LIETUVOS RESPUBLIKOS VYRIAUSYBĖS KANCELIARIJA
POLITIKOS ĮGYVENDINIMO GRUPĖ

PAŽYMA
DĖL LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMO NR. XII-1428 PAKEITIMO ĮSTATYMO PROJEKTO IR LIETUVOS RESPUBLIKOS ADMINISTRACINIŲ NUSIŽENGIMŲ KODEKSO 479, 480, 589 STRAIPSNIŲ IR PRIEDO PAKEITIMO ĮSTATYMO PROJEKTO

(toliau – Projektai))

(TAP-18-356–18-358) (TAIS NR.18-2648)

2018-03-22 Nr. NV-752

Vilnius

Projektų rengėjas: Krašto apsaugos ministerija.

Projektų tikslas: Įgyvendinti Europos Sąjungos direktyvos, nustatančios priemones aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti, nuostatas, kaip tai būtina įstatymo lygmeniu ir sukurti sąlygas nuostatoms įgyvendinti įgyvendinamųjų teisės aktų lygmeniu.

Dabartinė situacija:

- Europos Parlamentas ir Europos Sąjungos Taryba 2016 m. liepos 6 d. priėmė direktyvą (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (toliau – TIS direktyva), **kurios nuostatos turi būti perkeltos į nacionalinę teisė ne vėliau kaip 2018 m. gegužės 9 d.**
- Nuo 2018 m. gegužės 25 d. įsigalioja Europos Sąjungos reglamentas (ES) 2019/679, dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis duomenų apsaugos reglamentas), todėl esamas Kibernetinio saugumo reguliavimas dėl Valstybinės duomenų apsaugos inspekcijos įgaliojimų tampa perteklinis.

Projektų esmė: Siūloma Kibernetinio saugumo įstatymą išdėstyti nauja redakcijos ir pakeisti Administracinių nusižengimų kodekso tris straipsnius:

- Siūloma perkelti TIS direktyvos nuostatas į Kibernetinio saugumo įstatymą:
  - nustatyti subjektą, tvirtinantį nacionalinę kibernetinio saugumo strategiją;
  - apibrėžti kibernetinio saugumo subjektus ir nustatyti jų pareigas;
  - įtvirtinti nuostatas dėl kibernetinio saugumo rizikos valdymo;
  - stiprinti tarptautinį bendradarbiavimą Europos Sąjungos lygmeniu;
  - įstatymą papildyti naujais kibernetinio saugumo principais (standartizacijos ir technologinio neutralumo)
- Siūloma Kibernetinio saugumo įstatyme panaikinti Valstybinės duomenų apsaugos inspekcijos kompetenciją, užduotis ir įgaliojimus, bei reikalavimus dėl pranešimų apie asmens duomenų saugumo pažeidimus priežiūros institucijoms.
- Siūloma, Kibernetinio saugumo įstatymą dėstant nauja redakcija, jo nuostatas peržiūrėti iš esmės: atsisakyti perteklinių nuostatų, tiksliau apibrėžti subjektų kompetenciją, įstatymą tikslinti teisės technikos aspektu.

- Įgyvendinant TIS direktyvos nuostatas, siūloma išplėsti Administracinių nusižengimų kodekse nustatytų subjektų, kuriems taikoma administracinė atsakomybė už nusižengimų susijusių su ryšių sistemomis, padarymą, ratą:
  - nustatyti administracinę atsakomybę visiems kibernetinio saugumo subjektams už nustatytų organizacinių ir techninių kibernetinio saugumo reikalavimų nesilaikymo;
  - nustatyti administracinę atsakomybę visiems kibernetinio saugumo subjektams už informacijos apie kibernetinio saugumo būklę nepateikimo, kuriems yra nustatyta prievolė šią informaciją teikti.

Atsižvelgiant į tai, kad TIS direktyvos nuostatos turi būti perkeltos į nacionalinę teisę iki 2018 m. gegužės 9 d., siūloma Vyriausybei teikti Seimui svarstyti projektus skubos tvarka. Siūloma Projektais teikiamų įstatymų įsigaliojimo data 2018 m. balandžio 9 d. Vyriausybė ir Krašto apsaugos ministerija iki 2018 m. gegužės 9 d. turi priimti įgyvendinamuosius teisės aktus.

Rengėjų nuomone Projektams įgyvendinti papildomų valstybės biudžeto lėšų nereikės.

