LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMAS

2014 m. gruodžio 11 d. Nr. XII-1428
Vilnius

I SKYRIUS
BENDROSIOS NUOSTATOS

1 straipsnis. Įstatymo paskirtis ir taikymas

1. Šis įstatymas nustato kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, apibrėžia kibernetinio saugumo politiką formuojančias ir įgyvendinančias institucijas, jų kompetenciją, funkcijas, teises ir pareigas, valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų pareigas bei atsakomybę ir kibernetinio saugumo užtikrinimo priemones.

2. Šis įstatymas jame nustatytomis sąlygomis ir tvarka taikomas valstybės institucijoms, formuojančioms ir įgyvendinančioms kibernetinio saugumo politiką, viešojo administravimo subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams ir elektroninės informacijos prieglobos paslaugų teikėjams, informacinių technologijų srityje veiklą vykdantiems verslo subjektams, mokslo ir studijų institucijoms (toliau – kibernetinio saugumo dalyviai).

3. Šis įstatymas taikomas tiek, kiek šiame įstatyme reglamentuojamų visuomeninių santykių nereglamentuoja Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, Lietuvos Respublikos elektroninių ryšių įstatymas, Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas ir Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas.

2 straipsnis. Pagrindinės šio įstatymo sąvokos

1. **Elektroninės informacijos prieglobos paslaugos** – informacinės visuomenės paslaugos, apimančios galimybės naudotis elektroninės informacijos ir elektroninių duomenų (toliau – elektroninė informacija) kūrimo ir tvarkymo priemonėmis sudarymą ir (arba) paslaugų gavėjo pateiktos elektroninės informacijos saugojimą.

2. **Ypatingos svarbos informacinė infrastruktūra** – elektroninių ryšių tinklas ar jo dalis, informacinė sistema ar jos dalis, informacinių sistemų grupė ar pramoninių procesų valdymo sistema ar jos dalis, nepaisant to, ar jos valdytojas yra privatus ar viešojo administravimo subjektas, kuriuose įvykęs kibernetinis incidentas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ir visuomenės interesams.

3. **Kibernetinė erdvė** – aplinka, kurioje pavieniuose kompiuteriuose ar kitoje informacinėje ir ryšių technologijų įrangoje sukuriama elektroninė informacija ir (arba) perduodama per elektroninių ryšių tinklu sujungtus kompiuterius ar kitą informacinių ir ryšių technologijų įrangą.

4. **Kibernetinis incidentas** – įvykis ar veika, kuri sukelia ar gali sukelti neteisėtą prisijungimą ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos, sutrikdyti ar pakeisti, įskaitant valdymo perėmimą, informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, taip pat sudaryti sąlygas pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims.

5. **Kibernetinis saugumas** – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti.

6. **Pramoninių procesų valdymo sistema** – iš informacinėmis ir ryšių technologijomis grindžiamos įrangos sudaryta sistema, skirta technologiniams procesams stebėti ar valdyti pramonės, energetikos, transporto, vandens tiekimo paslaugų ir kituose ūkinės veiklos sektoriuose.

7. Kitos šiame įstatyme vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos elektroninių ryšių įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos informacinės visuomenės paslaugų įstatyme, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, Lietuvos Respublikos žvalgybos įstatyme, Lietuvos Respublikos kriminalinės žvalgybos įstatyme ir Lietuvos Respublikos viešojo administravimo įstatyme.

3 straipsnis. Kibernetinio saugumo principai

1. Kibernetinis saugumas grindžiamas bendraisiais teisės principais, elektroninių ryšių veiklos reguliavimo principais ir šiais kibernetinio saugumo principais:

1) kibernetinės erdvės nediskriminavimo – įstatymų ir kitų teisės aktų nuostatos ir saugomi gėriai vienodai taikomi tiek fizinėje, tiek kibernetinėje erdvėje;

2) kibernetinio saugumo proporcingumo – taikomos kibernetinio saugumo užtikrinimo priemonės negali būti griežtesnės, negu būtina kibernetiniam saugumui užtikrinti, o taikomi teisiniai, organizaciniai ir techniniai kibernetinio saugumo reikalavimai neturi apriboti kibernetinio saugumo dalyvių veiklos kibernetinėje erdvėje labiau, negu tai būtina;

3) viešojo intereso viršenybės – naudojamos kibernetinio saugumo užtikrinimo priemonės pirmiausia turi užtikrinti visuomenės viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų teisių ar neproporcingai apriboti jų laisvės kibernetinėje erdvėje.

