, sustabdo arba atšaukia šio įstatymo 35 straipsnyje nustatytais atvejais;

3) Viešojo administravimo įstatymo nustatyta tvarka nagrinėja Reglamento (ES) 2019/881 58 straipsnio 7 dalies f punkte nurodytus skundus;

4) Reglamento (ES) 2019/881, šio įstatymo 36 straipsnyje ir Nacionalinio kibernetinio saugumo centro nustatyta tvarka atlieka tyrimus, kaip laikomasi Reglamento (ES) 2019/881 III antraštinės dalies ar Europos kibernetinio saugumo sertifikavimo schemų, kurios taikomos informacinių ir ryšių technologijų produktų, informacinių ir ryšių technologijų paslaugų, informacinių ir ryšių technologijų procesų sertifikavimui, nuostatų;

5) atlikdamas šios dalies 4 punkte nurodytus tyrimus, turi teisę įeiti į atitikties vertinimo įstaigų ir Europos kibernetinio saugumo sertifikatų turėtojų patalpas (tarp jų ir nuomojamas ar naudojamas kitais pagrindais), ne ilgesniam kaip 30 kalendorinių dienų terminui paimti dokumentų kopijas ir nuorašus, duomenų kopijas bei kitus daiktus, reikalingus atliekant tyrimus. Įeiti į juridinio asmens patalpas (tarp jų ir nuomojamas ar naudojamas kitais pagrindais) galima tik juridinio asmens darbo laiku, pateikus tarnybinį pažymėjimą. Įeiti į fiziniam asmeniui priklausančias patalpas (tarp jų ir nuomojamas ar naudojamas kitais pagrindais) galima tik pateikus teismo nutartį dėl leidimo įeiti į fiziniam asmeniui priklausančias patalpas;

6) atlikdamas šios dalies 4 punkte nurodytus tyrimus, turi teisę gauti žodinius ir rašytinius paaiškinimus iš tikrinamų juridinių ir fizinių asmenų ir reikalauti, kad jie atvyktų į nacionalinės kibernetinio saugumo sertifikavimo institucijos patalpas duoti paaiškinimų;

7) atlieka kitas Lietuvos Respublikos teisės aktuose nustatytas funkcijas kibernetinio saugumo sertifikavimo srityje.

3. Nacionalinio kibernetinio saugumo centro prašymai dėl teismo leidimo įeiti į fiziniam asmeniui priklausančias patalpas (tarp jų ir nuomojamas ar naudojamas kitais pagrindais) nagrinėjami Civilinio proceso kodekso XXXIX skyriuje nustatyta tvarka.

35 straipsnis. Papildomų įgaliojimų atitikties vertinimo įstaigoms suteikimas, apribojimas ir sustabdymas, papildomų įgaliojimų apribojimo ir sustabdymo panaikinimas, papildomų įgaliojimų atšaukimas

1. Papildomi įgaliojimai atitikties vertinimo įstaigoms suteikiami, apribojami ir sustabdomi, papildomų įgaliojimų apribojimas ir sustabdymas panaikinamas, papildomi įgaliojimai atšaukiami šiame straipsnyje ir šio įstatymo 34 straipsnio 2 dalies 2 punkte nurodytame teisės akte nustatyta tvarka.

2. Papildomi įgaliojimai suteikiami atitikties vertinimo įstaigoms užduotims atlikti pagal Europos kibernetinio saugumo sertifikavimo schemas, kai tenkinamos visos šios sąlygos:

1) atitikties vertinimo įstaiga atitinka Reglamento (ES) 2019/881 priede nustatytus reikalavimus ir turi tai patvirtinantį galiojantį akreditavimo pažymėjimą;

2) atitikties vertinimo įstaiga atitinka Europos kibernetinio saugumo sertifikavimo schemoje nustatytus specialiuosius ar papildomus reikalavimus.

3. Sprendimas dėl papildomų įgaliojimų suteikimo priimamas per 30 kalendorinių dienų nuo visų tinkamai užpildytų dokumentų, įrodančių atitikties vertinimo įstaigų atitiktį šio straipsnio 2 dalyje nurodytoms sąlygoms, gavimo.

4. Papildomus įgaliojimus suteikti atsisakoma, jeigu Nacionalinis kibernetinio saugumo centras nustato, kad atitikties vertinimo įstaiga neatitinka šio straipsnio 2 dalyje nurodytų sąlygų.

5. Papildomi įgaliojimai apribojami Nacionalinio kibernetinio saugumo centro sprendimu, kuriame nurodomas papildomų įgaliojimų apribojimo pagrindas, taikomi apribojimai ir, jeigu papildomi įgaliojimai apribojami šios dalies 2 punkte nustatytu pagrindu, terminas, kuris negali būti ilgesnis kaip 6 mėnesiai ir per kurį atitikties vertinimo įstaiga turi pašalinti pažeidimus, dėl kurių apribojami papildomi įgaliojimai, kai yra bent viena iš šių sąlygų:

1) pasikeitė Europos kibernetinio saugumo sertifikavimo schemoje nustatyti specialieji ar papildomi reikalavimai;

2) Nacionalinis kibernetinio saugumo centras, atlikdamas tyrimą, nustato, kad atitikties vertinimo įstaiga nesilaiko Reglamento (ES) 2019/881 reikalavimų arba pažeidė Europos kibernetinio saugumo sertifikavimo schemoje, dėl kurios buvo suteikti papildomi įgaliojimai, nustatytus reikalavimus;

3) Lietuvos Respublikos atitikties įvertinimo įstatymo nustatyta tvarka pakeistas akreditavimo pažymėjimas.

6. Priėmus sprendimą apriboti papildomus įgaliojimus, atitikties vertinimo įstaigai draudžiama vykdyti sprendime nurodytas užduotis pagal Europos kibernetinio saugumo sertifikavimo schemą, dėl kurios buvo išduoti papildomi įgaliojimai.

