Suvestinė redakcija nuo 2024-05-01 iki 2024-10-17

Įstatymas paskelbtas: TAR 2014-12-23, i. k. 2014-20553

Nauja redakcija nuo 2018-07-04:
Nr. XIII-1299, 2018-06-27, paskelbta TAR 2018-07-03, i. k. 2018-11180

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 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.

Straipsnio dalies pakeitimai:
Nr. XIV-2438, 2023-12-21, paskelbta TAR 2023-12-29, i. k. 2023-26027

2. Šis įstatymas netaikomas patikimumo užtikrinimo paslaugų teikėjams, kuriems taikomi 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB, 19 straipsnyje nustatyti reikalavimai.

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

Straipsnio pakeitimai:
Nr. XIV-413, 2021-06-17, paskelbta TAR 2021-06-23, i. k. 2021-14159

2 straipsnis. Pagrindinės šio įstatymo sąvokos

1. **Debesijos paslaugos** – paslaugos, kurių gavėjai nuotoliniu būdu naudojasi šių paslaugų teikėjų valdoma ryšių ir informacinių sistemų infrastruktūra.

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

3. **Elektroninės prekyvietės paslauga** – paslauga, kuria sudaromos sąlygos vartotojams ir (arba) komercinės veiklos subjektams sudaryti elektroninės prekybos ar paslaugų sutartis su komercinės veiklos subjektais elektroninės prekyvietės svetainėje arba komercinės veiklos subjekto svetainėje, kurioje naudojamasi elektroninės prekyvietės teikiamomis kompiuterijos paslaugomis.

4. **Ypatingos svarbos informacinė infrastruktūra** – ryšių ir informacinė sistema ar jos dalis, ryšių ir informacinių sistemų grupė, kurioje įvykęs kibernetinis incidentas gali padaryti didelį neigiamą poveikį nacionaliniam saugumui, valstybės ūkiui, valstybės ir visuomenės interesams.

5. **Ypatingos svarbos informacinės infrastruktūros valdytojas** – asmuo, valdantis ypatingos svarbos informacinę infrastruktūrą.

6. **Kibernetinė erdvė** – aplinka, kurią sudaro kompiuteriai ir kita ryšių ir informacinių technologijų įranga ir juose sukuriama ir (arba) jais perduodama elektroninė informacija.

7. **Kibernetinio saugumo krizė** – kibernetinis incidentas arba incidentai, kurių sukelto neigiamo poveikio Lietuvos Respublika negali pašalinti viena pati arba kurie Lietuvos Respublikai ir kitoms valstybėms, priklausančioms tarptautinėms organizacijoms, kurių narė yra Lietuvos Respublika, arba tų tarptautinių organizacijų institucijoms sukelia tokio masto ir tokios techninės arba politinės reikšmės neigiamą poveikį, kad iškyla poreikis koordinuoti politiką ir reaguoti tarptautiniu lygmeniu.

8. **Kibernetinio saugumo subjektas** – subjektas, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas.

Straipsnio dalies pakeitimai:
Nr. XIV-638, 2021-11-11, paskelbta TAR 2021-11-25, i. k. 2021-24247

9. **Kibernetinis incidentas** – įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.

10. **Kibernetinis saugumas** – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir

informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą.

11. **Kibernetinių incidentų valdymas** – procedūros, kurių tikslas – aptikti, analizuoti kibernetinius incidentus ir reaguoti į juos, taip pat atkurti įprastinę ryšių ir informacinių sistemų veiklą.

12. **Paieškos internete paslauga** – paslauga, kuria interneto vartotojams sudaromos sąlygos atlikti paiešką svetainėse pagal kokio nors dalyko užklausą, vartojant raktinį žodį, frazę arba kitus įvesties duomenis. Atlikus paiešką pateikiamos nuorodos, kuriose gali būti su ieškomu turiniu susijusios informacijos.

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

14. **Ryšių ir informacinė sistema** – elektroninių ryšių tinklas, informacinė sistema, registras, pramoninių procesų valdymo sistema ir jų valdymo, naudojimo, apsaugos ir priežiūros tikslais laikoma, tvarkoma, atkuriama arba perduodama elektroninė informacija.

14[1]. **Ryšių ir informacinės sistemos spraga** (toliau – spraga) – ryšių ir informacinės sistemos trūkumas, dėl kurio gali įvykti kibernetinis incidentas.

Papildyta straipsnio dalimi:
Nr. XIV-413, 2021-06-17, paskelbta TAR 2021-06-23, i. k. 2021-14159

15. **Rizika** – pagrįstai nustatoma aplinkybė ar įvykis, galintis turėti neigiamą poveikį ryšių ir informacinių sistemų saugumui.

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.

Papildyta straipsnio dalimi:
Nr. XIV-2438, 2023-12-21, paskelbta TAR 2023-12-29, i. k. 2023-26027

16. **Skaitmeninės paslaugos** – ryšių ir informacinėmis technologijomis grindžiama paslaugų grupė, apimanti elektroninės prekyvietės, paieškos internete ir (arba) debesijos paslaugas.