Derinimas: Projektai suderinti su Teisingumo ministerija, Europos teisės departamentu prie Teisingumo ministerijos, Valstybine duomenų apsaugos inspekcija. Vidaus reikalų ministerija Projektų vertinimo išvados neteikė. Dėl Europos teisės departamento prie Teisingumo ministerijos ir papildomai gautų asociacijos „Infobalt“ pastabų ir pasiūlymų, į kuriuos neatsižvelgta, pateikta derinimo pažyma. Europos teisės departamento prie Teisingumo ministerijos nuomone, Kibernetinio saugumo įstatyme turėtų būti nustatytos Nacionalinio kibernetinio centro veiklos garantijos (užtikrinami pakankami ištekliai užduočių atlikimui ir prieiga prie tinkamos infrastruktūros), o taip pat nustatyti Nacionaliniam Kibernetinio saugumo centrui atitinkami reikalavimai bei užduotys. Krašto apsaugos ministerijos nuomone visa tai reglamentuoti įstatyme netikslinga. Vyriausybės kanceliarijos Teisės grupė pateikė eilę pastabų ir pasiūlymų.

Atitiktis Vyriausybės programai: Projektai atitinka Vyriausybės programos įgyvendinimo plano 5.2.1. darbo „Kibernetinių incidentų prevencija ir valdymo sistemos tobulinimas“ nuostatas. Projektai įtraukti į Vyriausybės siūlomą Seimo IV (pavasario) sesijos darbų sąrašą.

Dalykinio vertinimo išvada: Siūlome rengėjams patikslinti Projektus įvertinus Vyriausybės kanceliarijos Teisės grupės 2018 m. kovo 21 d. išvadoje Nr. NV-748 pateiktas pastabas ir Projektą svarstyti Vyriausybės posėdžio B dalyje, prieš tai aptarus Tarpinstituciniame pasitarime nesuderintas Teisingumo ministerijos, asociacijos „Infobalt“ ir Vyriausybės kanceliarijos Teisės grupės pastabas.

Politikos įgyvendinimo grupės patarėjas Valdas Kiveris

Valdas Kiveris, tel. 870661805, el. p. valdas.kiveris@lrv.lt

LIETUVOS RESPUBLIKOS
VYRIAUSYBĖS KANCELIARIJA
Teisės akto projekto lydraštis
2018-03-13 Nr. G-2783

LIETUVOS RESPUBLIKOS KRAŠTO APSAUGOS MINISTERIJA

Biudžetinė įstaiga, Totorių g. 25, LT-01121 Vilnius, tel.: (8 5) 273 5501 / 262 4821, faks. (8 5) 264 8517, el. p. kam@kam.lt.
Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 188602751, PVM mokėtojo kodas LT100001016116

Lietuvos Respublikos Vyriausybei

2018-03-12 Nr. 12-01-356

DĖL LIETUVOS RESPUBLIKOS ĮSTATYMŲ PROJEKTŲ ĮVERTINIMO

Lietuvos Respublikos krašto apsaugos ministerija parengė ir teikia išvadoms gauti Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymo projektą (toliau – Kibernetinio saugumo įstatymo projektas) ir Lietuvos Respublikos administracinių nusižengimų kodekso 479, 480, 589 straipsnių ir priedo pakeitimo įstatymo projektą (toliau visi kartu – Įstatymų projektai).

I. Sprendžiama problema	• Europos Parlamentas ir Europos Sąjungos Taryba, atsižvelgdami į Europos Komisijos pasiūlymą, 2016 m. liepos 6 d. priėmė direktyvą (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (toliau – TIS direktyva), kurios nuostatos turi būti perkeltos į nacionalinę teisę ne vėliau kaip 2018 m. gegužės 9 d. • Nuo 2018 m. gegužės 25 d. įsigalioja tiesioginio taikymo teisės aktas – 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis duomenų apsaugos reglamentas), todėl esamas Kibernetinio saugumo įstatymo reguliavimas dėl Valstybinės duomenų apsaugos inspekcijos įgaliojimų tampa perteklinis.
II. Siūlomos priemonės	• Perkelti TIS direktyvos nuostatas į nacionalinę teisę. • Panaikinti reikalavimus dėl pranešimų priežiūros institucijoms apie asmens duomenų saugumo pažeidimus ir priežiūros institucijų kompetenciją, užduotis ir įgaliojimus. • Kibernetinio saugumo įstatymą dėstant nauja redakcija, peržiūrėti jo nuostatas iš esmės: atsisakyti perteklinių nuostatų, tiksliau apibrėžti subjektų kompetenciją, įstatymą tikslinti teisės technikos

100 Atkurtai Lietuvai

	aspektu.
III. Priemonių kaštai	Įstatymams įgyvendinti papildomų valstybės biudžeto lėšų nereikės. Įstatymų projektuose siūlomų pakeitimų įgyvendinimas neturės įtakos žmogiškųjų, infrastruktūros ar finansinių išteklių pokyčiams, nes Nacionaliniam kibernetinio saugumo centrui nustatomas funkcijas numatoma vykdyti naudojantis turimais krašto apsaugos sistemos ištekliais.
IV. Nauda visuomenei	Įstatymo įgyvendinimas turės įtakos kuriant saugesnę kibernetinę erdvę Lietuvos Respublikoje, todėl turėtų sukurti palankesnes verslo sąlygas ir skatinti verslo, naudojančio ryšių ir informacines technologijas, plėtrą.