7. Papildomų įgaliojimų apribojimas panaikinamas, kai atitikties vertinimo įstaiga ne vėliau kaip per 7 mėnesius nuo sprendimo apriboti papildomus įgaliojimus priėmimo dienos pateikia prašymą, o Nacionalinis kibernetinio saugumo centras atlieka tyrimą šio įstatymo 36 straipsnyje nustatyta tvarka ir nustato, kad:

1) atitikties įvertinimo įstaiga atitinka Europos kibernetinio saugumo sertifikavimo schemoje nustatytus reikalavimus, jeigu papildomi įgaliojimai buvo apriboti šio straipsnio 5 dalies 1 punkte nustatytu pagrindu;

2) atitikties įvertinimo įstaiga per Nacionalinio kibernetinio saugumo centro nustatytą terminą pašalino pažeidimus, dėl kurių papildomi įgaliojimai buvo apriboti;

3) Lietuvos Respublikos atitikties vertinimo įstatymo nustatyta tvarka keičiant akreditavimo pažymėjimą nėra susiaurinta akreditavimo sritis, dėl kurios buvo išduoti papildomi įgaliojimai, jeigu papildomi įgaliojimai buvo apriboti šio straipsnio 5 dalies 3 punkte nustatytu pagrindu.

8. Papildomi įgaliojimai sustabdomi Nacionalinio kibernetinio saugumo centro sprendimu. Šiame sprendime nurodomas papildomų įgaliojimų sustabdymo pagrindas ir, jeigu papildomi įgaliojimai sustabdomi šios dalies 2 punkte nustatytu pagrindu, terminas, kuris negali būti ilgesnis kaip 6 mėnesiai ir per kurį atitikties vertinimo įstaiga turi pašalinti pažeidimus, dėl kurių sustabdomi papildomi įgaliojimai, kai yra bent viena iš šių sąlygų:

1) atitikties vertinimo įstaiga pateikė prašymą Nacionaliniam kibernetinio saugumo centrui sustabdyti jai suteiktus papildomus įgaliojimus prašyme nurodytam terminui, kuris negali būti ilgesnis kaip 6 mėnesiai;

2) Nacionalinis kibernetinio saugumo centras, atlikdamas tyrimą, nustato, kad atitikties vertinimo įstaiga, kurios papildomi įgaliojimai buvo apriboti šio straipsnio 5 dalies 2 punkte nustatytu pagrindu, per Nacionalinio kibernetinio saugumo centro nustatytą terminą nepašalino pažeidimų, dėl kurių papildomi įgaliojimai buvo apriboti;

3) Atitikties vertinimo įstatymo nustatyta tvarka sustabdomas akreditavimo pažymėjimo galiojimas.

9. Papildomų įgaliojimų sustabdymas panaikinamas, kai atitikties vertinimo įstaiga ne vėliau kaip per 7 mėnesius nuo sprendimo sustabdyti papildomus įgaliojimus priėmimo dienos pateikia prašymą, o Nacionalinis kibernetinio saugumo centras atlieka tyrimą šio įstatymo 36 straipsnyje nustatyta tvarka ir nustato, kad:

1) atitikties vertinimo įstaiga atitinka Europos kibernetinio saugumo sertifikavimo schemoje nustatytus reikalavimus, jeigu jai suteikti papildomi įgaliojimai buvo sustabdyti šio straipsnio 8 dalies 1 punkte nustatytu pagrindu;

2) atitikties vertinimo įstaiga per Nacionalinio kibernetinio saugumo centro nustatytą terminą pašalino pažeidimus, dėl kurių papildomi įgaliojimai buvo sustabdyti;

3) Atitikties įvertinimo įstatymo nustatyta tvarka panaikintas akreditavimo pažymėjimo galiojimo sustabdymas, jeigu papildomi įgaliojimai buvo sustabdyti šio straipsnio 8 dalies 3 punkte nustatytu pagrindu.

10. Papildomi įgaliojimai atšaukiami Nacionalinio kibernetinio saugumo centro sprendimu, kai yra bent viena iš šių sąlygų:

1) atitikties vertinimo įstaiga pateikė prašymą Nacionaliniam kibernetinio saugumo centrui atšaukti jai suteiktus papildomus įgaliojimus;

2) atitikties vertinimo įstaiga nepateikė prašymo dėl papildomų įgaliojimų apribojimo ar sustabdymo panaikinimo per šio straipsnio 7 ir 9 dalyse nurodytus terminus;

3) atitikties vertinimo įstaiga per Nacionalinio kibernetinio saugumo centro nustatytą terminą nepašalino pažeidimų, dėl kurių papildomi įgaliojimai buvo sustabdyti;

4) atitikties vertinimo įstaiga, kurios papildomi įgaliojimai apriboti ar sustabdyti, toliau atlieka užduotis pagal Europos kibernetinio saugumo sertifikavimo schemą, dėl kurios papildomi įgaliojimai buvo apriboti ar sustabdyti;

5) Atitikties įvertinimo įstatymo nustatyta tvarka panaikintas akreditavimo pažymėjimo galiojimas arba yra susiaurinta akreditavimo sritis, dėl kurios buvo išduoti papildomi įgaliojimai.

36 straipsnis. Tyrimo atlikimas

1. Nacionalinis kibernetinio saugumo centras turi teisę pradėti tyrimą bet kokiu klausimu, susijusiu su Reglamento (ES) 2019/881 III antraštinės dalies ar Europos kibernetinio saugumo sertifikavimo schemų nuostatų galimu pažeidimu ar jų laikymosi stebėsena.

2. Pagrindas pradėti tyrimą gali būti skundai, teikiami pagal Reglamento (ES) 2019/881 58 straipsnio 7 dalies f punktą, atitikties vertinimo įstaigų prašymai, teikiami pagal šio įstatymo 35 straipsnį, ir kiti šaltiniai. Nacionalinis kibernetinio saugumo centras turi teisę pradėti tyrimą ir savo iniciatyva.