17. **Skaitmeninių paslaugų teikėjas** – juridinis asmuo, teikiantis skaitmenines paslaugas Lietuvoje Respublikoje ir (arba) kitose Europos Sąjungos valstybėse narėse.

17[1]. Sąvokos „Europos kibernetinio saugumo sertifikavimo schema“, „Europos kibernetinio saugumo sertifikatas“, „akreditavimas“ ir „atitikties vertinimo įstaiga“ šiame įstatyme suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2019/881.

Papildyta straipsnio dalimi:
Nr. XIV-413, 2021-06-17, paskelbta TAR 2021-06-23, i. k. 2021-14159

18. Kriterijai, kuriais remiantis vertinama, ar šio įstatymo 2 straipsnio 4 dalyje nurodytas neigiamas poveikis yra didelis, nustatomi ypatingos svarbos informacinės infrastruktūros identifikavimo metodikoje.

19. Kitos šiame įstatyme vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, Lietuvos Respublikos elektroninių ryšių įstatyme, Lietuvos Respublikos informacinės visuomenės paslaugų įstatyme, Lietuvos Respublikos kriminalinės žvalgybos 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 ir 2012 m. spalio 25 d. Europos Parlamento ir Tarybos reglamente (ES) Nr. 1025/2012 dėl Europos standartizacijos, kuriuo iš dalies keičiamos Tarybos direktyvos 89/686/EEB ir 93/15/EEB ir Europos Parlamento ir Tarybos direktyvos 94/9/EB, 94/25/EB, 95/16/EB, 97/23/EB, 98/34/EB, 2004/22/EB, 2007/23/EB, 2009/23/EB ir 2009/105/EB ir panaikinamas Tarybos sprendimas Nr. 87/95/EEB ir Europos Parlamento ir Tarybos sprendimas Nr. 1673/2006/EB.

Straipsnio dalies pakeitimai:
Nr. XIII-3114, 2020-06-25, paskelbta TAR 2020-07-09, i. k. 2020-15325
Nr. XIV-413, 2021-06-17, paskelbta TAR 2021-06-23, i. k. 2021-14159

3 straipsnis. Kibernetinio saugumo principai

1. Kibernetinis saugumas grindžiamas šiais kibernetinio saugumo principais:

1) kibernetinės erdvės nediskriminavimo – teisės aktų nuostatos yra taikomos, o gėriai yra saugomi vienodai tiek fizinėje, tiek kibernetinėje erdvėje;

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

3) kibernetinio saugumo proporcingumo – taikomos teisinės, organizacinės ir techninės kibernetinio saugumo priemonės neturi apriboti kibernetinio saugumo subjektų veiklos kibernetinėje erdvėje labiau, negu tai būtina;

4) viešojo intereso viršenybės – taikomos kibernetinio saugumo priemonės pirmiausia turi užtikrinti viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų teisių ar neproporcingai apriboti jų laisvės kibernetinėje erdvėje;

5) standartizacijos ir technologinio neutralumo – įgyvendinant kibernetinio saugumo priemones, kibernetinio saugumo subjektai skatinami vadovautis nacionaliniais, Europos Sąjungos ir kitais tarptautiniais ryšių ir informacinių sistemų kibernetinio saugumo standartais ir

specifikacijomis, nereikalaujant taikyti kokios nors konkrečios rūšies technologijos ir nesuteikiant jai pirmenybės;

6) subsidiarumo – už ryšių 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 ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinio saugumo negali užtikrinti 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 politikos strateginius tikslus, pažangos uždavinius ir jiems pasiekti būtinas priemones nustato Lietuvos Respublikos Vyriausybė.

Straipsnio dalies pakeitimai:
Nr. XIII-3114, 2020-06-25, paskelbta TAR 2020-07-09, i. k. 2020-15325

2. Kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija. Nacionalinis kibernetinio saugumo centras formuojant kibernetinio saugumo politiką dalyvauja tiek, kiek šiame įstatyme nustatytoms funkcijoms atlikti reikia nustatyti kibernetinio saugumo subjektų veiklos teisinį reguliavimą.

3. Kibernetinio saugumo politiką įgyvendina Nacionalinis kibernetinio saugumo centras, Valstybinė duomenų apsaugos inspekcija, Lietuvos policija ir kitos institucijos, kurių funkcijos yra susijusios su kibernetiniu saugumu.

5 straipsnis. Vyriausybės įgaliojimai kibernetinio saugumo srityje

Vyriausybė:

1) nustato kibernetinio saugumo politikos strateginius tikslus ir (arba) pažangos uždavinius tvirtindama Nacionalinį pažangos planą;

Straipsnio punkto pakeitimai:
Nr. XIII-3114, 2020-06-25, paskelbta TAR 2020-07-09, i. k. 2020-15325

2) tvirtina Kibernetinio saugumo tarybos institucinę sudėtį;

3) tvirtina ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką ir ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą;

4) tvirtina organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus kibernetinio saugumo subjektams;

5) tvirtina Nacionalinį kibernetinių incidentų valdymo planą;

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);

Papildyta straipsnio punktu:
Nr. XIV-2438, 2023-12-21, paskelbta TAR 2023-12-29, i. k. 2023-26027

7) vadovauja kibernetinio saugumo krizių valdymui.