2. Taikant kibernetinį saugumą reglamentuojančias teisės normas, turi būti tinkamai 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 politikos strateginius tikslus ir jiems pasiekti būtinas priemones nustato Lietuvos Respublikos Vyriausybė (toliau – Vyriausybė).

2. Kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija (toliau – Krašto apsaugos ministerija). Lietuvos Respublikos vidaus reikalų ministerija (toliau – Vidaus reikalų ministerija), Nacionalinis kibernetinio saugumo centras, Lietuvos Respublikos ryšių reguliavimo tarnyba (toliau – Ryšių reguliavimo tarnyba), Valstybinė duomenų apsaugos inspekcija ir Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Policijos departamentas) formuojant kibernetinio saugumo politiką dalyvauja tiek, kiek šiame įstatyme nustatytoms funkcijoms atlikti reikia nustatyti viešojo administravimo subjektų, valdančių valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų veiklos teisinį reguliavimą.

3. Kibernetinio saugumo politiką pagal kompetenciją įgyvendina Vidaus reikalų ministerija, Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija ir Policijos departamentas.

5 straipsnis. Vyriausybės įgaliojimai kibernetinio saugumo srityje

Vyriausybė:

1) sudaro Kibernetinio saugumo tarybą ir tvirtina jos reglamentą, tarybos narių skaičių ir paveda krašto apsaugos ministrui nustatyti tarybos personalinę sudėtį;

2) tvirtina Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką ir ypatingos svarbos informacinę infrastruktūrą ir (arba) šios infrastruktūros valdytojų sąrašą;

3) tvirtina organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus ypatingos svarbos informacinei infrastruktūrai, organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus valstybės informaciniams ištekliams;

4) tvirtina Nacionalinį kibernetinių incidentų valdymo planą;

5) tvirtina tipinius kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus;

6) atlieka kitas Lietuvos Respublikos teisės aktuose nustatytas funkcijas kibernetinio saugumo užtikrinimo srityje.

6 straipsnis. Krašto apsaugos ministerijos įgaliojimai kibernetinio saugumo srityje

Krašto apsaugos ministerija, formuodama kibernetinio saugumo politiką ir organizuodama, kontroliuodama ir koordinuodama jos įgyvendinimą:

1) rengia ir teikia Vyriausybei tvirtinti organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus ypatingos svarbos informacinei infrastruktūrai, ir organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus valstybės informaciniams ištekliams;

2) rengia ir teikia Vyriausybei tvirtinti Nacionalinį kibernetinių incidentų valdymo planą;

3) teikia Vyriausybei tvirtinti tipinius kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus;

4) tvirtina ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planus;

5) rengia ir tvirtina Kibernetinio saugumo informacinio tinklo nuostatus;

6) atlieka kitas Lietuvos Respublikos teisės aktuose nustatytas funkcijas kibernetinio saugumo užtikrinimo srityje.

7 straipsnis. Vidaus reikalų ministerijos įgaliojimai kibernetinio saugumo srityje

Vidaus reikalų ministerija:

1) rengia ir teikia Vyriausybei tvirtinti Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką ir ypatingos svarbos informacinę infrastruktūrą ir (arba) šios infrastruktūros valdytojų sąrašą;

2) atlieka kitas Lietuvos Respublikos teisės aktuose nustatytas funkcijas kibernetinio saugumo užtikrinimo srityje.