3. Tyrimas turi būti atliktas per kuo trumpesnį terminą, bet ne vėliau kaip per 4 mėnesius nuo šio straipsnio 2 dalyje nurodyto skundo ar prašymo gavimo dienos arba sprendimo atlikti tyrimą kitų šaltinių, nurodytų šio straipsnio 2 dalyje, pagrindu priėmimo dienos.

4. Atsižvelgiant į tyrimo sudėtingumą, tyrimo mastą, atitikties vertinimo įstaigų, Europos kibernetinio saugumo sertifikatų turėtojų ir Europos Sąjungos atitikties pareiškimų išdavėjų veiklos pobūdį bei vengimą vykdyti Nacionalinio kibernetinio saugumo centro reikalavimus, tyrimo metu paaiškėjusias naujas aplinkybes arba kitas objektyvias priežastis, šio straipsnio 3 dalyje nustatytas terminas Nacionalinio kibernetinio saugumo centro sprendimu gali būti pratęstas, bet ne ilgiau kaip 2 mėnesiams. Bendras tyrimo atlikimo terminas negali būti ilgesnis kaip 6 mėnesiai nuo šio straipsnio 2 dalyje nurodyto skundo ar prašymo gavimo dienos arba sprendimo atlikti tyrimą kitų šaltinių, nurodytų šio straipsnio 2 dalyje, pagrindu priėmimo dienos. Apie tyrimo termino pratęsimą ir priežastis, dėl kurių šis terminas pratęstas, Nacionalinis kibernetinio saugumo centras privalo nedelsdamas, bet ne vėliau kaip iki šio straipsnio 3 dalyje nurodyto termino pabaigos, pranešti atitikties vertinimo įstaigai, Europos kibernetinio saugumo sertifikatų turėtojui ar Europos Sąjungos atitikties pareiškimų išdavėjui.

5. Nacionalinis kibernetinio saugumo centras, baigęs tyrimą, priima bent vieną iš šių sprendimų:

1) konstatuoti, kad pažeidimų nenustatyta;

2) pateikti atitikties vertinimo įstaigai, Europos kibernetinio saugumo sertifikatų turėtojui ar Europos Sąjungos atitikties pareiškimų išdavėjui nurodymus ir rekomendacijas, jeigu tyrimo metu nustatoma, kad taikomi netinkami veiklos būdai ar praktikos;

3) pradėti administracinio nusižengimo teiseną;

4) pripažinti Europos Sąjungos atitikties pareiškimą, išduotą pagal Reglamento (ES) 2019/881 53 straipsnio 2 dalį, negaliojančiu, jeigu tyrimo metu nustatoma, kad nesilaikoma Reglamento (ES) 2019/881 arba Europos kibernetinio saugumo sertifikavimo schemoje nustatytų reikalavimų;

5) panaikinti savo paties arba pagal Reglamento (ES) 2019/881 56 straipsnio 6 dalį atitikties vertinimo įstaigos išduoto Europos kibernetinio saugumo sertifikato galiojimą, jeigu tyrimo metu nustatoma, kad Europos kibernetinio saugumo sertifikatas neatitinka Reglamento (ES) 2019/881 arba Europos kibernetinio saugumo sertifikavimo schemoje nustatytų reikalavimų;

6) apriboti, sustabdyti, atšaukti atitikties vertinimo įstaigų papildomus įgaliojimus arba panaikinti papildomų įgaliojimų apribojimą ar sustabdymą šio įstatymo 35 straipsnyje nustatytais atvejais.

6. Šio straipsnio 5 dalies 2 punkte numatyti nurodymai ir rekomendacijos pateikiami per 20 darbo dienų nuo sprendimo priėmimo dienos.

7. Nacionalinio kibernetinio saugumo centro sprendimai, išskyrus sprendimą, nurodytą šio straipsnio 5 dalies 3 punkte, gali būti skundžiami teismui Administracinių bylų teisenos įstatymo nustatyta tvarka.

VII SKYRIUS
SAUGIOJO VALSTYBINIO DUOMENŲ PERDAVIMO TINKLO NAUDOJIMO PAGRINDAI

37 straipsnis. Saugusis valstybinis duomenų perdavimo tinklas

1. Valstybės ir savivaldybių institucijos ir įstaigos, valstybės valdomos įmonės ir viešosios įstaigos (toliau kartu – institucijos), įrašytos į Saugiojo valstybinio duomenų perdavimo tinklo (toliau – Saugusis tinklas) naudotojų sąrašą, privalo naudotis tik Saugiuoju tinklu teikiamomis elektroninių ryšių paslaugomis ir jungtis prie viešųjų elektroninių ryšių tinklų tik per Saugųjį tinklą, išskyrus atvejus, kai elektroninių ryšių paslaugomis naudotis ir (ar) prie viešųjų elektroninių ryšių tinklų jungtis ne per Saugųjį tinklą yra būtina renkant ir (ar) teikiant žvalgybos informaciją. Kai nėra techninių galimybių jungtis prie viešųjų elektroninių ryšių tinklų tik per Saugųjį tinklą, institucijos turi teisę Vyriausybės ar jos įgaliotos institucijos nustatytais atvejais ir tvarka prie viešųjų elektroninių ryšių tinklų jungtis ne per Saugųjį tinklą. Saugiojo tinklo naudotojų sąrašą krašto apsaugos ministro teikimu tvirtina Vyriausybė. Saugiuoju tinklu negali naudotis į Saugiojo tinklo naudotojų sąrašą neįtraukti subjektai. Krašto apsaugos ministras bent kartą per metus peržiūri Saugiojo tinklo naudotojų sąrašą ir prireikus inicijuoja šio sąrašo pakeitimus.