Įstatymų projektai skelbiami Lietuvos Respublikos Seimo kanceliarijos teisės aktų informacinėje sistemoje. Papildomų konsultacijų su visuomene nenumatoma.

Įstatymų projektai suderinti su Lietuvos Respublikos teisingumo ministerija, Europos teisės departamentu prie Lietuvos Respublikos teisingumo ministerijos, Valstybine duomenų apsaugos inspekcija. Dėl Teisingumo ministerijos, Valstybinės duomenų apsaugos inspekcijos pastabų ir pasiūlymų projektai suderinti darbo tvarka. Atsižvelgta į Europos teisės departamento pastabas, o dėl pastabų, į kurias neatsižvelgta, teikiama derinimo pažyma.

2018 m. vasario 27 d. gautos ir asociacijos „Infobalt“ pastabos ir pasiūlymai. 2018 m. kovo 2 d. surengtas asociacijos „Infobalt“ ir Krašto apsaugos ministerijos atstovų susitikimas, kuriame aptartos pastabos ir pasiūlymai. Dėl pastabų ir pasiūlymų, neaptartų susitikime, teikiama derinimo pažyma.

Įstatyme vartojamos sąvokos suderintos su Krašto apsaugos ministerijos terminų aprobavimo ir vartojimo priežiūros komisija ir pateiktos svarstyti Valstybinei lietuvių kalbos komisijai.

Įstatymų projektai 2018 m. vasario 15 d. teikti derinti ir Lietuvos Respublikos vidaus reikalų ministerijai, tačiau, vadovaujantis Lietuvos Respublikos Vyriausybės darbo reglamento 27 punktu, Vidaus reikalų ministerijos išvada per 12 darbo dienų nebuvo gauta.

Atsižvelgdami į tai, kad TIS direktyvos nuostatos turi būti perkeltos ne vėliau kaip 2018 m. gegužės 9 d., prašome taikyti Lietuvos Respublikos Vyriausybės darbo reglamento 48 punktą ir išvadas dėl Įstatymų projektų pateikti skubos tvarka.

Įstatymų projektus parengė Krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų departamento (direktorius Jonas Skardinskas, tel. 8 706 80 800, el. p. jonas.skardinskas@kam.lt) Kibernetinio saugumo ir elektroninės informacijos saugos skyriaus viršininkas Artūras Litvaitis (tel. 8 706 80 806, el. p. arturas.litvaitis@kam.lt) ir Krašto apsaugos ministerijos Teisės departamento (direktorė Judita Nagienė, tel. (8 5) 273 5545, el. p. judita.nagiene@kam.lt) Teisėkūros skyriaus (viršininkė Inga Šilinytė, tel. (8 5) 273 5563, el. p. inga.silinyte@kam.lt) vyr. specialistas Mantas Keliotis (tel. (8 5) 273 5597, el. p. mantas.keliotis@kam.lt).

PRIDEDAMA:

1. Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymo projektas, 11 lapų.

2. Lietuvos Respublikos administracinių nusižengimų kodekso 479, 480, 589 straipsnių ir priedo pakeitimo įstatymo projektas, 2 lapai.

3. Lietuvos Respublikos administracinių nusižengimų kodekso 479, 480, 589 straipsnių ir priedo pakeitimo įstatymo projekto lyginamasis variantas, 3 lapai.

4. Aiškinamasis raštas, 9 lapai.

5. 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyvos (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti ir nacionalinių teisės aktų atitikties lentelė, 43 lapai.

6. Lietuvos Respublikos Vyriausybės nutarimo „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymo ir Lietuvos Respublikos administracinių nusižengimų kodekso 479, 480, 589 straipsnių ir priedo pakeitimo įstatymo projektų pateikimo Lietuvos Respublikos Seimui“ projektas, 1 lapas.