Straipsnio punkto numeracijos pakeitimas:
Nr. XIV-2438, 2023-12-21, paskelbta TAR 2023-12-29, i. k. 2023-26027

6 straipsnis. Krašto apsaugos ministerijos įgaliojimai kibernetinio saugumo srityje

Krašto apsaugos ministerija:

1) dalyvauja rengiant Nacionalinį pažangos planą dėl kibernetinio saugumo politikos strateginių tikslų ir (arba) pažangos uždavinių nustatymo;

Straipsnio punkto pakeitimai:
Nr. XIII-3114, 2020-06-25, paskelbta TAR 2020-07-09, i. k. 2020-15325

1^1) rengia kibernetinio saugumo politikos pažangos uždavinius įgyvendinančias nacionalines plėtros programas, organizuoja, koordinuoja ir kontroliuoja jų įgyvendinimą;

Papildyta straipsnio punktu:
Nr. XIII-3114, 2020-06-25, paskelbta TAR 2020-07-09, i. k. 2020-15325

2) teikia Vyriausybei tvirtinti organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus kibernetinio saugumo subjektams;

3) teikia Vyriausybei tvirtinti Nacionalinį kibernetinių incidentų valdymo planą;

4) teikia Vyriausybei tvirtinti ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką;

5) teikia Vyriausybei tvirtinti ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą;

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

Papildyta straipsnio punktu:
Nr. XIV-2438, 2023-12-21, paskelbta TAR 2023-12-29, i. k. 2023-26027

6) tvirtina tipinį kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planą;

7) tvirtina ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planą;

8) nustato Nacionalinio kibernetinio saugumo centro reagavimo į kibernetinio saugumo subjektų ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus tvarką;

9) tvirtina techninių kibernetinio saugumo priemonių sąrašą, kuriame nurodoma kibernetinio saugumo priemonių paskirtis ir tvarkomi duomenys (jeigu jie yra tvarkomi), techninių kibernetinio saugumo priemonių diegimo planą, nustato jų diegimo ir valdymo valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėje infrastruktūroje tvarką;

Straipsnio punkto pakeitimai:
Nr. XIV-413, 2021-06-17, paskelbta TAR 2021-06-23, i. k. 2021-14159

10) dalyvauja kibernetinio saugumo krizių valdyme;

11) steigia Kibernetinio saugumo informacinį tinklą ir tvirtinta jo nuostatus;

11^{1}) valdo Saugųjį tinklą;

Papildyta straipsnio punktu:
Nr. XIV-2438, 2023-12-21, paskelbta TAR 2023-12-29, i. k. 2023-26027

12) tvirtina Kibernetinio saugumo tarybos reglamentą ir personalinę sudėtį;

13) tvirtina nacionalinės spragų atskleidimo tvarkos aprašą.

Papildyta straipsnio punktu:
Nr. XIV-413, 2021-06-17, paskelbta TAR 2021-06-23, i. k. 2021-14159

7 straipsnis. Kibernetinio saugumo taryba

1. Kibernetinio saugumo taryba yra nuolatinė kolegiali nepriklausoma patariamoji institucija, analizuojanti kibernetinio saugumo užtikrinimo būklę Lietuvos Respublikoje ir teikianti kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijoms, kibernetinio saugumo subjektams, mokslo ir studijų institucijoms ir informacinių technologijų srityje veiklą vykdantiems verslo subjektams (toliau – kibernetinio saugumo dalyviai) pasiūlymus dėl kibernetinio saugumo užtikrinimo būklės gerinimo.

2. Kibernetinio saugumo tarybai vadovauja Krašto apsaugos ministerijos atstovas.

3. Kibernetinio saugumo tarybą ūkiškai ir techniškai aptarnauja Krašto apsaugos ministerija ar jos įgaliota institucija.

4. Kibernetinio saugumo taryba:

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

2) teikia kibernetinio saugumo dalyviams pasiūlymus dėl 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.

8 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 ir užtikrindamas valstybės informacinių išteklių saugą, pagal kompetenciją:

Straipsnio dalies pakeitimai:
Nr. XIV-2438, 2023-12-21, paskelbta TAR 2023-12-29, i. k. 2023-26027

1) atlieka kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams, priežiūrą ir kibernetinio saugumo būklės tyrimus;

2) duoda nurodymus kibernetinio saugumo subjektams pateikti informaciją, būtiną kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams, ir kibernetinio saugumo būklės įvertinimui atlikti;

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

4) duoda nurodymus, susijusius su kibernetinio saugumo užtikrinimu ir nustatytų kibernetinio saugumo trūkumų pašalinimu, nustato šių nurodymų įvykdymo terminą subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams ir elektroninės informacijos prieglobos paslaugų teikėjams;

Straipsnio punkto pakeitimai:
Nr. XIV-638, 2021-11-11, paskelbta TAR 2021-11-25, i. k. 2021-24247