8 straipsnis. Ryšių reguliavimo tarnybos įgaliojimai kibernetinio saugumo srityje

1. Ryšių reguliavimo tarnyba, įgyvendindama kibernetinio saugumo politiką, reguliuoja viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų veiklą kibernetinio saugumo užtikrinimo srityje ir pagal kompetenciją:

1) rengia ir tvirtina informacijos apie kibernetinius incidentus ir taikytas šių incidentų valdymo priemones teikimo Ryšių reguliavimo tarnybai tvarkos ir sąlygų aprašą;

2) rengia ir tvirtina organizacinius ir techninius reikalavimus, taikomus elektroninės informacijos prieglobos paslaugų saugumui ir vientisumui užtikrinti;

3) rengia ir tvirtina techninės informacijos, reikalingos vertinti viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir (arba) elektroninės informacijos prieglobos paslaugų kibernetinio saugumo būseną, teikimo Ryšių reguliavimo tarnybai tvarkos ir sąlygų aprašą;

4) atlieka viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų interneto prieigos tinklų infrastruktūros vientisumo tyrimus;

5) atlieka viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir (arba) elektroninės informacijos prieglobos paslaugų kibernetinio saugumo būsenos tyrimus;

6) atlieka kitas Lietuvos Respublikos teisės aktuose nustatytas funkcijas kibernetinio saugumo užtikrinimo srityje.

2. Ryšių reguliavimo tarnyba, siekdama užtikrinti viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų saugumą ir vientisumą, užkirsti kelią kibernetiniams incidentams plisti, mažinti viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų, elektroninės informacijos prieglobos paslaugų teikėjų ir (arba) viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų gavėjų dėl kibernetinių incidentų patiriamos žalos atsiradimo riziką, turi teisę duoti privalomus nurodymus ir nustatyti nurodymų įvykdymo terminą viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams ir (arba) elektroninės informacijos prieglobos paslaugų teikėjams. Ryšių reguliavimo tarnybos nurodymai turi būti motyvuoti ir proporcingi tikslui pasiekti.

9 straipsnis. Kibernetinio saugumo taryba

1. Kibernetinio saugumo taryba yra nuolatinė kolegiali institucija, analizuojanti kibernetinio saugumo užtikrinimo būklę Lietuvos Respublikoje ir teikianti pasiūlymus kibernetinio saugumo dalyviams dėl šios būklės gerinimo. Kibernetinio saugumo taryba yra sudaroma iš kibernetinio saugumo politiką formuojančių ir įgyvendinančių valstybės institucijų, informacinių technologijų srityje veiklą vykdančių verslo subjektų atstovų, mokslo ir studijų

institucijų atstovų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų, elektroninės informacijos prieglobos paslaugų teikėjų atstovų, o prireikus ir iš kitų asmenų.

2. Kibernetinio saugumo tarybai vadovauja Krašto apsaugos ministerijos atstovas.

3. Kibernetinio saugumo tarybos darbo ūkinį ir techninį aptarnavimą vykdo Krašto apsaugos ministerija ar jos įgaliota institucija.

4. Kibernetinio saugumo taryba:

1) teikia pasiūlymus kibernetinio saugumo dalyviams dėl kibernetinio saugumo prioritetų, plėtros krypčių, siektinų rezultatų ir jų įgyvendinimo būdų;

2) teikia pasiūlymus kibernetinio saugumo dalyviams dėl platesnio viešojo sektoriaus, verslo ir mokslo bendradarbiavimo galimybių kibernetinio saugumo užtikrinimo srityje;

3) analizuoja kibernetinio saugumo užtikrinimo tobulinimo tendencijas, teikia kibernetinio saugumo dalyviams išvadas ir pasiūlymus dėl kibernetinių incidentų valdymo;

4) teikia kibernetinio saugumo dalyviams rekomendacijas dėl kibernetinio saugumo stiprinimo.