7. Derinimo pažyma, 5 lapai.

Užsienio reikalų ministras, pavaduojantis
krašto apsaugos ministrą Linas Antanas Linkevičius

A. Litvaitis, tel. 8 706 80 806, el. p. arturas.litvaitis@kam.lt
M. Keliotis, tel. (8 5) 273 5597, el. p. mantas.keliotis@kam.lt

LIETUVOS RESPUBLIKOS
VYRIAUSYBĖS KANCELIARIJA
Teisės akto projektas
2018-03-13 Nr. TAP-18-358
TAIS Nr. 18-2648

Projektas

LIETUVOS RESPUBLIKOS VYRIAUSYBĖ

NUTARIMAS
DĖL LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMO NR. XII-1428 PAKEITIMO ĮSTATYMO IR LIETUVOS RESPUBLIKOS ADMINISTRACINIŲ NUSIŽENGIMŲ KODEKSO 479, 480, 589 STRAIPSNIŲ IR PRIEDO PAKEITIMO ĮSTATYMO PROJEKTŲ PATEIKIMO LIETUVOS RESPUBLIKOS SEIMUI

Nr.
Vilnius

Lietuvos Respublikos Vyriausybė n u t a r i a:

1. Pritarti Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymo ir Lietuvos Respublikos administracinių nusižengimų kodekso 479, 480, 589 straipsnių ir priedo pakeitimo įstatymo projektams ir pateikti juos Lietuvos Respublikos Seimui.

2. Atsižvelgiant į tai, kad, vadovaujantis 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyvos (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti 25 straipsnio 1 dalimi, teisės aktai, įgyvendinantys šią direktyvą, turi įsigalioti 2018 m. gegužės 9 d., prašyti Lietuvos Respublikos Seimą svarstyti nurodytus įstatymų projektus skubos tvarka.

3. Įgalioti krašto apsaugos ministrą Raimundą Karoblį, o jam negalint dalyvauti – krašto apsaugos viceministrą Edviną Kerzą atstovauti Lietuvos Respublikos Vyriausybei, svarstant nurodytus įstatymų projektus Lietuvos Respublikos Seime.

Ministras Pirmininkas

Krašto apsaugos ministras

Užsienio reikalų ministras
Linas Linkevičius

Krašto apsaugos ministerijos
Teisės departamento direktorė
Judita Nagienė

KAM
Dokumentų ad
skyriaus vyr
Jurg
Redagavo
Birutė Kulitienė

Krašto apsaugos viceministras
Vytautas Um

LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMO NR. XII-1428 PAKEITIMO ĮSTATYMO IR LIETUVOS RESPUBLIKOS ADMINISTRACINIŲ NUSIŽENGIMŲ KODEKSO 479, 480, 589 STRAIPSNIŲ IR PRIEDO PAKEITIMO ĮSTATYMO PROJEKTŲ AIŠKINAMASIS RAŠTAS

1. Įstatymų projektų rengimą paskatinusios priežastys, parengtų projektų tikslai ir uždaviniai

Europos Parlamentas ir Europos Sąjungos Taryba, atsižvelgdami į Europos Komisijos pasiūlymą, 2016 m. liepos 6 d. priėmė direktyvą (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (toliau – TIS direktyva). TIS direktyva siekiama nustatyti priemones aukštam bendram tinklų ir informacinių sistemų saugumo lygiui Sąjungoje užtikrinti, kad būtų pagerintas vidaus rinkos veikimas, o įgyvendinant šį tikslą TIS direktyva:

1) visoms valstybėms narėms nustatomos pareigos priimti nacionalinę tinklų ir informacinių sistemų saugumo strategiją;

2) sukuriama Bendradarbiavimo grupė, kad būtų remiamas ir lengvinamas valstybių narių strateginis bendradarbiavimas ir keitimasis informacija, taip pat didinama jų atsakomybė ir tarpusavio pasitikėjimas;

3) sukuriamas Reagavimo į kompiuterinius saugumo incidentus tarnybų tinklas, kad būtų prisidedama prie valstybių narių atsakomybės ir tarpusavio pasitikėjimo didinimo ir skatinamas greitas bei veiksmingas operatyvinis bendradarbiavimas;

4) nustatomi saugumo ir pranešimo reikalavimai esminių paslaugų operatoriams ir skaitmeninių paslaugų teikėjams;

5) nustatomos valstybių narių pareigos paskirti nacionalines kompetentingas institucijas, bendruosius informacinius centrus ir reagavimo į kibernetinius incidentus tarnybas, kuriems pavedamos užduotys, susijusios su tinklų ir informacinių sistemų saugumu.

TIS direktyvos nuostatos turi būti perkeltos į nacionalinę teisę ne vėliau kaip 2018 m. gegužės 9 d.