5) duoda nurodymus kibernetinio saugumo subjektams, išskyrus skaitmeninių paslaugų teikėjus, savo lėšomis atlikti nepriklausomą ryšių ir informacinių sistemų arba jomis teikiamų paslaugų saugumo auditą ir pateikti šio audito rezultatus, jei jie organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše nustatyta tvarka nepateikia techninės informacijos, reikalingos ryšių ir informacinių sistemų ar jomis teikiamų paslaugų kibernetinio saugumo būklei įvertinti;

6) gavęs iš kibernetinio saugumo subjekto, skaitmeninės paslaugos vartotojo arba kitos Europos Sąjungos valstybės narės, kurioje yra teikiama skaitmeninė paslauga, kompetentingos institucijos, prižiūrinčios skaitmeninių paslaugų teikėjų veiklą kibernetinio saugumo srityje, įrodymų, kad skaitmeninių paslaugų teikėjai neatitinka šio įstatymo nustatytų reikalavimų, duoda nurodymus skaitmeninių paslaugų teikėjams, kad šie pateiktų informaciją, reikalingą jų valdomų ryšių ir informacinių sistemų kibernetiniam saugumui įvertinti, ir pašalintų kibernetinio saugumo reikalavimų įgyvendinimo trūkumus;

7) nacionaliniu lygmeniu stebi kibernetinius incidentus ir atlieka rizikos kibernetinėje erdvėje bei kibernetinių incidentų analizę;

8) pagal techninių kibernetinio saugumo priemonių diegimo planą, suderintą su subjektais, valdančiais ir (arba) tvarkančiais valstybės informacinius išteklius, ar ypatingos svarbos informacinės infrastruktūros valdytojais, laikydamasis krašto apsaugos ministro nustatytos tvarkos, diegia ir valdo 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 prižiūrimos, jų remontas atliekamas Nacionalinio kibernetinio saugumo centro lėšomis;

9) nacionaliniu lygmeniu organizuoja kibernetinių incidentų kibernetinio saugumo subjektų ryšių ir informacinėse sistemose valdymą;

10) kibernetinio incidento metu taiko būtinas kibernetinio saugumo priemones;

11) siekdamas stabdyti kibernetinio incidento poveikį valstybės informacinių išteklių ar ypatingos svarbos informacinių infrastruktūrų kibernetiniam saugumui, duoda nurodymą viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjui ne ilgiau negu 48 valandoms apriboti viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikimą šių paslaugų gavėjui. Nacionalinis kibernetinio saugumo centras apie viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams pagal šį punktą duotus nurodymus ne vėliau kaip kitą darbo dieną praneša Lietuvos Respublikos ryšių reguliavimo tarnybai;

Straipsnio punkto pakeitimai:
Nr. XIV-638, 2021-11-11, paskelbta TAR 2021-11-25, i. k. 2021-24247

12) dalyvauja kibernetinio saugumo krizių valdyme;

13) kai būtina informuoti visuomenę siekiant išvengti kibernetinio incidento arba valdyti vykstantį kibernetinį incidentą, pasikonsultavęs su kibernetinio saugumo subjektu, pranešusiu

apie kibernetinį incidentą, informuoja visuomenę apie pavienius kibernetinius incidentus arba reikalauja, kad tai padarytų kibernetinio saugumo subjektas;

14) bendradarbiauja su tarptautinių organizacijų kompetentingomis institucijomis, jų įsteigtomis bendradarbiavimo grupėmis ir užsienio valstybių kompetentingomis institucijomis ir tarnybomis, turi teisę jas pasitelkti kartu atliekant šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje;

15) tvarko asmens duomenis, būtinus Nacionalinio kibernetinio saugumo centro funkcijoms kibernetinio saugumo užtikrinimo srityje atlikti. Nacionalinis kibernetinio saugumo centras asmens duomenis tvarko Asmens duomenų teisinės apsaugos įstatymo nustatyta tvarka;

16) kartu su verslo subjektais, mokslo ir studijų institucijomis ir kibernetinio saugumo subjektais plėtoja nacionalinį kibernetinį saugumą stiprinančius projektus;

16[1]) analizuoja informaciją apie spragas, duoda nurodymus subjektams, valdantiems ir (ar) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjams ir elektroninės informacijos prieglobos paslaugų teikėjams dėl spragų patvirtinimo ir informavimo apie jas;

Papildyta straipsnio punktu:
Nr. XIV-413, 2021-06-17, paskelbta TAR 2021-06-23, i. k. 2021-14159

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

Papildyta straipsnio punktu:
Nr. XIV-2438, 2023-12-21, paskelbta TAR 2023-12-29, i. k. 2023-26027

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

Papildyta straipsnio punktu:
Nr. XIV-2438, 2023-12-21, paskelbta TAR 2023-12-29, i. k. 2023-26027

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

Papildyta straipsnio punktu:
Nr. XIV-2438, 2023-12-21, paskelbta TAR 2023-12-29, i. k. 2023-26027

16[5]) organizuoja valstybės informacinių išteklių saugos vertinimą;

Papildyta straipsnio punktu:
Nr. XIV-2438, 2023-12-21, paskelbta TAR 2023-12-29, i. k. 2023-26027

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

9 straipsnis. Valstybinės duomenų apsaugos inspekcijos įgaliojimai kibernetinio saugumo srityje

Valstybinė duomenų apsaugos inspekcija įgyvendina kibernetinio saugumo politiką asmens duomenų apsaugos srityje ir atlieka 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (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) nustatytas priežiūros institucijos užduotis.

