Suvestinė redakcija nuo 2021-01-01

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, taip pat tarpinstitucinį bendradarbiavimą.

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, (OL 2014 L 257, p. 73) 19 straipsnyje nustatyti reikalavimai.

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

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 ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas.

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.

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

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.

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 elektroninių ryšių įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos informacinės visuomenės paslaugų įstatyme, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, Lietuvos Respublikos žvalgybos įstatyme, Lietuvos Respublikos kriminalinės žvalgybos įstatyme, Lietuvos Respublikos nesąžiningos komercinės veiklos vartotojams draudimo įstatyme, Lietuvos Respublikos smulkiojo ir vidutinio verslo plėtros įstatyme, Lietuvos Respublikos strateginio valdymo 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 (OL 2012 L 316, p. 12).

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

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) vadovauja kibernetinio saugumo krizių valdymui.

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;

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 diegimo planą, nustato jų diegimo ir valdymo valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėje infrastruktūroje tvarką;

10) dalyvauja kibernetinio saugumo krizių valdyme;

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

12) tvirtina Kibernetinio saugumo tarybos reglamentą ir personalinę sudėtį.

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:

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 ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams ir elektroninės informacijos prieglobos paslaugų teikėjams;

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 ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjui ne ilgiau negu 48 valandoms apriboti viešųjų ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikimą šių paslaugų gavėjui. Nacionalinis kibernetinio saugumo centras apie viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams pagal šį punktą duotus nurodymus ne vėliau kaip kitą darbo dieną praneša Lietuvos Respublikos ryšių reguliavimo tarnybai;

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;

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) (OL 2016 L 119, p. 1) nustatytas priežiūros institucijos užduotis.

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 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 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;

4) turi teisę duoti nurodymą viešųjų 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.

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 skaitmeninės 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, 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.

3. Viešųjų 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 ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų teikiamomis paslaugomis.

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 informacinio tinklo paskirtis – dalytis informacija apie galimus ir įvykusius kibernetinius incidentus, taip pat rekomendacijomis, nurodymais, techniniais sprendimais ir kitomis priemonėmis, užtikrinančiomis kibernetinį saugumą ir kibernetinio saugumo informacinio tinklo narių tarpusavio bendradarbiavimą kibernetinio saugumo srityje.

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.

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
BAIGIAMOSIOS NUOSTATOS

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.

Skelbiu šį Lietuvos Respublikos Seimo priimtą įstatymą.

Respublikos Prezidentė Dalia Grybauskaitė

Lietuvos Respublikos
kibernetinio saugumo įstatymo
priedas

ĮGYVENDINAMI EUROPOS SĄJUNGOS TEISĖS AKTAI

1. 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos (Pagrindų direktyva) (OL 2004 m. *specialusis leidimas*, 13 skyrius, 29 tomas, p. 349) su paskutiniais pakeitimais, padarytais 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/140/EB (OL 2009 L 337, p. 37).

2. 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 (OL 2016 L 194, p. 1).

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