LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMO NR. XII-1428 1, 2, 5, 6, 8, 12 STRAIPSNIŲ PAKEITIMO IR ĮSTATYMO PAPILDYMO VII SKYRIUMI ĮSTATYMAS

2023 m. gruodžio 21 d. Nr. XIV-2438
Vilnius

1 straipsnis. 1 straipsnio pakeitimas

Pakeisti 1 straipsnio 1 dalį ir ją išdėstyti taip:

„1. Šis įstatymas nustato kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijas, šių institucijų įgaliojimus kibernetinio saugumo srityje, kibernetinio saugumo subjektų pareigas, tarpinstitucinį bendradarbiavimą, ryšių ir informacinių sistemų spragų paieškos ir pranešimo apie jas ir kibernetinius incidentus pagrindus, nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas ir įgaliojimus, taip pat valstybės informacinių išteklių saugos reikalavimus.“

2 straipsnis. 2 straipsnio pakeitimas

Papildyti 2 straipsnį 15^1 dalimi:

„15^1. **Saugusis valstybinis duomenų perdavimo tinklas** (toliau – Saugusis tinklas) – valstybės valdomas specialiuosius organizacinius ir techninius reikalavimus atitinkantis ir nuo viešųjų elektroninių ryšių tinklų nepriklausomas elektroninių ryšių tinklas.“

3 straipsnis. 5 straipsnio pakeitimas

1. Papildyti 5 straipsnį nauju 6 punktu:

„6) tvirtina bendrųjų elektroninės informacijos saugos reikalavimų aprašą, saugos dokumentų turinio gairių aprašą Valstybės informacinių išteklių valdymo įstatyme nurodytiems registrų informacinių sistemų, valstybės ir vidaus administravimo informacinių sistemų valdytojams ir tvarkytojams (toliau kartu – subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius);“.

2. Buvusį 5 straipsnio 6 punktą laikyti 7 punktu.

4 straipsnis. 6 straipsnio pakeitimas

1. Papildyti 6 straipsnį 5^1 punktu:

„5^1) teikia Vyriausybei tvirtinti bendrųjų elektroninės informacijos saugos reikalavimų aprašą, saugos dokumentų turinio gairių aprašą subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius;“.

2. Papildyti 6 straipsnį 11^1 punktu:

„11^1) valdo Saugųjį tinklą;“.

5 straipsnis. 8 straipsnio pakeitimas

1. Pakeisti 8 straipsnio 2 dalies nuostatą iki dvitaškio ir ją išdėstyti taip:

„2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką ir užtikrindamas valstybės informacinių išteklių saugą, pagal kompetenciją:“.

2. Papildyti 8 straipsnio 2 dalį 16^2, 16^3, 16^4 ir 16^5 punktais:

„16^2) atlieka valstybės informacinių išteklių atitikties teisės aktų nustatytiems elektroninės informacijos saugos reikalavimams stebėseną;

16^3) derina su valstybės informacinių išteklių sauga susijusių teisės aktų ir saugos dokumentų projektus;

16^4) konsultuoja subjektus, valdančius ir (arba) tvarkančius valstybės informacinius išteklius, valstybės informacinių išteklių saugos klausimais;

16^5) organizuoja valstybės informacinių išteklių saugos vertinimą;“.

6 straipsnis. 12 straipsnio pakeitimas

Pakeisti 12 straipsnio 2 dalį ir ją išdėstyti taip:

„2. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius:

1) sudaro sąlygas Nacionaliniam kibernetinio saugumo centrui diegti ir valdyti technines kibernetinio saugumo priemones valstybės informaciniuose ištekliuose ir taikyti technines priemones, siekdami įvertinti valstybės informacinių išteklių atsparumą kibernetiniams incidentams;

2) planuoja atitinkamiems Vyriausybės ir (arba) jos įgaliotos institucijos nustatytiems valstybės informacinių išteklių saugos reikalavimams įgyvendinti reikalingas lėšas ir jas skiria kibernetiniam saugumui ir valstybės informacinių išteklių saugai užtikrinti, taip pat imasi veiksmų, kad suplanuotos lėšos būtų skiriamos, ir kontroliuoja, kaip skirtos lėšos panaudojamos.“

7 straipsnis. Įstatymo papildymas VII skyriumi

Papildyti Įstatymą VII skyriumi:

„VII SKYRIUS
VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ SAUGA

21 straipsnis. Valstybės informacinių išteklių saugos užtikrinimas

1. Tvarkant valstybės informacinius išteklius, Valstybės informacinių išteklių valdymo įstatyme nurodytiems registrų informacinių sistemų, valstybės ir vidaus administravimo informacinių sistemų (toliau kartu – informacinės sistemos) tvarkytojams privaloma įgyvendinti saugos priemones, skirtas informacinėse sistemose tvarkomos elektroninės informacijos tikslumui užtikrinti ir jai nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, sugadinimo, atskleidimo, neteisėto pasisavinimo, paskelbimo, pateikimo ar kitokio panaudojimo, taip pat nuo bet kokio kito neteisėto tvarkymo apsaugoti.

2. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, siekdami užtikrinti valstybės informacinių išteklių saugą, vadovaudamiesi Vyriausybės tvirtinamu bendrųjų elektroninės informacijos saugos reikalavimų aprašu, rengia, derina ir tvirtina informacinės sistemos saugos dokumentus. Informacinės sistemos valdytojas gali tvirtinti visų jo valdymo sričiai priskirtų informacinių sistemų bendrus saugos dokumentus. Organizuojant valstybės informacinių išteklių saugą, rekomenduojama vadovautis pripažintų standartizacijos organizacijų ir standartizacijos institucijų priimtais ir paskelbtais standartais.

3. Už informacinėje sistemoje tvarkomų duomenų saugą pagal kompetenciją atsako subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius. Subjektai, tvarkantys valstybės informacinius išteklius, privalo saugos nuostatuose ir kituose saugos dokumentuose nustatyta tvarka užtikrinti reikiamas technines ir organizacines saugos priemones ir tokių priemonių laikymąsi.

4. Valstybės tarnautojai arba darbuotojai, dirbantys pagal darbo sutartis ir gaunantys darbo užmokestį iš valstybės ir savivaldybių biudžetų ir valstybės pinigų fondų, tvarkantys duomenis informacinėje sistemoje, privalo įsipareigoti saugoti elektroninės informacijos paslaptį, kurią sudaro bet kokia skaitmeninės išraiškos informacija, dokumentai ir (ar) jų kopijos, įskaitant garso, vaizdo arba garso ir vaizdo įrašus, taip pat asmens duomenys, kurie saugomi, perduodami, interpretuojami ir apdorojami informacinių technologijų priemonėmis. Įsipareigojimas saugoti paslaptį galioja ir tada, kai su elektroninės informacijos tvarkymu susijusi veikla nutraukiama perėjus dirbti į kitas pareigas, pasibaigus darbo ar sutartiniams santykiams.

5. Fizinių asmenų asmens duomenų saugumas užtikrinamas vadovaujantis Reglamentu (ES) 2016/679 ir (ar) Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymu.

6. Informacija apie saugos priemones, nurodytas šio straipsnio 1 dalyje, ir valstybės informacinių išteklių pažeidžiamumą nėra viešai skelbiama. Informacija teikiama tik jeigu teisė gauti šią informaciją yra nustatyta įstatymuose ar jų pagrindu priimtuose kituose norminiuose teisės aktuose.

22 straipsnis. Saugos įgaliotinis

1. Saugos įgaliotinis atsako už saugos reikalavimų vykdymą ir atlieka informacinės sistemos saugos nuostatuose ir kituose valstybės informacinių išteklių saugą reglamentuojančiuose teisės aktuose nustatytas funkcijas.

2. Saugos įgaliotinis skiriamas teisės aktu, kuriuo tvirtinami informacinės sistemos saugos nuostatai, arba informacinės sistemos valdytojas paveda informacinės sistemos tvarkytojui paskirti saugos įgaliotinį. Gali būti skiriamas kelių informacinių sistemų saugos įgaliotinis.

3. Saugos įgaliotinis negali turėti neišnykusio ar nepanaikinto teistumo už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat negali turėti paskirtos administracinės nuobaudos už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo veikimui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo nuobaudos paskyrimo yra praėję mažiau kaip vieni metai.

23 straipsnis. Valstybės informacinių išteklių atitikties nustatytiems elektroninės informacijos saugos reikalavimams stebėsena

Subjektai, valdantys valstybės informacinius išteklius (išskyrus įslaptintos informacijos tvarkymą), valstybės informacinių išteklių atitikties saugos reikalavimams stebėsenos sistemoje šios sistemos nuostatuose nustatyta tvarka teikia duomenis apie organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, ir elektroninės informacijos saugos reikalavimų, taikomų valstybės informacinius išteklius valdantiems ir (arba) tvarkantiems subjektams, įgyvendinimą savo valdomuose valstybės informaciniuose ištekliuose.