Straipsnio pakeitimai:
Nr. XIV-413, 2021-06-17, paskelbta TAR 2021-06-23, i. k. 2021-14159

10 straipsnis. Policijos įgaliojimai kibernetinio saugumo srityje

Policija, vykdydama kibernetinių incidentų, galimai turinčių nusikalstamų veikų požymių, užkardymą ir atlikdama jų tyrimą:

1) renka, analizuoja ir apibendrina informaciją apie kibernetinius incidentus, galimai turinčius nusikalstamų veikų požymių;

2) nustato kibernetinio saugumo subjektams informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamų veikų požymių, užkardyti ir tirti, pateikimo policijai tvarką;

3) turi teisę, kai paslaugų gavėjas galimai dalyvauja ar jo naudojama ryšių ir informacinių technologijų įranga galimai yra naudojama nusikalstamai veikai, be teismo sankcijos duoti nurodymą viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjui, elektroninės informacijos prieglobos paslaugų teikėjui ir skaitmeninių paslaugų teikėjui ne ilgiau kaip 48 valandoms, o ilgesniam laikui – su apylinkės teismo sankcija apriboti viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikimą paslaugų gavėjui ir (arba) nurodyti taikyti priemones, šalinančias nusikalstamų veikų kibernetinėje erdvėje priežastis. Šiais atvejais apylinkės teismo pirmininkui ar jo įgaliotam 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. Jeigu teisėjas motyvuota nutartimi nepatvirtina teikime nurodytų veiksmų teisėtumo ar pagrįstumo, nurodymas nedelsiant stabdomas;

Straipsnio punkto pakeitimai:
Nr. XIV-638, 2021-11-11, paskelbta TAR 2021-11-25, i. k. 2021-24247

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

nustatyti naudotos ryšio paslaugos tipą, taikytas technines priemones ir naudojimo laiką, paslaugos gavėjo 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, o kai yra motyvuota teismo nutartis, gauti paslaugų gavėjo srauto duomenis ir kontroliuoti šiame punkte nurodytos perduodamos informacijos turinį.

Straipsnio punkto pakeitimai:
Nr. XIV-638, 2021-11-11, paskelbta TAR 2021-11-25, i. k. 2021-24247

III SKYRIUS
KIBERNETINIO SAUGUMO SUBJEKTŲ PAREIGOS

11 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos

1. Kibernetinio saugumo subjektai:

1) atsako už jų valdomų ryšių ir informacinių sistemų ar teikiamų paslaugų kibernetinį saugumą, užtikrina jų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams;

2) organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše nustatyta tvarka atlieka rizikos vertinimą ir įdiegia kitas, naujausiais technikos laimėjimais paremtas ir nustatytai rizikai proporcingas, technines ir organizacines kibernetinio saugumo priemones;

3) Nacionaliniame kibernetinių incidentų valdymo plane nustatytomis sąlygomis ir tvarka praneša Nacionaliniam kibernetinio saugumo centrui apie jų valdomose ir (arba) tvarkomose ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones;

4) policijos generalinio komisaro nustatyta tvarka teikia policijai informaciją, reikalingą teisės pažeidimams, turintiems nusikalstamų veikų požymių, kibernetinėje erdvėje užkardyti ir tirti, ir vykdo kitus policijos nurodymus, duotus šio įstatymo nustatytais pagrindais. Policijos nurodymus dėl paslaugų teikimo jų gavėjui apribojimo privaloma įvykdyti ne vėliau kaip per 8 valandas nuo policijos nurodymo gavimo;

5) paskiria kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, ir Nacionaliniam kibernetinio saugumo centrui pateikia šio asmens ar padalinio kontaktinę informaciją;

6) vykdo šio įstatymo 8 straipsnyje nustatytus Nacionalinio kibernetinio saugumo centro nurodymus.

2. Šio straipsnio nuostatos netaikomos skaitmenines paslaugas Lietuvos Respublikoje ir (arba) kitoje Europos Sąjungos valstybėje narėje teikiančioms mažoms ir labai mažoms įmonėms, kurios yra apibrėžtos Smulkiojo ir vidutinio verslo plėtros įstatyme.

12 straipsnis. Specialiosios kibernetinio saugumo subjektų pareigos

1. Ypatingos svarbos informacinės infrastruktūros valdytojai:

1) vadovaudamiesi krašto apsaugos ministro patvirtintu tipiniu kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planu, patvirtina ir Nacionaliniam kibernetinio saugumo centrui pateikia kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus;

2) Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka praneša skaitmeninių paslaugų teikėjams apie neigiamą poveikį ypatingos svarbos informacinės infrastruktūros veiklai, kurį lėmė skaitmeninių paslaugų teikėjų ryšių ir informacinėse sistemose įvykę sutrikimai;

3) ne rečiau kaip kartą per kalendorinius metus išbando kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planuose numatytų priemonių veikimą ir bandymų rezultatus organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše nustatyta tvarka pateikia Nacionaliniam kibernetinio saugumo centrui;

4) sudaro sąlygas Nacionaliniam kibernetinio saugumo centrui diegti ir valdyti technines kibernetinio saugumo priemones ypatingos svarbos informacinėje infrastruktūroje ir taikyti technines priemones, siekiant įvertinti ypatingos svarbos informacinių infrastruktūrų atsparumą kibernetiniams incidentams.