Siekdama įgyvendinti TIS direktyvos nuostatas, Lietuvos Respublikos krašto apsaugos ministerija parengė šiuos įstatymų pakeitimų projektus: Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymo projektą (toliau – Kibernetinio saugumo įstatymo projektas) ir Lietuvos Respublikos administracinių nusižengimų kodekso 479, 480, 589 straipsnių ir priedo pakeitimo įstatymo projektą (toliau – ANK projektas) (toliau kartu – Įstatymų projektai). Įstatymų projektais siekiama įgyvendinti TIS direktyvos nuostatas, kaip tai būtina įstatymo lygmeniu, ir sukurti sąlygas nuostatoms įgyvendinti įgyvendinamųjų teisės aktų lygmeniu.

Pastebėtina, kad Įstatymų projektais nesiekiama įgyvendinti TIS direktyvos nuostatų visa direktyvos apimtimi. Pirma, tam tikros TIS direktyvos nuostatos savo esme sutampa su jau galiojančiomis Kibernetinio saugumo įstatymo nuostatomis, todėl neturi būti iš naujo perkeltos į nacionalinę teisę. Antra, Kibernetinio saugumo įstatymas nėra vienintelė priemonė TIS direktyvos nuostatoms įgyvendinti, šiuo tikslu keičiami ir kiti nacionaliniai teisės aktai. Platesnė informacija pateikiama pridedamoje atitikties lentelėje.

Įgyvendinant nurodytą Įstatymų projektų tikslą, nustatomi šie Kibernetinio saugumo įstatymo pakeitimo projekto uždaviniai:

1. Nustatyti subjektą, tvirtinantį nacionalinę kibernetinio saugumo strategiją.
2. Apibrėžti kibernetinio saugumo subjektus ir nustatyti jų pareigas.
3. Įtvirtinti nuostatas dėl kibernetinio saugumo rizikos valdymo.
4. Stiprinti tarptautinį bendradarbiavimą Europos Sąjungos (toliau – ES) lygmeniu.
5. Kibernetinio saugumo įstatymą papildyti naujais principais.

Įgyvendinant nurodytą Įstatymų projektų tikslą, nustatomi šis ANK projekto uždavinys: išplėsti subjektų, kuriems taikoma administracinė atsakomybė už administracinių nusižengimų, susijusių su ryšių sistema, padarymą, ratą.

Be to, 2018 m. gegužės 25 d. įsigalioja tiesioginio taikymo teisės aktas – 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis duomenų apsaugos reglamentas), nustatantis reikalavimus dėl pranešimų priežiūros institucijoms apie asmens duomenų saugumo pažeidimus ir priežiūros institucijų kompetenciją, užduotis ir įgaliojimus. Įsigaliojus nurodytam reglamentui, esamas Kibernetinio saugumo įstatymo reguliavimas dėl Valstybinės duomenų apsaugos inspekcijos įgaliojimų tampa perteklinis. Atsižvelgiant į tai ir turint galvoje atliekamų Kibernetinio saugumo įstatymo pakeitimų, įgyvendinant TIS direktyvą, aprėptį, Kibernetinio saugumo įstatymo projektu siekiama persvarstyti Kibernetinio saugumo įstatymą iš esmės.

Siekiant nurodyto tikslo, nustatomi šie Kibernetinio saugumo įstatymo pakeitimo projekto uždaviniai:

1. Atsisakyti perteklinių Kibernetinio saugumo įstatymo nuostatų.
2. Tiksliau apibrėžti kibernetinio saugumo politiką formuojančių ir įgyvendinančių institucijų kompetenciją.
3. Patikslinti Kibernetinio saugumo įstatymą teisės technikos aspektu.

2. Įstatymų projektų iniciatoriai (institucija, asmenys ar piliečių įgalioti atstovai) ir rengėjai

Kibernetinio saugumo įstatymo pakeitimo projekto rengimą inicijavo Krašto apsaugos ministerija. Šį projektą parengė Krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų departamento (direktorius Jonas Skardinskas, tel. 8 706 80 800, el. p. jonas.skardinskas@kam.lt) Kibernetinio saugumo ir elektroninės informacijos saugos skyriaus viršininkas Artūras Litvaitis (tel. 8 706 80 806, el. p. arturas.litvaitis@kam.lt) ir Krašto apsaugos ministerijos Teisės departamento (direktorė Judita Nagienė, tel. (8 5) 273 5545, el. p. judita.nagiene@kam.lt) Teisėkūros skyriaus (viršininkė Inga Šilinytė, tel. (8 5) 273 5563, el. p. inga.silinyte@kam.lt) vyr. specialistas Mantas Keliotis (tel. (8 5) 273 5597, el. p. mantas.keliotis@kam.lt).