10 straipsnis. Nacionalinis kibernetinio saugumo centras

1. Nacionalinio kibernetinio saugumo centro funkcijas vykdo įstaiga prie Krašto apsaugos ministerijos.

2. Nacionalinis kibernetinio saugumo centras, pagal kompetenciją įgyvendindamas kibernetinio saugumo politiką ir vykdydamas valstybės informacinių išteklių ir ypatingos svarbos informacinių infrastruktūrų kibernetinių incidentų valdymo padalinio veiklą:

1) pagal savo kompetenciją rengia ir teikia pasiūlymus krašto apsaugos ministrui dėl organizacinių ir techninių kibernetinio saugumo reikalavimų valstybės informaciniams ištekliams ir ypatingos svarbos informacinei infrastruktūrai;

2) atlieka valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams stebėseną;

3) rengia tipinius kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus;

4) teikia konsultacijas ir rekomendacijas valstybės informacinių išteklių valdytojams ir ypatingos svarbos infrastruktūros valdytojams kibernetinio saugumo klausimais;

5) analizuoja nacionalinę kibernetinio saugumo situaciją ir rengia nacionalinio kibernetinio saugumo būklės ataskaitas;

6) ne rečiau kaip kartą per metus rengia ir teikia nacionalinio kibernetinio saugumo būklės ataskaitas krašto apsaugos ministrui;

7) rengia ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planus;

8) valdo kibernetinio saugumo informacinį tinklą;

9) vykdo informacijos sklaidą kibernetinio saugumo klausimais;

10) laikydamasis krašto apsaugos ministro nustatytos tvarkos, reaguoja į kibernetinius incidentus valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėse infrastruktūrose;

11) atlieka kitas Lietuvos Respublikos teisės aktuose nustatytas funkcijas kibernetinio saugumo užtikrinimo srityje.

3. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką, turi teisę:

1) pagal su valstybės informacinių išteklių valdytojais ar ypatingos svarbos informacinės infrastruktūros valdytojais suderintą diegimo planą, laikydamasis krašto apsaugos ministro nustatytos tvarkos, savo lėšomis diegti ir valdyti technines kibernetinio saugumo priemones valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėse infrastruktūrose. Nacionalinio kibernetinio saugumo centro lėšomis įdiegtos priemonės naudojamos išimtinai tik kibernetiniam saugumui užtikrinti. Nacionalinio kibernetinio saugumo centro lėšomis įdiegtos techninės kibernetinio saugumo priemonės techniškai aptarnaujamos, jų remontas atliekamas Nacionalinio kibernetinio saugumo centro lėšomis. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojai savo lėšomis ir ištekliais privalo sudaryti kibernetinio saugumo priemonių funkcionavimui būtinas technines sąlygas ir parengti valdomus valstybės informacinius išteklius ar ypatingos svarbos informacinę infrastruktūrą Nacionalinio kibernetinio saugumo centro techninių kibernetinio saugumo priemonių diegimui ir valdymui bei užtikrinti nenutrūkstamą šių priemonių veikimą;

2) susipažinti su valstybės informacinių išteklių audito išvadomis ir ypatingos svarbos informacinių infrastruktūrų informacinių technologijų audito išvadomis, rizikos analizėmis ir gauti papildomą informaciją apie kibernetinio saugumo būklę;

3) taikyti technines priemones, siekdamas įvertinti valstybės informacinių išteklių ir ypatingos svarbos informacinių infrastruktūrų atsparumą kibernetiniams incidentams;

4) kibernetinio incidento metu duoti motyvuotus privalomus nurodymus, susijusius su kibernetinio saugumo užtikrinimu, viešojo administravimo subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ir ypatingos svarbos informacinės infrastruktūros valdytojams;

5) kibernetinio incidento metu taikyti būtinas kibernetinio saugumo užtikrinimo priemones;

6) siekdamas stabdyti kibernetinio incidento poveikį valstybės informacinių išteklių ar ypatingos svarbos informacinių infrastruktūrų kibernetiniam saugumui, be teismo sankcijos duoti motyvuotą nurodymą viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams laikinai, bet ne ilgiau negu 48 valandoms apriboti viešųjų elektroninių ryšių paslaugų teikimą šių paslaugų gavėjui; Nacionalinis kibernetinio saugumo centras apie viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams pagal šį punktą duotus nurodymus ne vėliau kaip kitą darbo dieną informuoja Ryšių reguliavimo tarnybą;

7) pasitelkti į pagalbą informacinių technologijų ir kibernetinio saugumo specialistus;

8) tvarkyti asmens duomenis, būtinus šio įstatymo ir kitų teisės aktų numatytoms funkcijoms kibernetinio saugumo užtikrinimo srityje atlikti;

9) kartu su verslo subjektais, mokslo ir studijų institucijomis ir kitais kibernetinio saugumo dalyviais plėtoti bendrus kibernetinio saugumo projektus.