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.

Straipsnio dalies pakeitimai:
Nr. XIV-2438, 2023-12-21, paskelbta TAR 2023-12-29, i. k. 2023-26027

3. Viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai viešai skelbia savo interneto svetainėse ar kitomis visuomenės informavimo priemonėmis paslaugų gavėjams rekomendacijas dėl priemonių kibernetiniam saugumui užtikrinti naudojantis viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų teikiamomis paslaugomis.

Straipsnio dalies pakeitimai:
Nr. XIV-638, 2021-11-11, paskelbta TAR 2021-11-25, i. k. 2021-24247

4. Elektroninės informacijos prieglobos paslaugų teikėjai viešai skelbia savo interneto svetainėse ar kitomis visuomenės informavimo priemonėmis elektroninės informacijos prieglobos paslaugų gavėjams rekomendacijas dėl priemonių kibernetiniam saugumui užtikrinti naudojantis elektroninės informacijos prieglobos paslaugomis.

5. Skaitmeninių paslaugų teikėjai:

1) viešai skelbia savo interneto svetainėse ar kitomis visuomenės informavimo priemonėmis paslaugų gavėjams rekomendacijas dėl priemonių kibernetiniam saugumui užtikrinti naudojantis skaitmeninių paslaugų teikėjų teikiamomis paslaugomis;

2) skiria atstovą veiklai skaitmeninių paslaugų teikėjo vardu vykdyti Europos Sąjungoje. Šis atstovas skiriamas, jei skaitmeninių paslaugų teikėjas nėra įsisteigęs Europos Sąjungos valstybėje narėje. Atstovas turi būti fizinis arba juridinis asmuo, įsisteigęs vienoje iš tų Europos Sąjungos valstybių narių, kurioje yra teikiamos skaitmeninės paslaugos. Kibernetinio saugumo politikos įgyvendinimo institucijos turi teisę kreiptis į skaitmeninių paslaugų teikėjo atstovą dėl šiame įstatyme nustatytų skaitmeninių paslaugų teikėjo pareigų atlikimo. Jei skaitmeninių paslaugų teikėjas skiria atstovą veiklai Lietuvos Respublikoje vykdyti, laikoma, kad skaitmeninių paslaugų teikėjas priklauso Lietuvos Respublikos jurisdikcijai.

6. Šio straipsnio nuostatos netaikomos skaitmenines paslaugas Lietuvos Respublikoje ir (arba) kitoje Europos Sąjungos valstybėje narėje teikiančioms mažoms ir labai mažoms įmonėms, kurios yra apibrėžtos Smulkiojo ir vidutinio verslo plėtros įstatyme.

IV SKYRIUS
KEITIMASIS INFORMACIJA IR TARPINSTITUCINIS BENDRADARBIAVIMAS

13 straipsnis. Kibernetinio saugumo informacinis tinklas

1. Kibernetinio saugumo informacinis tinklas yra valstybės informacinė sistema, kurios paskirtis – informacinių technologijų priemonėmis tvarkyti duomenis, surinktus techninėmis kibernetinio saugumo priemonėmis, siekiant užkardyti ir valdyti kibernetinius incidentus, keistis

informacija apie galimus ir įvykusius kibernetinius incidentus šio straipsnio 4 dalyje nustatytais atvejais, taip pat kita su kibernetinio saugumo užtikrinimu susijusia informacija.

Straipsnio dalies pakeitimai:
Nr. XIV-413, 2021-06-17, paskelbta TAR 2021-06-23, i. k. 2021-14159

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

3. Kibernetinio saugumo informaciniame tinkle skelbiama aktuali kibernetinio saugumo subjektų paskirtų asmenų ar padalinių, atsakingų už kibernetinio saugumo organizavimą ir kibernetinių incidentų valdymą, kontaktinė informacija.

4. Kibernetinio saugumo informacinio tinklo duomenys, susiję su kibernetiniais incidentais, yra konfidencialūs ir teikiami tik šiais atvejais:

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

2) Nacionaliniam kibernetinio saugumo centrui atliekant šio įstatymo 8 straipsnio 2 dalies 13 punkte nustatytą funkciją;

3) valdant ir tiriant kibernetinius incidentus tiek, kiek tai būtina šio įstatymo 14 straipsnio 1 ir 2 dalyse nustatytoms institucijų funkcijoms atlikti;

Papildyta straipsnio punktu:
Nr. XIV-1864, 2023-03-30, paskelbta TAR 2023-04-05, i. k. 2023-06471

4) jeigu galimybė teikti šiuos duomenis yra nustatyta įstatymuose ar jų pagrindu priimtuose teisės aktuose.

