Projekto
lyginamasis variantas

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

2023 m. d. Nr.
Vilnius

1 straipsnis. 1 straipsnio pakeitimas

Pakeisti 1 straipsnio 1 dalį ir ją išdėstyti taip:

„1. Šis įstatymas nustato kibernetinio saugumo principus, kibernetinio saugumo **ir valstybės informacinių išteklių saugos** politikos **(toliau kartu – kibernetinio saugumo politika)** 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, taip pat nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas ir įgaliojimus.“

2 straipsnis. 2 straipsnio pakeitimas

Papildyti 2 straipsnį 15^1 dalimi ir ją išdėstyti taip:

„**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 ir jį išdėstyti taip:

„**7) tvirtina subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, taikomų elektroninės informacijos saugos reikalavimų (toliau – elektroninės informacijos saugos reikalavimai) aprašą ir saugos dokumentų turinio gaires;**“.

2. Buvusį 5 straipsnio 6 punktą laikyti 7 punktu.

4 straipsnis. 6 straipsnio pakeitimas

1. Pakeisti 6 straipsnio 2 punktą ir jį išdėstyti taip:

„2) teikia Vyriausybei tvirtinti organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus kibernetinio saugumo subjektams**, elektroninės informacijos saugos reikalavimų aprašą ir saugos dokumentų turinio gaires**;“.

2. Pakeisti 6 straipsnį 11 punktu ir jį išdėstyti taip:

„11) steigia Kibernetinio saugumo informacinį tinklą ir tvirtinta jo nuostatus**, taip pat valdo Saugųjį tinklą**;“.

5 straipsnis. 8 straipsnio pakeitimas

1. Papildyti 8 straipsnį nauju 17 punktu ir jį išdėstyti taip:

„**17) atlieka valstybės informacinių išteklių atitikties teisės aktų nustatytiems elektroninės informacijos saugos reikalavimams stebėseną;**“.

2. Papildyti 8 straipsnį 18 punktu ir jį išdėstyti taip:

„**18) derina su valstybės informacinių išteklių sauga susijusių teisės aktų ir saugos dokumentų projektus;**“.

3. Papildyti 8 straipsnį 19 punktu ir jį išdėstyti taip:

„**19) konsultuoja subjektus, valdančius ir (arba) tvarkančius valstybės informacinius išteklius, kitus subjektus valstybės informacinių išteklių saugos klausimais;**“.

4. Papildyti 8 straipsnį 20 punktu ir jį išdėstyti taip:

„**20) organizuoja valstybės informacinių išteklių saugos vertinimą;**“.

5. Buvusį 8 straipsnio 17 punktą laikyti 21 punktu.

6 straipsnis. 12 straipsnio pakeitimas

Pakeisti 12 straipsnio 2 dalį ir ją išdėstyti taip:

„2. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius~~, sudaro sąlygas Nacionaliniam kibernetinio saugumo centrui diegti ir valdyti technines kibernetinio saugumo priemones valstybės informaciniuose ištekliuose ir taikyti technines priemones, siekiant įvertinti valstybės informacinių išteklių atsparumą kibernetiniams incidentams~~**:**

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

2) skiria lėšas valstybės informacinių išteklių saugai užtikrinti ir elektroninės informacijos saugos reikalavimams įgyvendinti.“

7 straipsnis. Įstatymo papildymas VII skyriumi

Papildyti Įstatymą VII skyriumi ir jį išdėstyti taip:

„**VII SKYRIUS**
VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ SAUGA

21 straipsnis. Valstybės informacinių išteklių sauga

1. Tvarkant valstybės informacinius išteklius, privaloma įgyvendinti teisines, organizacines ir technines elektroninės informacijos saugos priemones, skirtas apsaugoti informacinėse sistemose tvarkomus duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, sugadinimo, atskleidimo, neteisėto pasisavinimo, paskelbimo, pateikimo ar kitokio panaudojimo, taip pat nuo bet kokio kito neteisėto tvarkymo.

2. Siekiant užtikrinti valstybės informacinių išteklių saugą, vadovaujantis Vyriausybės tvirtinamu elektroninės informacijos saugos reikalavimų aprašu rengiami, derinami ir tvirtinami informacinės sistemos saugos dokumentai. Informacinės sistemos valdytojas gali tvirtinti visų jo valdymo sričiai priskirtų informacinių sistemų bendrus saugos dokumentus. Tais atvejais, kai informacinės sistemos tvarkytojas tvarko skirtingų valdytojų valdomas informacines sistemas, informacinės sistemos valdytojas gali tvirtinti bendrus jo valdymo sričiai priskirtų informacinių sistemų, kurias tvarko tas pats tvarkytojas, 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. Darbuotojai, informacinėje sistemoje tvarkantys duomenis, privalo įsipareigoti saugoti duomenų paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su duomenų tvarkymu susijusią veiklą.

5. Fizinių asmenų asmens duomenų saugumas užtikrinamas vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) ir 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 elektroninės informacijos saugos priemones, nurodytas šio straipsnio 1 dalyje, ir valstybės informacinių išteklių pažeidžiamumą yra konfidenciali ir teikiama, jeigu galimybė teikti šią informaciją yra numatyta įstatymuose ar jų pagrindu priimtuose kituose norminiuose teisės aktuose.

22 straipsnis. Saugos įgaliotinis

1. Saugos įgaliotiniu skiriamas darbuotojas, kuris atsako už elektroninės informacijos saugos reikalavimų vykdymą ir atlieka kitas informacinės sistemos saugos nuostatuose ir kituose teisės aktuose nustatytas funkcijas.