24 straipsnis. Valstybės informacinių išteklių saugos vertinimas

1. Vertinant ypatingos svarbos ir svarbių valstybės informacinių išteklių saugą, o jeigu kartu yra tvarkomi vidutinės ir (ar) mažos svarbos valstybės informaciniai ištekliai, atliekant saugos auditą kartu įtraukiami ir šie ištekliai. Šių išteklių saugos auditas atliekamas ne rečiau kaip kartą per 3 metus.

2. Valstybės informacinių išteklių saugos auditą atlieka nepriklausomi visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai arba minėtų organizacijų sertifikatus turintys informacinių technologijų specialistai, kuriems negali būti pavedama vertinti savo valdomų ir (arba) tvarkomų valstybės informacinių išteklių saugos.

25 straipsnis. Saugusis tinklas

1. Valstybės ir savivaldybių institucijos ir įstaigos, valstybės valdomos įmonės ir viešosios įstaigos (toliau kartu – institucijos), įrašytos į Saugiojo tinklo 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 (arba) prie viešųjų elektroninių ryšių tinklų jungtis ne per Saugųjį tinklą yra būtina renkant ir (arba) 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 (arba) tvarkančioms valstybės informacinius išteklius, būtinus gyvybiškai svarbioms valstybės funkcijoms atlikti ir valstybinėms mobilizacinėms užduotims vykdyti, ir (arba) 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 (arba) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esančių institucijų ar duomenų centrų.

3. Saugųjį tinklą 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.

26 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) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esančiuose duomenų centruose, vadovaudamosi Valstybės informacinių išteklių valdymo įstatymo 45 straipsnio 1–4 ir 6 dalyse nustatyta tvarka. 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) Šiaurės Atlanto sutarties organizacijos (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) Šiaurės Atlanto sutarties organizacijos (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) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esantiems duomenų centrams, kuriuose laikomi valstybės informaciniai ištekliai, tvirtinami Valstybės informacinių išteklių įstatymo nustatyta tvarka.“

8 straipsnis. Įstatymo įsigaliojimas ir taikymas

1. Šis įstatymas įsigalioja 2024 m. sausio 1 d.

2. Iki šio įstatymo įsigaliojimo dienos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka paskirtiems saugos įgaliotiniams taikomos šio įstatymo 7 straipsnyje išdėstyto Lietuvos Respublikos kibernetinio saugumo įstatymo VII skyriaus „Valstybės informacinių išteklių sauga“ 22 straipsnio nuostatos.

3. Iki šio įstatymo įsigaliojimo dienos Valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka pradėtiems informacinių technologijų auditams taikomas iki šio įstatymo įsigaliojimo galiojęs teisinis reguliavimas. Laikotarpis valstybės informacinių išteklių saugos auditams atlikti pradedamas skaičiuoti nuo šio įstatymo įsigaliojimo dienos.

4. Iki šio įstatymo įsigaliojimo dienos Valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka į Saugiojo tinklo naudotojų sąrašą įtrauktoms institucijoms taikomos šio įstatymo 7 straipsnyje išdėstyto Kibernetinio saugumo įstatymo VII skyriaus „Valstybės informacinių išteklių sauga“ 25 ir 26 straipsnių nuostatos.

Skelbiu šį Lietuvos Respublikos Seimo priimtą įstatymą.

Respublikos Prezidentas Gitanas Nausėda

LIETUVOS RESPUBLIKOS
KIBERNETINIO SAUGUMO ĮSTATYMO NR. XII-1428 1, 2, 5, 6, 8, 12 STRAIPSNIŲ PAKEITIMO IR ĮSTATYMO PAPILDYMO VII SKYRIUMI
ĮSTATYMAS

2023 m. gruodžio 21 d. Nr. XIV-2438
Vilnius

1 straipsnis. 1 straipsnio pakeitimas

Pakeisti 1 straipsnio 1 dalį ir ją išdėstyti taip:

„1. Šis įstatymas nustato kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijas, šių institucijų įgaliojimus kibernetinio saugumo srityje, kibernetinio saugumo subjektų pareigas, tarpinstitucinį bendradarbiavimą, ryšių ir informacinių sistemų spragų paieškos ir pranešimo apie jas ir kibernetinius incidentus pagrindus, nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas ir įgaliojimus, taip pat valstybės informacinių išteklių saugos reikalavimus.“