3. Kaip šiuo metu yra reguliuojami įstatymų projektuose aptarti teisiniai santykiai

Dėl Nacionalinės kibernetinio saugumo strategijos

1. Kibernetinio saugumo įstatymo 4 straipsnio 1 dalyje numatoma, kad kibernetinio saugumo politikos strateginius tikslus ir jiems pasiekti būtinas priemones nustato Lietuvos Respublikos Vyriausybė, tačiau nenustatyta, kuri institucija tvirtina nacionalinę kibernetinio saugumo strategiją, kaip to reikalauja TIS direktyvos 1 straipsnio 2 dalies a punktas ir 7 straipsnis.

Dėl kibernetinio saugumo subjektų

2. Kibernetinio saugumo įstatymo 1 straipsnio 2 dalis įtvirtina kibernetinio saugumo dalyvius. Jais laikomi: valstybės institucijos, formuojančios ir įgyvendinančios kibernetinio saugumo politiką, viešojo administravimo subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai ir elektroninės informacijos prieglobos paslaugų teikėjai, informacinių technologijų srityje veiklą vykdantys verslo subjektai, mokslo ir studijų institucijos. Nors TIS direktyvos 1 straipsnio 2 dalies d punktas ir numato pareigas skaitmeninių paslaugų teikėjams, toks subjektas Kibernetinio saugumo įstatyme nenumatytas.

3. Kibernetinio saugumo įstatymo 2 straipsnio 2 dalis ir 14 straipsnis nustato ypatingos svarbos informacinės infrastruktūros valdytojus, kaip subjektų grupę, kuriai keliami aukštesni nei kitiems subjektams kibernetinio saugumo reikalavimai. TIS direktyvos 1 straipsnio 2 dalies d punktas nustato saugumo reikalavimus esminių paslaugų operatoriams, kurie pagal identifikavimo kriterijus ir jiems keliamus saugumo reikalavimus nacionalinėje teisėje atitinka ypatingos svarbos informacinės infrastruktūros valdytojus. Pažymėtina, kad nacionalinėje teisėje tikslinga toliau

vartoti tarptautinėje praktikoje plačiau naudojamą ypatingos svarbos (kritinės) informacinės infrastruktūros sąvoką.

Dėl kibernetinio saugumo rizikos

4. TIS direktyvos 14 straipsnio 1 dalyje nurodoma, kad valstybės narės turi užtikrinti, kad esminių paslaugų operatoriai imtųsi tinkamų ir proporcingų techninių ir organizacinių priemonių, kad galėtų valdyti riziką, kylančią tinklų ir informacinių sistemų, kuriais jie naudojasi vykdydami savo veiklą, saugumui. Kibernetinio saugumo įstatymo III skyriuje viešojo administravimo subjektams, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams, elektroninės informacijos prieglobos paslaugų teikėjams nustatoma pareiga įgyvendinti kibernetinio saugumo reikalavimus. Kibernetinio saugumo įstatymo įgyvendinamieji teisės aktai nustato, kad kibernetinio saugumo dalyviai gali taikyti ir papildomas kibernetinio saugumo priemones, tačiau pažymėtina, kad nenustatoma pareiga įvertinti kibernetinio saugumo riziką ir taikyti proporcingas įvertintai rizikai kibernetinio saugumo priemones.

Dėl tarptautinio bendradarbiavimo stiprinimo ES lygmeniu

5. Kibernetinio saugumo įstatymo 17 ir 18 straipsniuose nustatoma sąveika tarp nacionalinių institucijų, tačiau TIS direktyva (14 straipsnio 5 dalis) ir kiti ES teisės aktai akcentuoja tarpvalstybinio ir ES lygmens bendradarbiavimo svarbą valdant didelio poveikio kibernetinius incidentus, kurių šalis negali savarankiškai suvaldyti, arba incidentus, kurių neigiamas poveikis apima daugiau nei vieną valstybę narę, o tai pagal esamą teisinį reguliavimą nenumatyta. Kibernetinio saugumo įstatymo 2 straipsnio 4 dalis nustato kibernetinio incidento sąvoką, tačiau plačiau kibernetinių incidentų samprata nedetalizuojama, kas yra didelio poveikio kibernetinis incidentas, neaiškinama.