2. Į Saugiojo tinklo naudotojų sąrašą yra įrašomos institucijos, atitinkančios bent vieną iš šių kriterijų:

1) institucija valdo ar tvarko valstybės informacinius išteklius, būtinus gyvybiškai svarbioms valstybės funkcijoms atlikti ir valstybinėms mobilizacinėms užduotims vykdyti;

2) institucija, atlikdama gyvybiškai svarbias valstybės funkcijas, dalyvauja vykdant valstybines mobilizacines užduotis, kurioms atlikti būtina perduoti duomenis institucijoms, valdančioms ir (ar) tvarkančioms valstybės informacinius išteklius, būtinus gyvybiškai svarbioms valstybės funkcijoms atlikti ir valstybinėms mobilizacinėms užduotims vykdyti, ir (ar) gauti tokius duomenis;

3) institucija Vyriausybės įgaliotos institucijos išvadoje įvardijama kaip būtina nacionaliniam saugumui, gynybai ar gyvybiškai svarbioms valstybės funkcijoms užtikrinti;

4) institucijai atliekant savo funkcijas būtina naudotis Saugiuoju tinklu arba jai reikalinga prieiga prie Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (ar) NATO valstybėse narėse esančių institucijų ar duomenų centrų.

3. Saugųjį tinklą valdo Krašto apsaugos ministerija, o tvarko krašto apsaugos ministro įgaliota valstybės biudžetinė įstaiga.

4. Specialiuosius organizacinius ir techninius reikalavimus, taikomus Saugiajam tinklui, Saugiojo tinklo paslaugoms bei prekių ir paslaugų Saugiajam tinklui teikėjams, ir Saugiojo tinklo nuostatus tvirtina Saugiojo tinklo valdytojas. Saugiojo tinklo tvarkytojas užtikrina, kad būtų įgyvendinti specialieji organizaciniai ir techniniai reikalavimai, taikomi Saugiajam tinklui, taip pat kad būtų teikiamos Saugiojo tinklo standartinės ir papildomos elektroninių ryšių ir kibernetinio saugumo paslaugos. Saugiuoju tinklu teikiamų elektroninių ryšių ir kibernetinio saugumo paslaugų teikimo sąlygas ir taisykles nustato Vyriausybė ar jos įgaliota institucija. Saugiajam tinklui veikti reikiamos prekės ir paslaugos įsigyjamos laikantis Lietuvos Respublikos viešųjų pirkimų įstatymo reikalavimų.

5. Saugiuoju tinklu teikiamas standartines elektroninių ryšių ir kibernetinio saugumo paslaugas (toliau – standartinės paslaugos) sudaro:

1) šio tinklo valdytojo nustatytos spartos duomenų perdavimas Saugiojo tinklo naudotojams ir jų struktūriniams padaliniams;

2) šio tinklo valdytojo nustatytos spartos prieiga prie viešųjų ryšių tinklų;

3) kolektyvinė apsauga kibernetinio saugumo priemonėmis;

4) sąveika su Europos Sąjungos ir jos valstybių narių institucijų valdomais informaciniais ištekliais;

5) valstybės valdomų elektroninių ryšių tinklų, kurie naudojami vykdant valstybines mobilizacines užduotis, dalių sujungimas;

6) techninės bendradarbiavimo priemonės Saugiojo tinklo naudotojų ir jų struktūrinių padalinių tarpusavio sąveikai užtikrinti.

6. Standartinių paslaugų kiekybiniai ir kokybiniai rodikliai nustatomi Vyriausybės ar jos įgaliotos institucijos Saugiuoju tinklu teikiamų elektroninių ryšių ir kibernetinio saugumo paslaugų teikimo sąlygų apraše ir taisyklėse. Saugiojo tinklo tvarkytojas užtikrina neatlygintiną standartinių paslaugų teikimą Saugiojo tinklo naudotojams. Išlaidos, patirtos dėl neatlygintinai teikiamų standartinių paslaugų, apmokamos iš Saugiajam tinklui tvarkyti skiriamų valstybės biudžeto lėšų ir (ar) kitų teisės aktuose nustatytų finansavimo šaltinių.

7. Saugiuoju tinklu teikiamas papildomas elektroninių ryšių ir kibernetinio saugumo paslaugas (toliau – papildomos paslaugos) sudaro šio straipsnio 5 dalyje nurodytos paslaugos, kurių kiekybiniai ar kokybiniai rodikliai, atsižvelgiant į Saugiojo tinklo naudotojų poreikius, skiriasi nuo nustatytų standartinių paslaugų rodiklių.

8. Atlyginimo už naudojimąsi papildomomis paslaugomis dydžių nustatymo kriterijus ir atlyginimo apskaičiavimo tvarkos aprašą tvirtina Vyriausybė. Krašto apsaugos ministras, atsižvelgdamas į atlyginimo už naudojimąsi Saugiuoju tinklu dydžių kriterijus, tvirtina atlyginimo už naudojimąsi Saugiuoju tinklu dydžius. Atlyginimas už papildomas paslaugas neturi viršyti sąnaudų, patiriamų teikiant šias paslaugas. Papildomų paslaugų teikimo sąnaudos Saugiojo tinklo tvarkytojo lėšomis turi būti patikrintos auditoriaus ar audito įmonės, o patikrinti duomenys apie patirtas sąnaudas per 2 mėnesius nuo kalendorinių metų pabaigos turi būti pateikti Vyriausybės įgaliotai institucijai. Vyriausybės įgaliota institucija vertina, ar atlyginimo už papildomų paslaugų teikimą dydžiai nustatyti atsižvelgiant į Vyriausybės patvirtintus atlyginimo už naudojimąsi papildomomis paslaugomis dydžių nustatymo kriterijus, ir teikia išvadą Saugiojo tinklo tvarkytojui.

9. Institucijų prisijungimo prie Saugiojo tinklo ir atsijungimo nuo jo sąlygas, planą ir terminus nustato Vyriausybė ar jos įgaliota institucija.