Straipsnio punkto numeracijos pakeitimas:
Nr. XIV-1864, 2023-03-30, paskelbta TAR 2023-04-05, i. k. 2023-06471

Papildyta straipsnio dalimi:
Nr. XIV-413, 2021-06-17, paskelbta TAR 2021-06-23, i. k. 2021-14159

13[1] straipsnis. Duomenų apie privalomus nurodymus tvarkymas Kibernetinio saugumo informaciniame tinkle

1. Kibernetinio saugumo informaciniame tinkle įstatymų nustatytais atvejais tvarkomi duomenys apie privalomus nurodymus blokuoti domeno vardą, identifikuojantį interneto svetainę.

2. Šio straipsnio 1 dalyje 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.

3. Kibernetinio saugumo informaciniame tinkle viešai skelbiami duomenys apie privalomus nurodymus blokuoti domeno vardą, identifikuojantį interneto svetainę.

Papildyta straipsniu:
Nr. XIV-1864, 2023-03-30, paskelbta TAR 2023-04-05, i. k. 2023-06471

14 straipsnis. Tarpinstitucinis bendradarbiavimas valdant ir tiriant kibernetinius incidentus

1. Nacionalinis kibernetinio saugumo centras ir policija konsultuojasi ir bendradarbiauja tiriant kibernetinius incidentus, keičiasi su kibernetinių incidentų tyrimu susijusia informacija, reikalinga pagal kompetenciją šių institucijų funkcijoms atlikti. Prireikus apie kibernetinių incidentų tyrimą gali būti pranešama kitiems kriminalinės žvalgybos subjektams ir (arba) žvalgybos institucijoms.

2. Nacionalinis kibernetinio saugumo centras ir Valstybinė duomenų apsaugos inspekcija bendradarbiauja tiriant kibernetinius incidentus, susijusius su asmens duomenų ir (ar) privatumo apsaugos pažeidimais, keičiasi informacija, reikalinga teisės aktų nustatytoms funkcijoms, susijusioms su asmens duomenų ir (ar) privatumo apsaugą pažeidžiančių kibernetinių incidentų tyrimu, atlikti.

3. Tarpinstitucinio bendradarbiavimo valdant ir tiriant kibernetinius incidentus tvarka nustatoma Nacionaliniame kibernetinių incidentų valdymo plane.

15 straipsnis. Informacijos apsauga

Kibernetinio saugumo politikos įgyvendinimo institucijos kibernetinio saugumo subjektų pateikta informacija, įskaitant ir konfidencialią informaciją, turi teisę keistis tik tiek, kiek tai yra būtina šių institucijų funkcijoms pagal kompetenciją atlikti, ir privalo užtikrinti gautos informacijos apsaugą.

V SKYRIUS
PRANEŠIMAI APIE SPRAGAS IR KIBERNETINIUS INCIDENTUS

Pakeistas skyriaus pavadinimas:
Nr. XIV-413, 2021-06-17, paskelbta TAR 2021-06-23, i. k. 2021-14159

16 straipsnis. Savanoriškas pranešimas apie kibernetinius incidentus

1. Asmenys, kuriems šiame įstatyme nėra nustatytos pareigos pranešti apie kibernetinius incidentus jų valdomose ryšių ir informacinėse sistemose, turi teisę savanoriškai pranešti Nacionaliniam kibernetinio saugumo centrui apie kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones. Nacionalinis kibernetinio saugumo centras tokius pranešimus tvarko Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka.

2. Asmeniui, savanoriškai pranešusiam apie kibernetinį incidentą, nenustatoma pareigų, susijusių su pranešimo pateikimu.

17 straipsnis. Spragų paieška ir atskleidimas

1. Spragų paieška ir atskleidimas laikomi teisėtais ir tokius veiksmus atlikusiam asmeniui neužtraukia teisinės atsakomybės tik tais atvejais, kai spragų paieška atliekama laikantis šio straipsnio 2 dalyje, nacionalinės spragų atskleidimo tvarkos apraše ir (ar) kibernetinio saugumo subjekto nustatytos spragų atskleidimo tvarkos apraše, taip pat šio straipsnio 5 dalyje numatytų apribojimų.

2. Atliekant spragų paiešką laikomasi šių apribojimų:

1) negali būti trikdomas ar keičiamas ryšių 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) asmuo, 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 (arba) kibernetinio saugumo subjektui, kurio ryšių 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) nebandoma atspėti slaptažodžių, nenaudojami neteisėtu būdu gauti slaptažodžiai ir nėra manipuliuojama kibernetinio saugumo subjekto darbuotojais ar kitais asmenimis, turinčiais teisę naudotis viešai neskelbtina informacija, reikšminga spragų paieškai;

6) nesidalijama informacija apie aptiktą spragą, išskyrus šios dalies 3 punkte ir šio straipsnio 5 dalyje nustatytus atvejus.

3. 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, asmenims termino nustatymo tvarka nustatomi nacionalinės spragų atkleidimo tvarkos apraše.

4. Kibernetinio saugumo subjektas turi teisę nustatyti spragų jo valdomose ir (ar) tvarkomose ryšių 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 Nacionaliniam kibernetinio saugumo centrui tvarka ir numatomos šio straipsnio 5 dalyje nustatyto reguliavimo išimtys.