4. Nacionalinio kibernetinio saugumo centro, įgyvendinančio kibernetinio saugumo politiką, pareigos:

1) skelbti visuomenei kibernetinio saugumo užtikrinimo metodinę informaciją, rekomendacijas ir kitą su kibernetinio saugumo užtikrinimu susijusią neįslaptintą informaciją;

2) kibernetinio incidento metu kartu su valstybės informacinių išteklių valdytoju ir ypatingos svarbos informacinės infrastruktūros valdytoju užtikrinti valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros kibernetinį saugumą.

11 straipsnis. Valstybinės duomenų apsaugos inspekcijos įgaliojimai kibernetinio saugumo srityje

Valstybinė duomenų apsaugos inspekcija įgyvendina kibernetinio saugumo politiką asmens duomenų apsaugos srityje ir pagal kompetenciją:

1) teisės aktų nustatyta tvarka atlieka juridinių asmenų patikrinimus, kai yra rizikos, kad kibernetiniai incidentai gali turėti įtakos asmens duomenų apsaugai;

2) teikia visuomenei ir suinteresuotoms institucijoms informaciją apie kibernetinio saugumo, susijusio su asmens duomenų apsauga, rizikos veiksnius, pavojus ir grėsmes kibernetinėje erdvėje;

3) nustato viešojo administravimo subjektams, valdantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams, elektroninės informacijos prieglobos

paslaugų teikėjams informacijos apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones pateikimo tvarką;

4) renka, analizuoja ir vertina informaciją apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones;

5) tikrina asmens duomenų tvarkymo teisėtumą ir priima sprendimus dėl asmens duomenų tvarkymo pažeidimų kibernetinėje erdvėje;

6) atlieka kitas Lietuvos Respublikos teisės aktuose nustatytas funkcijas kibernetinio saugumo užtikrinimo srityje.

12 straipsnis. Policijos įgaliojimai kibernetinio saugumo srityje

Policija teisės aktų nustatyta tvarka vykdydama kibernetinių incidentų, galimai turinčių nusikalstamos veikos požymių, užkardymą ir tyrimą:

1) renka, analizuoja ir apibendrina informaciją apie kibernetinius incidentus, galimai turinčius nusikalstamos veikos požymių;

2) nustato viešojo administravimo subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams, elektroninės informacijos prieglobos paslaugų teikėjams informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veikos požymių, užkardyti ir tirti, pateikimo tvarką;

3) turi teisę duoti motyvuotus nurodymus ne ilgiau kaip 48 valandoms be teismo sankcijos, ilgesniam laikui – su apylinkės teismo sankcija, apriboti viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų teikimą paslaugų gavėjui, kai paslaugų gavėjas ar jo naudojama informacinė ir ryšių technologijų įranga galimai dalyvauja nusikalstamoje veikoje, ir (arba) nurodyti viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjui ar elektroninės informacijos prieglobos paslaugų teikėjui taikyti priemones, šalinančias nusikalstamų veikų kibernetinėje erdvėje priežastis. Tokiais atvejais apylinkės teismo pirmininkui ar jo įgaliotam teisėjui pateikiamas teikimas dėl veiksmų teisėtumo ar pagrįstumo patvirtinimo motyvuota nutartimi. Jeigu terminas baigiasi poilsio ar švenčių dieną, teikimas pateikiamas ne vėliau kaip kitą darbo dieną po poilsio ar švenčių dienos. Jeigu teisėjas nepatvirtina nurodytų veiksmų teisėtumo ar pagrįstumo motyvuota nutartimi, nurodymas nedelsiant stabdomas;