Dėl kibernetinio saugumo principų

6. Kibernetinio saugumo įstatymo 3 straipsnyje yra įtvirtinti trys kibernetinio saugumo principai (kibernetinės erdvės nediskriminavimo, kibernetinio saugumo proporcingumo ir viešojo intereso viršenybės). Nors TIS direktyva tiesiogiai ir nenustato pareigos įtvirtinti naujus kibernetinio saugumo principus, atsižvelgiant į besikeičiantį kibernetinio saugumo teisinį reguliavimą, esamų principų nebepakanka.

Dėl subjektų, kuriems taikoma administracinė atsakomybė už administracinių nusižengimų, susijusių su ryšių sistema

7. TIS direktyvos 21 straipsnis nustato pareigą valstybėms narėms nustatyti sankcijas, taikomas pažeidus TIS direktyvos nuostatas. Administracinių nusižengimo kodekso 479 straipsnio 3 dalyje atsakomybė už informacijos, reikalingos vertinti šių kibernetinio saugumo subjektų ir jų ryšių ir informacinių sistemų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams ir kibernetinio saugumo būklę, nepateikimą nustatoma tik viešųjų ryšių tinklų ir viešųjų elektroninių ryšių paslaugų, elektroninės prieglobos paslaugų teikėjams, o 480 straipsnio 4 dalyje atsakomybė už ryšių ir informacinių sistemų neatitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams nustatoma tik ypatingos svarbos informacinės infrastruktūros valdytojams ir elektroninės informacijos prieglobos paslaugų teikėjams. Galiojantis teisinis reguliavimas neapima visų kibernetinio saugumo subjektų, kuriems taikomos Kibernetinio saugumo įstatymo nuostatos, įgyvendinančios TIS direktyvą.

Dėl perteklinių Kibernetinio saugumo įstatymo nuostatų

8. Kibernetinio saugumo įstatymo 11 straipsnyje nustatomi įgaliojimai Valstybinei duomenų apsaugos inspekcijai atlikti juridinių asmenų patikrinimus, kai yra rizikos, kad kibernetiniai incidentai gali turėti įtakos asmens duomenų apsaugai, tikrinti asmens duomenų tvarkymo teisėtumą ir priimti sprendimus dėl asmens duomenų tvarkymo pažeidimų kibernetinėje erdvėje, teikti

visuomenei ir suinteresuotoms institucijoms informaciją apie kibernetinio saugumo, susijusio su asmens duomenų apsauga, rizikos veiksnius, pavojus ir grėsmes kibernetinėje erdvėje, nustatyti informacijos apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones pateikimo tvarką. Kibernetinio saugumo įstatymas taip pat nustato pareigą viešojo administravimo subjektams, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams teikti Valstybinei duomenų apsaugos inspekcijai informaciją apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones šios institucijos nustatyta tvarka ir sąlygomis. Atsižvelgiant į tai, kad 2018 m. gegužės 25 d. įsigalioja tiesioginio taikymo teisės aktas Bendrasis duomenų apsaugos reglamentas, nustatantis reikalavimus dėl pranešimų priežiūros institucijoms apie asmens duomenų saugumo pažeidimus ir priežiūros institucijų kompetenciją, užduotis ir įgaliojimus, esamos teisinio reguliavimo nuostatos tampa perteklinės.

9. Kibernetinio saugumo įstatymo 9 straipsnyje nustatomos Nacionalinio kibernetinio saugumo centro, kaip įstaigos prie ministerijos, funkcijos, teisės ir pareigos. Pažymėtina, kad Lietuvos Respublikos civilinio kodekso 2.47 straipsnyje, Lietuvos Respublikos biudžetinių įstaigų 6 straipsnyje įtvirtinta, kad būtent biudžetinės įstaigos nuostatuose turėtų būti nurodomi biudžetinės įstaigos veiklos tikslai ir funkcijos, o Konstitucinis teismas savo jurisprudencijoje yra pažymėjęs, kad įstatymais turi būti reguliuojami tik svarbiausi visuomenės gyvenimo klausimai. Atsižvelgiant į tai, siūlytina atsisakyti Nacionalinio kibernetinio saugumo centro funkcijų, kurios nesusijusios su svarbiausiais visuomenės gyvenimo klausimais.