2. Asmuo gali būti skiriamas ir atlikti saugos įgaliotinio funkcijas, jeigu atitinka šiuos reikalavimus:

1) neturi neišnykusio ar nepanaikinto teistumo už:

a) neteisėtą poveikį elektroniniams duomenims;

b) neteisėtą poveikį informacinėms sistemoms;

c) neteisėtą elektroninių duomenų perėmimą ir panaudojimą;

d) neteisėtą prisijungimą prie informacinių sistemų;

e) neteisėtą disponavimą įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis;

2) per pastarus 12 mėnesių neturi paskirtos administracinės nuobaudos už:

a) neteisėtą valstybės informacinių sistemų duomenų tvarkymą;

b) Kibernetinio saugumo įstatyme nustatytų kibernetinio saugumo užtikrinimo pareigų neatlikimą ar netinkamų jų atlikimą;

c) įslaptintos informacijos administravimo ar apsaugos reikalavimų pažeidimą;

d) Reglamento (ES) 2019/881 nustatytos kibernetinio saugumo sertifikavimo tvarkos pažeidimus;

e) neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje;

f) elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą;

g) elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą;

h) elektroninių ryšių infrastruktūros įrengimo, žymėjimo, priežiūros ir naudojimo taisyklių pažeidimą.

3. Skirdamas saugos įgaliotinį, subjekto vadovas arba jo įgaliotas darbuotojas privalo patikrinti skiriamo asmens atitiktį šio straipsnio 2 dalies nustatytiems reikalavimams ir turi teisę šiuo tikslu gauti reikalingus informacinių sistemų duomenis, o jį paskyręs - privalo šio asmens atitiktį nustatytiems reikalavimams tikrinti ne rečiau kaip kartą per ketvirtį.

4. Asmuo negali atlikti saugos įgaliotinio funkcijų, jeigu paaiškėja, kad yra pradėtas ikiteisminis tyrimas (iškelta baudžiamoji byla) dėl jo galimai padarytų šio straipsnio 2 dalyje nurodytų draudžiamų veikų. Šiuo atveju tokio asmens įgaliojimai vykdyti saugos įgaliotinio funkcijas yra laikinai sustabdomi. Kol atliekamas ikiteisminis tyrimas ir (ar) vyksta teismo procesas, laikinai saugos įgaliotinio funkcijoms atlikti šio straipsnio 2 ir 3 dalyse nustatyta tvarka yra skiriamas kitas asmuo.

5. Saugos įgaliotinis skiriamas teisės aktu, kuriuo tvirtinami informacinės sistemos saugos nuostatai, arba informacinės sistemos valdytojas paveda informacinės sistemos tvarkytojui paskirti saugos įgaliotinį.

6. Saugos įgaliotinis gali būti paskiriamas kelioms informacinėms sistemoms.

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

Subjektai, valdantys valstybės informacinius išteklius teikia duomenis apie elektroninės informacijos saugos reikalavimų įgyvendinimą savo valdomuose valstybės informaciniuose ištekliuose Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatuose nustatyta tvarka.

24 straipsnis. Saugusis tinklas

1. Valstybės ir savivaldybių institucijos ir įstaigos, valstybės 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. 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 ministerijos teikimu tvirtina Vyriausybė. Saugiuoju tinklu negali naudotis į Saugiojo tinklo naudotojų sąrašą neįtraukti subjektai. Krašto apsaugos ministerija 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 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 (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, ir 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 reikiamų prekių ir paslaugų įsigijimui taikomi Viešųjų pirkimų įstatymo reikalavimai.

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

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

2) 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 sąlygose ir taisyklėse. Saugiojo tinklo tvarkytojas užtikrina neatlygintiną standartinių paslaugų teikimą Saugiojo tinklo naudotojams. Išlaidos, patirtos dėl neatlygintinai teikiamų standartinių paslaugų, finansuojamos 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 kriterijus ir atlyginimo nustatymo 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 apskaičiuoti atsižvelgiant į Vyriausybės patvirtintus atlyginimo už naudojimąsi papildomomis paslaugomis dydžių 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.

25 straipsnis. Duomenų centrų naudojimas

1. Institucijos, įrašytos į Saugiojo tinklo naudotojų sąrašą, savo valdomus valstybės informacinius išteklius laiko valstybiniuose duomenų centruose arba Lietuvos Respublikoje ar kitose Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (arba) Šiaurės Atlanto Sutarties Organizacijos (NATO) valstybėse narėse esančiuose duomenų centruose vadovaudamosi Valstybės informacinių išteklių valdymo įstatymo 49 straipsnio 1–4 ir 6 dalyse nustatyta tvarka.

2. 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 (arba) Šiaurės Atlanto Sutarties Organizacijos (NATO) valstybėse narėse esančiuose duomenų centruose, finansuojamos iš šioms institucijoms skirtų valstybės biudžeto lėšų ir (arba) padengiamos iš kitų teisės aktuose nustatytų finansavimo šaltinių.

3. Valstybinių duomenų centrų sąrašas, techniniai ir organizacinius reikalavimai, taikomi valstybiniams duomenų centrams ir Lietuvos Respublikoje ar kitose Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (arba) 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 taikymas ir įsigaliojimas

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

2. Iki šio įstatymo įsigaliojimo Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka paskirtiems saugos įgaliotiniams taikomos šio įstatymo 7 straipsnyje išdėstyto Lietuvos Respublikos kibernetinio saugumo įstatymo 22 straipsnio nuostatos.

3. Iki šio įstatymo įsigaliojimo Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka į Saugiojo tinklo naudotojų sąrašą įtrauktoms institucijos taikomos šio įstatymo 7 straipsnyje išdėstyto Lietuvos Respublikos kibernetinio saugumo įstatymo 24 ir 25 straipsnių nuostatos.

Skelbiu šį Lietuvos Respublikos Seimo priimtą įstatymą.

Respublikos Prezidentas