4) turi teisę duoti motyvuotus nurodymus viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų teikėjui išsaugoti informaciją, susijusią su jų teikiamomis paslaugomis, iš kurios galima nustatyti naudotos ryšio

paslaugos tipą, taikytas technines priemones ir naudojimo laiką, abonento tapatybę, pašto, geografinės padėties adresą, telefono ir bet kokį kitą prieigos 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, taip pat teisės aktų nustatyta tvarka, kai yra motyvuota teismo nutartis, gauti paslaugų naudotojo srauto duomenis ir kontroliuoti perduodamos informacijos turinį.

III SKYRIUS
KIBERNETINIO SAUGUMO DALYVIŲ PAREIGOS

13 straipsnis. Viešojo administravimo subjektų pareigos

1. Viešojo administravimo subjektai atsako už jų valdomų ir (arba) tvarkomų valstybės informacinių išteklių kibernetinį saugumą ir privalo savo lėšomis užtikrinti jų valdomų ir (arba) tvarkomų valstybės informacinių išteklių atitiktį Vyriausybės nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams.

2. Viešojo administravimo subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, privalo informuoti Nacionalinį kibernetinio saugumo centrą apie jų valdomuose ir (arba) tvarkomuose valstybės informaciniuose ištekliuose įvykusius kibernetinius incidentus, apibrėžtus organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose, ir taikytas kibernetinių incidentų valdymo priemones Vyriausybės ar jos įgaliotos institucijos nustatyta tvarka.

3. Viešojo administravimo subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, privalo teikti Valstybinei duomenų apsaugos inspekcijai informaciją apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones šios institucijos nustatyta tvarka ir sąlygomis.

4. Viešojo administravimo subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, privalo teikti policijai informaciją, reikalingą kibernetiniams incidentams, turintiems nusikalstamos veikos požymių, užkardyti ir tirti, policijos generalinio komisaro nustatyta tvarka ir sąlygomis.

5. Viešojo administravimo subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, turi paskirti kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, ir Nacionaliniam kibernetinio saugumo centrui pateikti paskirto asmens ar padalinio kontaktinę informaciją.

6. Viešojo administravimo subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, turi sudaryti sąlygas Nacionaliniam kibernetinio saugumo centrui diegti ir valdyti technines kibernetinio saugumo priemones valstybės informaciniuose ištekliuose.

14 straipsnis. Ypatingos svarbos informacinės infrastruktūros valdytojų pareigos

1. Ypatingos svarbos informacinės infrastruktūros valdytojai atsako už jų valdomos ypatingos svarbos informacinės infrastruktūros kibernetinį saugumą ir privalo savo lėšomis užtikrinti jų valdomos ypatingos svarbos informacinės infrastruktūros atitiktį Vyriausybės nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams.

2. Ypatingos svarbos informacinės infrastruktūros valdytojai privalo informuoti Nacionalinį kibernetinio saugumo centrą apie ypatingos svarbos informacinėje infrastruktūroje įvykusius kibernetinius incidentus, apibrėžtus organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose, ir taikytas kibernetinių incidentų valdymo priemones Vyriausybės ar jos įgaliotos institucijos nustatyta tvarka.

3. Ypatingos svarbos informacinės infrastruktūros valdytojai privalo teikti Valstybinei duomenų apsaugos inspekcijai informaciją apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones šios institucijos nustatyta tvarka ir sąlygomis.

4. Ypatingos svarbos informacinės infrastruktūros valdytojai privalo teikti policijai informaciją, reikalingą kibernetiniams incidentams, turintiems nusikalstamos veikos požymių, užkardyti ir tirti, policijos generalinio komisaro nustatyta tvarka ir sąlygomis.

5. Ypatingos svarbos informacinės infrastruktūros valdytojai privalo, vadovaudamiesi Vyriausybės patvirtintais tipiniais kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planais, parengti, patvirtinti ir Nacionaliniam kibernetinio saugumo centrui pateikti kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus.