2 straipsnis. 2 straipsnio pakeitimas

Papildyti 2 straipsnį 15^1 dalimi:

„15^1. **Saugusis valstybinis duomenų perdavimo tinklas** (toliau – Saugusis tinklas) – valstybės valdomas specialiuosius organizacinius ir techninius reikalavimus atitinkantis ir nuo viešųjų elektroninių ryšių tinklų nepriklausomas elektroninių ryšių tinklas.“

3 straipsnis. 5 straipsnio pakeitimas

1. Papildyti 5 straipsnį nauju 6 punktu:

„6) tvirtina bendrųjų elektroninės informacijos saugos reikalavimų aprašą, saugos dokumentų turinio gairių aprašą Valstybės informacinių išteklių valdymo įstatyme nurodytiems registrų informacinių sistemų, valstybės ir vidaus administravimo informacinių sistemų valdytojams ir tvarkytojams (toliau kartu – subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius);“.

2. Buvusį 5 straipsnio 6 punktą laikyti 7 punktu.

4 straipsnis. 6 straipsnio pakeitimas

1. Papildyti 6 straipsnį 5^1 punktu:

„5^1) teikia Vyriausybei tvirtinti bendrųjų elektroninės informacijos saugos reikalavimų aprašą, saugos dokumentų turinio gairių aprašą subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius;“.

2. Papildyti 6 straipsnį 11^1 punktu:

„11^1) valdo Saugųjį tinklą;“.

5 straipsnis. 8 straipsnio pakeitimas

1. Pakeisti 8 straipsnio 2 dalies nuostatą iki dvitaškio ir ją išdėstyti taip:

„2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką ir užtikrindamas valstybės informacinių išteklių saugą, pagal kompetenciją:“.

2. Papildyti 8 straipsnio 2 dalį 16^2, 16^3, 16^4 ir 16^5 punktais:

„16^2) atlieka valstybės informacinių išteklių atitikties teisės aktų nustatytiems elektroninės informacijos saugos reikalavimams stebėseną;

16^3) derina su valstybės informacinių išteklių sauga susijusių teisės aktų ir saugos dokumentų projektus;

16^4) konsultuoja subjektus, valdančius ir (arba) tvarkančius valstybės informacinius išteklius, valstybės informacinių išteklių saugos klausimais;

16^5) organizuoja valstybės informacinių išteklių saugos vertinimą;“.

6 straipsnis. 12 straipsnio pakeitimas

Pakeisti 12 straipsnio 2 dalį ir ją išdėstyti taip:

„2. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius:

1) sudaro sąlygas Nacionaliniam kibernetinio saugumo centrui diegti ir valdyti technines kibernetinio saugumo priemones valstybės informaciniuose ištekliuose ir taikyti technines priemones, siekdami įvertinti valstybės informacinių išteklių atsparumą kibernetiniams incidentams;

2) planuoja atitinkamiems Vyriausybės ir (arba) jos įgaliotos institucijos nustatytiems valstybės informacinių išteklių saugos reikalavimams įgyvendinti reikalingas lėšas ir jas skiria kibernetiniam saugumui ir valstybės informacinių išteklių saugai užtikrinti, taip pat imasi veiksmų, kad suplanuotos lėšos būtų skiriamos, ir kontroliuoja, kaip skirtos lėšos panaudojamos.“

7 straipsnis. Įstatymo papildymas VII skyriumi

Papildyti Įstatymą VII skyriumi:

„**VII SKYRIUS**

VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ SAUGA

21 straipsnis. Valstybės informacinių išteklių saugos užtikrinimas

1. Tvarkant valstybės informacinius išteklius, Valstybės informacinių išteklių valdymo įstatyme nurodytiems registrų informacinių sistemų, valstybės ir vidaus administravimo informacinių sistemų (toliau kartu – informacinės sistemos) tvarkytojams privaloma įgyvendinti saugos priemones, skirtas informacinėse sistemose tvarkomos elektroninės informacijos tikslumui užtikrinti ir jai nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, sugadinimo, atskleidimo, neteisėto pasisavinimo, paskelbimo, pateikimo ar kitokio panaudojimo, taip pat nuo bet kokio kito neteisėto tvarkymo apsaugoti.

2. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, siekdami užtikrinti valstybės informacinių išteklių saugą, vadovaudamiesi Vyriausybės tvirtinamu bendrųjų elektroninės informacijos saugos reikalavimų aprašu, rengia, derina ir tvirtina informacinės sistemos saugos dokumentus. Informacinės sistemos valdytojas gali tvirtinti visų jo valdymo sričiai priskirtų informacinių sistemų bendrus saugos dokumentus. Organizuojant valstybės informacinių išteklių saugą, rekomenduojama vadovautis pripažintų standartizacijos organizacijų ir standartizacijos institucijų priimtais ir paskelbtais standartais.

3. Už informacinėje sistemoje tvarkomų duomenų saugą pagal kompetenciją atsako subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius. Subjektai, tvarkantys valstybės informacinius išteklius, privalo saugos nuostatuose ir kituose saugos dokumentuose nustatyta tvarka užtikrinti reikiamas technines ir organizacines saugos priemones ir tokių priemonių laikymąsi.

4. Valstybės tarnautojai arba darbuotojai, dirbantys pagal darbo sutartis ir gaunantys darbo užmokestį iš valstybės ir savivaldybių biudžetų ir valstybės pinigų fondų, tvarkantys duomenis informacinėje sistemoje, privalo įsipareigoti saugoti elektroninės informacijos paslaptį, kurią sudaro bet kokia skaitmeninės išraiškos informacija, dokumentai ir (ar) jų kopijos, įskaitant garso, vaizdo arba garso ir vaizdo įrašus, taip pat asmens duomenys, kurie saugomi, perduodami, interpretuojami ir apdorojami informacinių technologijų priemonėmis. Įsipareigojimas saugoti paslaptį galioja ir tada, kai su elektroninės informacijos tvarkymu susijusi veikla nutraukiama perėjus dirbti į kitas pareigas, pasibaigus darbo ar sutartiniams santykiams.

5. Fizinių asmenų asmens duomenų saugumas užtikrinamas vadovaujantis Reglamentu (ES) 2016/679 ir (ar) Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymu.

6. Informacija apie saugos priemones, nurodytas šio straipsnio 1 dalyje, ir valstybės informacinių išteklių pažeidžiamumą nėra viešai skelbiama. Informacija teikiama tik jeigu teisė gauti šią informaciją yra nustatyta įstatymuose ar jų pagrindu priimtuose kituose norminiuose teisės aktuose.

22 straipsnis. Saugos įgaliotinis

1. Saugos įgaliotinis atsako už saugos reikalavimų vykdymą ir atlieka informacinės sistemos saugos nuostatuose ir kituose valstybės informacinių išteklių saugą reglamentuojančiuose teisės aktuose nustatytas funkcijas.

2. Saugos įgaliotinis skiriamas teisės aktu, kuriuo tvirtinami informacinės sistemos saugos nuostatai, arba informacinės sistemos valdytojas paveda informacinės sistemos tvarkytojui paskirti saugos įgaliotinį. Gali būti skiriamas kelių informacinių sistemų saugos įgaliotinis.

3. Saugos įgaliotinis negali turėti neišnykusio ar nepanaikinto teistumo už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat negali turėti paskirtos administracinės nuobaudos už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo veikimui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo nuobaudos paskyrimo yra praėję mažiau kaip vieni metai.

23 straipsnis. Valstybės informacinių išteklių atitikties nustatytiems elektroninės informacijos saugos reikalavimams stebėsena

Subjektai, valdantys valstybės informacinius išteklius (išskyrus įslaptintos informacijos tvarkymą), valstybės informacinių išteklių atitikties saugos reikalavimams stebėsenos sistemoje šios sistemos nuostatuose nustatyta tvarka teikia duomenis apie organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, ir elektroninės informacijos saugos reikalavimų, taikomų valstybės informacinius išteklius valdantiems ir (arba) tvarkantiems subjektams, įgyvendinimą savo valdomuose valstybės informaciniuose ištekliuose.

24 straipsnis. Valstybės informacinių išteklių saugos vertinimas

1. Vertinant ypatingos svarbos ir svarbių valstybės informacinių išteklių saugą, o jeigu kartu yra tvarkomi vidutinės ir (ar) mažos svarbos valstybės informaciniai ištekliai, atliekant saugos auditą kartu įtraukiami ir šie ištekliai. Šių išteklių saugos auditas atliekamas ne rečiau kaip kartą per 3 metus.