38 straipsnis. Duomenų centrų naudojimas

1. Institucijos, įrašytos į Saugiojo tinklo naudotojų sąrašą, išskyrus žvalgybos institucijas, savo valdomus valstybės informacinius išteklius laiko valstybiniuose duomenų centruose arba Lietuvos Respublikoje ar kitose Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (ar) NATO valstybėse narėse esančiuose duomenų centruose, vadovaudamosi Valstybės informacinių išteklių valdymo įstatymo 45 straipsnio 1–4 ir 6 dalių nuostatomis. Į Saugiojo tinklo naudotojų sąrašą įrašytos žvalgybos institucijos savo valdomus valstybės informacinius išteklius laiko savo valdomuose duomenų centruose, o valstybės informacinius išteklius sudarančių duomenų ir informacinių sistemų, kuriose šie duomenys tvarkomi, kopijos žvalgybos institucijos vadovo sprendimu gali būti laikomos Lietuvos Respublikoje ar kitose Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (ar) NATO valstybėse narėse esančiuose duomenų centruose.

2. Visų institucijų išlaidos, patirtos dėl jų valdomų valstybės informacinių išteklių ir (ar) jų kopijų laikymo valstybiniuose duomenų centruose arba Lietuvos Respublikoje ar kitose Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (ar) NATO valstybėse narėse esančiuose duomenų centruose, apmokamos iš šioms institucijoms skirtų valstybės biudžeto lėšų ir (ar) iš šių institucijų veiklą reglamentuojančiuose kituose teisės aktuose nustatytų finansavimo šaltinių.

3. Valstybinių duomenų centrų sąrašas, techniniai ir organizaciniai reikalavimai, taikomi valstybiniams duomenų centrams ir Lietuvos Respublikoje ar kitose Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (ar) NATO valstybėse narėse esantiems duomenų

centrams, kuriuose laikomi valstybės informaciniai ištekliai, tvirtinami Valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka.

Lietuvos Respublikos
kibernetinio saugumo įstatymo
1 priedas

YPATINGOS SVARBOS SEKTORIAI

Sektorius	**Subsektorius**	**Subjekto rūšis**	**Institucija, atsakinga už identifikavimą**
1. Energetika	1.1. Elektra	1.1.1. Elektros energetikos įmonės, vykdančios elektros energijos tiekimo funkciją.	Lietuvos Respublikos energetikos ministerija
		1.1.2. Elektros energijos skirstomųjų tinklų operatorius.	Energetikos ministerija
		1.1.3. Elektros energijos perdavimo sistemos operatorius.	Energetikos ministerija
		1.1.4. Elektros energijos gamintojas.	Energetikos ministerija
		1.1.5. Paskirtieji elektros energijos rinkos operatoriai, kaip apibrėžta 2019 m. birželio 5 d. Europos Parlamento ir Tarybos reglamento (ES) 2019/943 dėl elektros energijos vidaus rinkos 2 straipsnio 8 punkte.	Energetikos ministerija
		1.1.6. Elektros energijos rinkos dalyviai, kaip apibrėžta 2019 m. birželio 5 d. Europos Parlamento ir Tarybos reglamento (ES) 2019/(ES) 2019/943 dėl elektros energijos vidaus rinkos 2 straipsnio 25 punkte, teikiantys elektros energijos paklausos telkimo, energijos kaupimo paslaugas, , bei teikiantys elektros energijos reguliavimo apkrovos paslaugas.	Energetikos ministerija
		1.1.7. Elektromobilių įkrovimo prieigos operatorius.	Energetikos ministerija
	1.2. Centralizuotas šilumos ir vėsumos tiekimas	1.2.1. Centralizuoto šilumos ar vėsumos energijos tiekimo operatoriai.	Energetikos ministerija
	1.3. Nafta	1.3.1. Naftotiekį valdanti įmonė.	Energetikos ministerija
		1.3.2. Naftos gamybos įmonė. Naftos perdirbimo įmonė. Naftą importuojanti įmonė, naftą įvežanti įmonė, naftos atsargas kaupianti įmonė, naftos atsargas tvarkanti įmonė.	Energetikos ministerija
		1.3.3.Centrinė naftos produktus ir naftos atsargas kaupianti ir tvarkanti organizacija.	Energetikos ministerija
	1.4. Dujos	1.4.1. Gamtinių dujų tiekimo įmonė.	Energetikos ministerija

		1.4.2. Gamtinių dujų skirstymo sistemos operatorius.	Energetikos ministerija
		1.4.3. Gamtinių dujų perdavimo sistemos operatorius.	Energetikos ministerija
		1.4.4. Gamtinių dujų laikymo sistemos operatorius.	Energetikos ministerija
		1.4.5. Suskystintų gamtinių dujų sistemos operatorius.	Energetikos ministerija
		1.4.6. Gamtinių dujų įmonė.	Energetikos ministerija
		1.4.7. Gamtinių dujų perdirbimo ir apdorojimo įrenginių operatoriai.	Energetikos ministerija
	1.5. Vandenilis	1.5.1. Vandenilio gamybos, laikymo ir perdavimo operatoriai.	Energetikos ministerija
2. Transportas	2.1. Oro transportas	2.1.1. Oro vežėjai, kaip apibrėžta 2008 m. kovo 11 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 300/2008 dėl civilinės aviacijos saugumo bendrųjų taisyklių ir panaikinančio Reglamentą (EB) Nr. 2320/2002 3 straipsnio 4 punkte, naudojami komerciniais tikslais.	Lietuvos Respublikos susisiekimo ministerija
		2.1.2. Oro uostas, įskaitant 2013 m. gruodžio 11 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 1315/2013 dėl Sąjungos transeuropinio transporto tinklo plėtros gairių, kuriuo panaikinamas Sprendimas Nr. 661/2010/ES, II priedo 2 skirsnyje išvardytus pagrindinius oro uostus, ir oro uostą valdančios įmonės vadovas. Subjektai, eksploatuojantys oro uostuose esančius pagalbinius įrenginius.	Susisiekimo ministerija
		2.1.3. Skrydžių valdymo operatoriai, teikiantys skrydžių valdymo paslaugas, kaip apibrėžta 2004 m. kovo 10 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 549/2004, nustatančio bendro Europos dangaus sukūrimo pagrindą, 2 straipsnio 1 punkte.	Susisiekimo ministerija
	2.2. Geležinkelių transportas	2.2.1. Geležinkelių infrastruktūros valdytojas.	Susisiekimo ministerija
		2.2.2. Geležinkelių įmonė (vežėjas).	Susisiekimo ministerija
		2.2.3. Geležinkelių paslaugų įrenginio operatorius.	Susisiekimo ministerija
	2.3. Vandens transportas	2.3.1. Vidaus vandenų, jūrų ir priekrantės keleivinio ir krovininio vandens transporto bendrovės, kaip apibrėžta jūrų transporto atžvilgiu 2004 m. kovo 31 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 725/2004 dėl laivų ir uostų įrenginių apsaugos stiprinimo I priede, neįskaitant tų bendrovių eksploatuojamų atskirų laivų.	Susisiekimo ministerija
		2.3.2. Uostus, , įskaitant jų uosto įrenginius, kaip apibrėžta 2004 m. kovo 31 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 725/2004 dėl laivų ir	Susisiekimo ministerija