6. Ypatingos svarbos informacinės infrastruktūros valdytojai privalo išbandyti kibernetinių incidentų valdymo planų veikimą, o bandymų rezultatus pateikti Nacionaliniam kibernetinio saugumo centrui.

7. Ypatingos svarbos informacinės infrastruktūros valdytojai turi paskirti kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, ir Nacionaliniam kibernetinio saugumo centrui pateikti paskirto asmens ar padalinio kontaktinę informaciją.

8. Ypatingos svarbos informacinės infrastruktūros valdytojai turi sudaryti sąlygas Nacionaliniam kibernetinio saugumo centrui diegti ir valdyti technines kibernetinio saugumo priemones ypatingos svarbos informacinėje infrastruktūroje.

15 straipsnis. Viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų pareigos

Viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai privalo:

1) viešai skelbti paslaugų gavėjams rekomendacijas apie priemones kibernetiniam saugumui užtikrinti naudojantis viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų teikiamomis paslaugomis;

2) teikti Ryšių reguliavimo tarnybai informaciją apie įvykusius kibernetinius incidentus, apibrėžtus Ryšių reguliavimo tarnybos patvirtintose viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų saugumo ir vientisumo užtikrinimo taisyklėse, ir taikytas šių incidentų valdymo priemones bei techninę informaciją, reikalingą vertinti viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų kibernetinio saugumo būseną, šios institucijos nustatyta tvarka ir sąlygomis;

3) teikti Valstybinei duomenų apsaugos inspekcijai informaciją apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones šios institucijos nustatyta tvarka ir sąlygomis;

4) policijos generalinio komisaro nustatyta tvarka ir sąlygomis teikti policijai informaciją, reikalingą teisės pažeidimams, galimai turintiems nusikalstamos veikos požymių, kibernetinėje erdvėje užkardyti ir tirti, ir vykdyti kitus policijos nurodymus, duotus šio įstatymo ar kitų teisės aktų nustatytais pagrindais. Policijos nurodymus dėl paslaugų teikimo jų gavėjui apribojimo privaloma įvykdyti ne vėliau kaip per 8 valandas nuo policijos nurodymo gavimo;

5) paskirti kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, ir Ryšių reguliavimo tarnybai pateikti paskirto asmens ar padalinio kontaktinę informaciją.

16 straipsnis. Elektroninės informacijos prieglobos paslaugų teikėjų pareigos

Elektroninės informacijos prieglobos paslaugų teikėjai privalo:

1) įgyvendinti kibernetinio saugumo užtikrinimo technines ir organizacines priemones, nustatytas Ryšių reguliavimo tarnybos, kiek tai susiję su jų teikiamomis paslaugomis, prireikus kartu su viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjais imtis reikiamų priemonių kibernetiniam saugumui užtikrinti;

2) viešai skelbti elektroninės informacijos prieglobos paslaugų gavėjams rekomendacijas apie priemones kibernetiniam saugumui užtikrinti naudojantis elektroninės informacijos prieglobos paslaugomis;

3) teikti Ryšių reguliavimo tarnybai informaciją apie kibernetinius incidentus, apibrėžtus organizaciniuose ir techniniuose reikalavimuose elektroninės informacijos prieglobos paslaugų

saugumui ir vientisumui užtikrinti, ir taikytas šių incidentų valdymo priemones bei techninę informaciją, reikalingą vertinti elektroninės informacijos prieglobos paslaugų kibernetinio saugumo būseną, šios institucijos nustatyta tvarka ir sąlygomis;

4) policijos generalinio komisaro nustatyta tvarka ir sąlygomis teikti policijai informaciją, reikalingą teisės pažeidimams, galimai turintiems nusikalstamos veikos požymių, kibernetinėje erdvėje užkardyti ir tirti, ir vykdyti kitus policijos nurodymus, duotus šio įstatymo ar kitų teisės aktų nustatytais pagrindais. Policijos nurodymus dėl paslaugų teikimo jų gavėjui apribojimo privaloma įvykdyti ne vėliau kaip per 8 valandas nuo policijos nurodymo gavimo;

5) paskirti kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, ir Ryšių reguliavimo tarnybai pateikti paskirto asmens ar padalinio kontaktinę informaciją.