2. Valstybės informacinių išteklių saugos auditą atlieka nepriklausomi visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai arba minėtų organizacijų sertifikatus turintys informacinių technologijų specialistai, kuriems negali būti pavedama vertinti savo valdomų ir (arba) tvarkomų valstybės informacinių išteklių saugos.

25 straipsnis. Saugusis tinklas

1. Valstybės ir savivaldybių institucijos ir įstaigos, valstybės valdomos įmonės ir viešosios įstaigos (toliau kartu – institucijos), įrašytos į Saugiojo tinklo 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 (arba) prie viešųjų elektroninių ryšių tinklų jungtis ne per Saugųjį tinklą yra būtina renkant ir (arba) 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 (arba) tvarkančioms valstybės informacinius išteklius, būtinus gyvybiškai svarbioms valstybės funkcijoms atlikti ir valstybinėms mobilizacinėms užduotims vykdyti, ir (arba) 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 (arba) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esančių institucijų ar duomenų centrų.

3. Saugųjį tinklą 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.

26 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) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esančiuose duomenų centruose, vadovaudamosi Valstybės informacinių išteklių valdymo įstatymo 45 straipsnio 1–4 ir 6 dalyse nustatyta tvarka. 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) Šiaurės Atlanto sutarties organizacijos (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) Šiaurės Atlanto sutarties organizacijos (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) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esantiems duomenų centrams, kuriuose laikomi valstybės informaciniai ištekliai, tvirtinami Valstybės informacinių išteklių įstatymo nustatyta tvarka.“

8 straipsnis. Įstatymo įsigaliojimas ir taikymas

1. Šis įstatymas įsigalioja 2024 m. sausio 1 d.

2. Iki šio įstatymo įsigaliojimo dienos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka paskirtiems saugos įgaliotiniams taikomos šio įstatymo 7 straipsnyje išdėstyto Lietuvos Respublikos kibernetinio saugumo įstatymo VII skyriaus „Valstybės informacinių išteklių sauga“ 22 straipsnio nuostatos.

3. Iki šio įstatymo įsigaliojimo dienos Valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka pradėtiems informacinių technologijų auditams taikomas iki šio įstatymo įsigaliojimo galiojęs teisinis reguliavimas. Laikotarpis valstybės informacinių išteklių saugos auditams atlikti pradedamas skaičiuoti nuo šio įstatymo įsigaliojimo dienos.

4. Iki šio įstatymo įsigaliojimo dienos Valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka į Saugiojo tinklo naudotojų sąrašą įtrauktoms institucijoms taikomos šio įstatymo 7 straipsnyje išdėstyto Kibernetinio saugumo įstatymo VII skyriaus „Valstybės informacinių išteklių sauga“ 25 ir 26 straipsnių nuostatos.

Skelbiu šį Lietuvos Respublikos Seimo priimtą įstatymą.

Respublikos Prezidentas Gitanas Nausėda

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Lietuvos Respublikos Seimo kanceliarija 188605295, Gedimino pr. 53 1 K-02, 01109 Vilniaus m.
Dokumento pavadinimas (antraštė)	Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 1, 2, 5, 6, 8, 12 straipsnių pakeitimo ir Įstatymo papildymo VII skyriumi įstatymas
Dokumento registracijos data ir numeris	2023-12-21 Nr. XIV-2438
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Kopijos tikrumo patvirtinimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Rita Koncijalovienė, Vyriausioji specialistė, Dokumentų departamentas
Sertifikatas išduotas	RITA,KONCIJALOVIENĖ
Parašo sukūrimo data ir laikas	2023-12-29 15:17:26
Parašo formatas	XAdES-X-L
Laiko žymoje nurodytas laikas	2023-12-29 15:17:45
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2023-06-01 - 2028-05-30
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	-
Pagrindinio dokumento priedų skaičius	1
Pagrindinio dokumento pridedamų dokumentų skaičius	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	eSeimas. Teisės aktų informacinė sistema (TAIS), versija 1.2.112
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Metadata entry "Index of the case (volume) the document is assigned to" must be specified Visi dokumente esantys elektroniniai parašai galioja (2023-12-31)
Paieškos nuoroda	https://www.e-tar.lt/portal/legalAct.html?documentId=59224c90a49011ee8172b53a675305ab
Papildomi metaduomenys	Nuorašą suformavo 2023-12-31 01:26:04 TAIS