		uostų įrenginių apsaugos stiprinimo 2 straipsnio 11 punkte, valdančios įmonės, bei subjektai, eksploatuojantys uostuose esančias įmones ir įrenginius.	
		2.3.3. Laivų eismo tarnybų operatoriai.	Susisiekimo ministerija
	2.4. Kelių transportas	2.4.1. Kelių direkcijos, kaip apibrėžta 2014 m. gruodžio 18 d. Komisijos deleguotojo (ES) Nr. 2015/962, kuriuo papildomos Europos Parlamento ir Tarybos direktyvos 2010/40/ES nuostatos, susijusios su visoje Europos Sąjungoje teikiamomis tikralaikės eismo informacijos paslaugomis, 2 straipsnio 12 punkte, atsakingos už eismo valdymo kontrolę, išskyrus viešuosius subjektus, kuriems eismo valdymo arba intelektinių transporto sistemų operatoriaus veikla yra tik neesminė jų bendrosios veiklos dalis.	Susisiekimo ministerija
		2.4.2. Intelektinių transporto sistemų operatoriai.	Susisiekimo ministerija
3. Bankininkystė		3.1.1. Kredito įstaigos, kaip apibrėžta 2013 m. birželio 26 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 575/2013 dėl prudencinių reikalavimų kredito įstaigoms ir investicinėms įmonėms ir kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012 4 straipsnio 1 punkte.	Lietuvos Respublikos finansų ministerija
4. Finansų rinkų infrastruktūros objektai		4.1.1. Prekybos vietų operatoriai.	Finansų ministerija
		4.1.2. Pagrindinės sandorio šalys, kaip apibrėžta 2013 m. birželio 26 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 648/2012 dėl ne biržos išvestinių finansinių priemonių, pagrindinių sandorio šalių ir sandorių duomenų saugyklų 2 straipsnio 1 punkte.	Finansų ministerija
5. Sveikatos priežiūra		5.1.1. Asmens sveikatos priežiūros įstaiga.	Lietuvos Respublikos sveikatos apsaugos ministerija
		5.1.2. Europos Sąjungos etaloninės laboratorijos, nurodytos 2022 m. lapkričio 23 d. Europos Parlamento ir Tarybos reglamento (ES) 2022/2371 dėl didelių tarpvalstybinio pobūdžio grėsmių sveikatai, kuriuo panaikinamas Sprendimas Nr. 1082/2013/ES, 15 straipsnyje.	Sveikatos apsaugos ministerija
		5.1.3. Subjektai, vykdantys vaistų (vaistinių preparatų), mokslinių tyrimų ir kūrimo veiklą.	Sveikatos apsaugos ministerija
		5.1.4. Subjektai, gaminantys pagrindinius farmacijos produktus ir farmacijos preparatus, nurodytus Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 21 skyriuje.	Sveikatos apsaugos ministerija

		5.1.5. Subjektai, gaminantys medicinos priemones, kurios laikomos ypatingos svarbos ekstremaliosios visuomenės sveikatos situacijos atveju (ypatingos svarbos medicinos priemonių ekstremaliosios visuomenės sveikatos situacijos atveju sąrašas), kaip tai suprantama pagal 2022 m. sausio 25 d. Europos Parlamento ir Tarybos reglamento (ES) 2022/123 dėl didesnio Europos vaistų agentūros vaidmens pasirengimo vaistų ir medicinos priemonių krizei ir jos valdymo srityje 22 straipsnį.	Sveikatos apsaugos ministerija
6. Geriamasis vanduo		6.1.1. Žmonėms vartoti skirto vandens tiekėjai ir skirstytojai, išskyrus skirstytojus, kuriems žmonėms vartoti skirto vandens skirstymas yra neesminė jų bendrosios kitų prekių ir produktų paskirstymo veiklos dalis.	Lietuvos Respublikos aplinkos ministerija
7. Nuotekos		7.1.1. Nuotekas renkančios, šalinančios ar valančios įmonės, išskyrus įmones, kurioms miesto nuotekų, buitinių nuotekų ar pramoninių nuotekų rinkimas, šalinimas ar valymas yra neesminė jų bendrosios veiklos dalis.	Aplinkos ministerija
8. Skaitmeninė infrastruktūra		8.1.1. Interneto duomenų srautų mainų taško teikėjai.	Susisiekimo ministerija
		8.1.2. Domenų vardų sistemos paslaugų teikėjai.	Lietuvos Respublikos ekonomikos ir inovacijų ministerija
		8.1.3. Aukščiausio lygio domenų vardų registro paslaugas teikiantys subjektai.	Ekonomikos ir inovacijų ministerija
		8.1.4. Debesijos kompiuterijos paslaugų teikėjai.	Ekonomikos ir inovacijų ministerija
		8.1.5. Duomenų centrų paslaugų teikėjai.	Ekonomikos ir inovacijų ministerija
		8.1.6. Turinio teikimo tinklo teikėjai.	Ekonomikos ir inovacijų ministerija
		8.1.7. Patikimumo užtikrinimo paslaugų teikėjai.	Ekonomikos ir inovacijų ministerija
		8.1.8. Viešųjų elektroninių ryšių tinklų teikėjai.	Susisiekimo ministerija
		8.1.9. Viešųjų elektroninių ryšių paslaugų teikėjai.	Susisiekimo ministerija
9. Informacinių ir ryšių technologijų paslaugų		9.1.1. Valdomų paslaugų teikėjai.	Ministerijos
		9.1.2. Valdomų saugumo paslaugų teikėjai.	Ministerijos