IV SKYRIUS
TARPINSTITUCINIS BENDRADARBIAVIMAS, INFORMACIJOS PASIKEITIMO TVARKA IR ATSAKOMYBĖ UŽ KIBERNETINIO SAUGUMO REIKALAVIMŲ PAŽEIDIMUS

17 straipsnis. Kibernetinio saugumo informacinis tinklas

1. Kibernetinio saugumo informacinis tinklas, kurio valdytojas – Nacionalinis kibernetinio saugumo centras, yra saugi informacijos mainų platforma, kurios paskirtis yra dalytis informacija apie galimus ir įvykusius kibernetinius incidentus, taip pat rekomendacijomis, nurodymais, techniniais sprendimais ir kitomis priemonėmis, užtikrinančiomis kibernetinį saugumą ir bendradarbiavimą tarp kibernetinio saugumo informacinio tinklo narių kibernetinio saugumo srityje.

2. Kibernetinio saugumo informaciniu tinklu gali naudotis tik tie subjektai, kurie atitinka Kibernetinio saugumo informacinio tinklo nuostatuose nurodytus reikalavimus.

3. Kibernetinio saugumo informaciniame tinkle skelbiama aktuali viešojo administravimo subjektų, valdančių ir (arba) tvarkančių valstybės informacinius išteklius, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų, elektroninės informacijos prieglobos paslaugų teikėjų ir ypatingos svarbos informacinės infrastruktūros valdytojų paskirtų asmenų ar padalinių, atsakingų už kibernetinio saugumo organizavimą ir kibernetinių incidentų valdymą, kontaktinė informacija.

18 straipsnis. Tarpinstitucinis bendradarbiavimas tiriant kibernetinius incidentus

1. Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, Policijos departamentas ir kitos policijos įstaigos bendradarbiauja tiriant kibernetinius incidentus, keičiasi

su kibernetinių incidentų tyrimais susijusia informacija, reikalinga institucijų pagal kompetenciją vykdomoms funkcijoms atlikti. Prireikus apie kibernetinių incidentų tyrimą gali būti informuojami kiti kriminalinės žvalgybos subjektai ir (arba) žvalgybos institucijos.

2. Valstybinė duomenų apsaugos inspekcija bendradarbiauja su Nacionalinio kibernetinio saugumo centru ir Ryšių reguliavimo tarnyba tiriant kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, keičiasi informacija, reikalinga teisės aktų nustatytoms funkcijoms, susijusioms su kibernetinių incidentų, pažeidžiančių asmens duomenų saugumą, tyrimu, atlikti.

3. Tarpinstitucinio bendradarbiavimo tiriant kibernetinius incidentus tvarka ir kibernetinių incidentų klasifikavimo tvarka nustatomos Nacionaliniame kibernetinių incidentų valdymo plane.

19 straipsnis. Atsakomybė už šio įstatymo ir jo įgyvendinamųjų teisės aktų pažeidimus

Už šio įstatymo ar jo įgyvendinamųjų teisės aktų nustatytų reikalavimų pažeidimus viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų, elektroninės informacijos prieglobos paslaugų teikėjų ir ypatingos svarbos informacinės infrastruktūros valdytojų administracijos vadovai atsako Lietuvos Respublikos administracinių teisės pažeidimų kodekso nustatyta tvarka.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

20 straipsnis. Įstatymo įsigaliojimas ir įgyvendinimas

1. Šis įstatymas, išskyrus šio straipsnio 2 dalį, įsigalioja 2015 m. sausio 1 d.

2. Vyriausybė, krašto apsaugos ministras, vidaus reikalų ministras, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija, Policijos departamentas iki 2014 m. gruodžio 31 d. priima šio įstatymo įgyvendinamuosius teisės aktus.

Skelbiu šį Lietuvos Respublikos Seimo priimtą įstatymą.

Respublikos Prezidentė Dalia Grybauskaitė