5. Asmuo, nustatęs spragą, laikydamasis šio straipsnio 1 dalyje nurodytų reikalavimų, turi teisę informaciją apie aptiktą spragą, tačiau ne daugiau informacijos, negu buvo pateikta Nacionaliniam kibernetinio saugumo centrui ir (ar) kibernetinio saugumo subjektui, atskleisti kitiems, negu nurodyti šio straipsnio 2 dalies 3 punkte, asmenims 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, asmenims terminą, tačiau ne trumpesnį kaip 3 kalendorinės dienos.

Papildyta straipsniu:
Nr. XIV-413, 2021-06-17, paskelbta TAR 2021-06-23, i. k. 2021-14159

VI SKYRIUS
NACIONALINĖS KIBERNETINIO SAUGUMO SERTIFIKAVIMO INSTITUCIJOS ĮGALIOJIMAI

18 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 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 19 straipsnyje nustatytais atvejais;

3) Lietuvos Respublikos 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 19 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 nuostatų;

5) atlikdamas šios dalies 4 punkte nurodytus tyrimus, įgalioja asmenis, turinčius 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 Lietuvos Respublikos civilinio proceso kodekso XXXIX skyriuje nustatyta tvarka.

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

1. Papildomi įgaliojimai suteikiami, apribojami ir sustabdomi, papildomų įgaliojimų apribojimas ir sustabdymas panaikinamas, papildomi įgaliojimai atšaukiami šiame straipsnyje ir šio įstatymo 18 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 20 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) 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 20 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.

20 straipsnis. Tyrimo atlikimo tvarka

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 19 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 19 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 Lietuvos Respublikos administracinių bylų teisenos įstatymo nustatyta tvarka.

Papildyta skyriumi:
Nr. XIV-413, 2021-06-17, paskelbta TAR 2021-06-23, i. k. 2021-14159

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.

Papildyta skyriumi:
Nr. XIV-2438, 2023-12-21, paskelbta TAR 2023-12-29, i. k. 2023-26027

Skelbiu šį Lietuvos Respublikos Seimo priimtą įstatymą.

Respublikos Prezidentė Dalia Grybauskaitė

Lietuvos Respublikos
kibernetinio saugumo įstatymo
priedas

ĮGYVENDINAMI EUROPOS SĄJUNGOS TEISĖS AKTAI

1. 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti.

2. 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas (nauja redakcija).

Priedo pakeitimai:
Nr. XIV-638, 2021-11-11, paskelbta TAR 2021-11-25, i. k. 2021-24247

Pakeitimai:

1.
Lietuvos Respublikos Seimas, Įstatymas
Nr. XII-2524, 2016-06-29, paskelbta TAR 2016-07-13, i. k. 2016-20282
Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 19 straipsnio pakeitimo įstatymas

2.
Lietuvos Respublikos Seimas, Įstatymas
Nr. XIII-798, 2017-11-21, paskelbta TAR 2017-11-28, i. k. 2017-18853
Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 4, 6 straipsnių pakeitimo ir 7 straipsnio pripažinimo netekusiu galios įstatymas

3.
Lietuvos Respublikos Seimas, Įstatymas
Nr. XIII-920, 2017-12-19, paskelbta TAR 2017-12-29, i. k. 2017-21592
Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 1, 2, 4, 6, 10, 15, 16, 18 straipsnių pakeitimo, 8 straipsnio pripažinimo netekusiu galios ir Įstatymo papildymo priedu įstatymas

4.
Lietuvos Respublikos Seimas, Įstatymas
Nr. XIII-1299, 2018-06-27, paskelbta TAR 2018-07-03, i. k. 2018-11180
Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas

5.
Lietuvos Respublikos Seimas, Įstatymas
Nr. XIII-3114, 2020-06-25, paskelbta TAR 2020-07-09, i. k. 2020-15325
Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 2, 4, 5 ir 6 straipsnių pakeitimo įstatymas

6.
Lietuvos Respublikos Seimas, Įstatymas
Nr. XIV-413, 2021-06-17, paskelbta TAR 2021-06-23, i. k. 2021-14159
Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 1, 2, 6, 8, 9, 13 straipsnių, V skyriaus pavadinimo, priedo pakeitimo ir Įstatymo papildymo 17 straipsniu ir VI skyriumi įstatymas

7.
Lietuvos Respublikos Seimas, Įstatymas
Nr. XIV-638, 2021-11-11, paskelbta TAR 2021-11-25, i. k. 2021-24247

Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 2, 8, 10, 12 straipsnių ir priedo pakeitimo įstatymas

8.
Lietuvos Respublikos Seimas, Įstatymas
Nr. XIV-1864, 2023-03-30, paskelbta TAR 2023-04-05, i. k. 2023-06471
Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 13 straipsnio pakeitimo ir Įstatymo papildymo 13-1 straipsniu įstatymas

9.
Lietuvos Respublikos Seimas, Įstatymas
Nr. XIV-2438, 2023-12-21, paskelbta TAR 2023-12-29, i. k. 2023-26027
Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 1, 2, 5, 6, 8, 12 straipsnių pakeitimo ir Įstatymo papildymo VII skyriumi įstatymas