valdymas (verslas verslui)			
10. Viešasis administravimas		10.1.1. Valstybinio administravimo subjektai.	Lietuvos Respublikos vidaus reikalų ministerija
		10.1.2. Regioninio administravimo subjektai ir savivaldybių administravimo subjektai.	Vidaus reikalų ministerija
11. Kosmosas		11.1.1. Lietuvos Respublikos įsteigtos arba privatiems subjektams priklausančios, jų valdomos ir eksploatuojamos antžeminės infrastruktūros operatoriai, kurie remia kosminių paslaugų teikimą, išskyrus viešųjų elektroninių ryšių tinklų teikėjus.	Ekonomikos ir inovacijų ministerija

Lietuvos Respublikos
kibernetinio saugumo įstatymo
2 priedas

KITI ITIN SVARBŪS SEKTORIAI

Sektorius	Subsektorius	Subjekto rūšis	Institucija, atsakinga už subjektų identifikavimą
1. Pašto paslaugos		1.1.1. Pašto paslaugos teikėjai.	Lietuvos Respublikos susisiekimo ministerija
2. Atliekų tvarkymas		2.1.1. Atliekų tvarkymo paslaugų teikėjai, išskyrus paslaugų teikėjus, kurių pagrindinė ekonominė veikla nėra atliekų tvarkymas.	Lietuvos Respublikos aplinkos ministerija
3. Cheminių medžiagų gamyba ir platinimas		3.1.1. Chemines medžiagas gaminančios ir chemines medžiagas ar mišinius platinančios įmonės, kaip nurodyta 2006 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 1907/2006 dėl cheminių medžiagų registracijos, įvertinimo, autorizacijos ir apribojimų (REACH), įsteigiančio Europos cheminių medžiagų agentūrą, iš dalies keičiančio Direktyvą 1999/45/EB bei panaikinančio Tarybos reglamentą (EEB) Nr. 793/93, Komisijos reglamentą (EB) Nr. 1488/94, Tarybos direktyvą 76/769/EEB ir Komisijos direktyvas 91/155/EEB, 93/67/EEB, 93/105/EB bei 2000/21/EB, 3 straipsnio 9 ir 14 punktuose, ir gaminius, kaip apibrėžta to paties reglamento 3 straipsnio 3 punkte, iš tų medžiagų ar mišinių gaminančios įmonės.	Aplinkos ministerija
4. Maisto gamyba, perdirbimas ir platinimas		4.1.1. Maisto verslo įmonės, kaip apibrėžta 2002 m. sausio 28 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 178/2002, nustatančio maistui skirtų teisės aktų bendruosius principus ir reikalavimus, įsteigiančio Europos maisto saugos tarnybą ir nustatančio su maisto saugos klausimais susijusias procedūras, 3 straipsnio 2 punkte, vykdančios didmeninio platinimo ir pramoninės gamybos bei perdirbimo veiklą.	Lietuvos Respublikos žemės ūkio ministerija
5. Gamyba	5.1. Medicinos priemonių ir *in vitro* diagnostikos medicinos priemonių gamyba	5.1.1. Medicinos priemones, kaip apibrėžta 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamento (ES) 2017/745 dėl medicinos priemonių, kuriuo iš dalies keičiama Direktyva 2001/83/EB, Reglamentas (EB) Nr. 178/2002 ir Reglamentas (EB) Nr. 1223/2009, ir kuriuo panaikinamos Tarybos direktyvos 90/385/EEB ir 93/42/EEB, 2 straipsnio 1 punkte, gaminantys subjektai ir *in vitro* diagnostikos medicinos priemones, kaip apibrėžta 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos	Lietuvos Respublikos sveikatos apsaugos ministerija

		reglamento (ES) 2017/746 dėl *in vitro* diagnostikos medicinos priemonių, kuriuo panaikinama Direktyva 98/79/EB ir Komisijos sprendimas 2010/227/ES, 2 straipsnio 2 punkte, gaminantys subjektai, išskyrus šios įstatymo I priedo 5.1.5 papunktyje nurodytas medicinos priemones gaminančius subjektus.	
	5.2. Kompiuterinių, elektroninių ir optinių gaminių gamyba	5.2.1. Subjektai, vykdantys bet kurią ekonominę veiklą, nurodytą Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 26 skyriuje.	Lietuvos Respublikos ekonomikos ir inovacijų ministerija
	5.3. Elektros įrangos gamyba	5.3.1. Subjektai, vykdantys bet kurią ekonominę veiklą, nurodytą Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 27 skyriuje.	Lietuvos Respublikos energetikos ministerija
	5.4. Niekur kitur nepriskirtų mašinų ir įrangos gamyba	5.4.1. Subjektai, vykdantys bet kurią ekonominę veiklą, nurodytą Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 28 skyriuje.	Ministerijos
	5.5. Motorinių transporto priemonių, priekabų ir puspriekabių gamyba	5.5.1. Subjektai, vykdantys bet kurią ekonominę veiklą, nurodytą Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 29 skyriuje.	Susisiekimo ministerija
	5.6. Kitos transporto įrangos gamyba	5.6.1. Subjektai, vykdantys bet kurią ekonominę veiklą, nurodytą Ekonominės veiklos rūšių klasifikatoriaus 2 redakcijos C skirsnio 30 skyriuje.	Susisiekimo ministerija
6. Infromacinės visuomenės paslaugos		6.1.1. Elektroninių prekyviečių paslaugų teikėjai.	Ekonomikos ir inovacijų ministerija
		6.1.2. Paieškos sistemų teikėjai.	Ekonomikos ir inovacijų ministerija
		6.1.3. Socialinių tinklų paslaugų platformos teikėjai.	Ekonomikos ir inovacijų ministerija
		6.1.4. Subjektas, teikiantis elektroninės informacijos prieglobos paslaugas.	Ekonomikos ir inovacijų ministerija
7. Moksliniai tyrimai		7.1.1. Mokslinius tyrimus vykdantys subjektai.	Lietuvos Respublikos švietimo, mokslo ir sporto ministerija

Lietuvos Respublikos
kibernetinio saugumo įstatymo
3 priedas

ĮGYVENDINAMI EUROPOS SĄJUNGOS TEISĖS AKTAI

1. 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013.

2. 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/887, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas.

3. 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148.“

2 straipsnis. Įstatymo įsigaliojimas, įgyvendinimas ir taikymas

1. Šis įstatymas, išskyrus šio įstatymo 2 dalį, įsigalioja 2024 m. spalio 18 d.

2. Lietuvos Respublikos Vyriausybė, krašto apsaugos ministras, Nacionalinio kibernetinio saugumo centro direktorius iki 2024 m. spalio 17 d. priima šio įstatymo įgyvendinamuosius teisės aktus.

3. Nacionalinis kibernetinio saugumo centras iki 2025 m. balandžio 17 d. identifikuoja šio įstatymo 1 ir 2 prieduose nurodytuose sektoriuose veikiančius kibernetinio saugumo subjektus, atitinkančius šiuo įstatymu nauja redakcija išdėstyto Kibernetinio saugumo įstatymo 11 straipsnyje nustatytus reikalavimus, ir juos įtraukia į Kibernetinio saugumo subjektų registrą.

4. Subjektai, kurie iki šio įstatymo įsigaliojimo buvo įtraukti į Vyriausybės patvirtintą ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą, iki 2025 m. balandžio 17 d. privalo toliau užtikrinti jų valdomų tinklų ir informacinių sistemų atitiktį iki šio įstatymo įsigaliojimo galiojusiems Lietuvos Respublikos kibernetinio saugumo įstatymo 11 straipsnio 1 dalies 1 punkte nurodytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams.

5. Subjektai, kurie iki šio įstatymo įsigaliojimo buvo įtraukti į Vyriausybės patvirtintą ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą, įtraukti į Kibernetinio saugumo subjektų registrą, privalo toliau užtikrinti jų valdomų tinklų ir informacinių sistemų atitiktį iki šio įstatymo įsigaliojimo galiojusiems Kibernetinio saugumo įstatymo 11 straipsnio 1 dalies 1 punkte nurodytiems kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams, tol, kol atsiras pareiga užtikrinti jų valdomų tinklų ir informacinių sistemų atitiktį šiuo įstatymu nauja redakcija išdėstyto Lietuvos Respublikos kibernetinio saugumo įstatymo 14 straipsnio 1 dalyje nurodytoms kibernetinio saugumo rizikos valdymo priemonėms.

6. Saugos įgaliotiniams, kuriems iki šio įstatymo įsigaliojimo buvo taikomos Kibernetinio saugumo įstatymo 22 straipsnio nuostatos dėl saugos įgaliotinio skyrimo ir atitikimo reikalavimams, toliau savo pareigas vykdo šiuo įstatymu nauja redakcija išdėstyto Lietuvos Respublikos kibernetinio saugumo įstatymo 15 straipsnio nustatyta tvarka. Šioje dalyje nurodytiems saugos įgaliotiniams šiuo įstatymu nauja redakcija išdėstyto Lietuvos Respublikos kibernetinio saugumo įstatymo 15 straipsnio 5 dalies 3 punkto reikalavimai netaikomi pirmus 2 metus nuo šio įstatymo įsigaliojimo.

7. Nacionalinis kibernetinio saugumo centas šio straipsnio 4 ir 5 dalyje nurodytais atvejais atlieka ryšių ir informacinių sistemų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams, priežiūrą ir turi iki šio įstatymo įsigaliojimo galiojusiuose Kibernetinio saugumo įstatymo 8 straipsnio 2 dalies 1, 2, 4 ir 5 punktuose nurodytus įgaliojimus.

8. Nacionalinis kibernetinio saugumo centras šio straipsnio 4 ir 5 dalyje nurodytais atvejais nustatęs iki šio įstatymo įsigaliojimo galiojusiame Kibernetinio saugumo įstatymo 11 straipsnio 1 dalies 1 punkte nurodytų organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, pažeidimų, taiko iki šio įstatymo įsigaliojimo galiojusias Lietuvos Respublikos administracinių nusižengimų kodekso 480 straipsnio 4 ir 5 dalies nuostatas.

9. Vadovaujantis iki šio įstatymo įsigaliojimo galiojusio Kibernetinio saugumo įstatymu pradėtos procedūros, tęsiamos ir baigiamos vadovaujantis iki šio įstatymo įsigaliojimo galiojusiomis Kibernetinio saugumo įstatymo ir jį įgyvendinančių teisės aktų nuostatomis.

10. Kituose teisės aktuose vartojama sąvoka „ryšių ir informacinė sistema“ atitinka šiame įstatyme vartojamą sąvoką „tinklų ir informacinė sistema“.

3 straipsnis. Įstatyme nustatyto galiojančio teisinio reguliavimo *ex post* vertinimas

1. Krašto apsaugos ministerija atlieka šiame įstatyme nustatyto galiojančio teisinio reguliavimo, susijusio su kibernetiniu saugumu, poveikio *ex post* vertinimą (toliau – *ex post* vertinimas).

2. Atliekant *ex post* vertinimą, turi būti nustatyta, kokį poveikį šiame įstatyme nustatytos priemonės, susijusios su kibernetiniu saugumu, turėjo kibernetinio saugumo subjektams.

3. *Ex post* vertinimo laikotarpis – 3 metai nuo šio įstatymo įsigaliojimo dienos.

4. *Ex post* vertinimas turi būti atliktas iki 2029 m. sausio 1 d.

Skelbiu šį Lietuvos Respublikos Seimo priimtą įstatymą.

Respublikos Prezidentas