Dėl kibernetinio saugumo politiką formuojančių ir įgyvendinančių institucijų

10. Nustatoma, kad Valstybinė duomenų apsaugos inspekcija ir Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Policijos departamentas) formuojant kibernetinio saugumo politiką dalyvauja tiek, kiek šiame Kibernetinio saugumo įstatyme nustatytoms funkcijoms atlikti reikia nustatyti viešojo administravimo subjektų, valdančių valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų veiklos teisinį reguliavimą. Lietuvos Respublikos valstybės tarnybos įstatymo 2 priede išaiškinama, kad dalyvavimas formuojant valstybės politiką suprantamas kaip valstybės institucijų ir įstaigų veikla, vykdoma darant poveikį rengiamų sprendimų projektų kokybei, vykdant vieną ar kelias aiškiai apibrėžtas funkcijas (siūlymų teikimo, sprendimų derinimo, sprendimų nagrinėjimo, išvadų formulavimo, analizių atlikimo), susijusias su sprendimų projektų rengimu. Analizuojant pateiktą išaiškinimą ir lyginant jį su Valstybinės duomenų apsaugos inspekcijos ir Policijos departamento atliekamomis funkcijomis kibernetinio saugumo srityje matyti, kad šios institucijos nedalyvauja formuojant kibernetinio saugumo politiką.

11. Kibernetinio saugumo įstatymo 4 straipsnio 3 dalyje nustatoma, kad viena iš kibernetinio saugumo politiką įgyvendinančių institucijų yra Policijos departamentas. Atsižvelgiant į tai, kad praktikoje kibernetinių incidentų tyrimu užsiima Lietuvos kriminalinės policijos biuras, kuris neįeina į Policijos departamento sudėtį, daroma išvada, kad esamas teisinis reguliavimas nėra tikslus.

12. Kibernetinio saugumo įstatymo 5 straipsnio 5 punktas nustato, kad Vyriausybė tvirtina tipinius kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus. Tipinis kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planas yra metodinė priemonė ypatingos svarbos informacinės infrastruktūros valdytojams rengiant savo kibernetinių incidentų valdymo planus, todėl laikytina, kad tokio pobūdžio teisės aktas neturėtų būti nustatomas Vyriausybės nutarimu.

4. Kokios siūlomos naujos teisinio reguliavimo nuostatos ir kokių teigiamų rezultatų laukiama

Dėl Nacionalinės kibernetinio saugumo strategijos

1. Kibernetinio saugumo įstatymo 6 straipsnio 1 punkte siūloma nustatyti pareigą Lietuvos Respublikos Vyriausybei nustatyti kibernetinio saugumo politikos strateginius tikslus, prioritetus ir jiems pasiekti būtinas priemones, pavedant Vyriausybei tvirtinti Nacionalinę kibernetinio saugumo strategiją. Taip būtų apibrėžiama Vyriausybės pareiga nustatyti kibernetinio saugumo politikos strateginius tikslus, prioritetus ir jiems pasiekti būtinas priemones.

Dėl kibernetinio saugumo subjektų

2. Kibernetinio saugumo įstatymą siūloma papildyti nauja 2 straipsnio 13 dalimi, kuria būtų nustatoma kibernetinio saugumo subjektų sąvoka. Taip būtų tiksliau apibrėžiami kibernetinio saugumo procese dalyvaujantys subjektai, nustatoma atskirtis tarp kibernetinio saugumo politiką formuojančių, įgyvendinančių institucijų ir subjektų, kuriems nustatomi reikalavimai, užtikrinantys kibernetinį saugumą.

3. Kibernetinio saugumo įstatyme siūloma nustatyti papildomą kibernetinio saugumo subjektų – skaitmeninių paslaugų teikėjų – kategoriją (2 straipsnio 17 dalyje), taip pat skaitmeninių paslaugų tiekėjams nustatyti TIS direktyvos nuostatas atitinkančias pareigas (12 straipsnis ir 13 straipsnio 5 dalis). Atsižvelgiant į tai, kad TIS direktyvoje skaitmeninių paslaugos suprantamos kaip elektroninės prekyvietės, interneto paieškos sistemos, debesijos kompiuterijos paslaugų visuma, Kibernetinio saugumo įstatymą siūloma papildyti debesijos paslaugų (2 straipsnio 1 dalis), elektroninės prekyvietės (2 straipsnio 3 dalis), interneto paieškos sistemos (2 straipsnio 4 dalis) sąvokomis, nenustatytomis kituose nacionaliniuose teisės aktuose.

4. TIS direktyvoje numatoma pareiga skaitmeninių paslaugų teikėjams turėti oficialų atstovą tuo atveju, jei skaitmeninių paslaugų teikėjas, kuris nėra įsisteigęs ES, teikia skaitmenines paslaugas ES teritorijoje. Atstovas turi būti įsisteigęs vienoje iš tų valstybių narių, kuriose teikiamos paslaugos. Atsižvelgiant į tai, Kibernetinio saugumo įstatyme siūloma nustatyti pareigą skaitmeninių paslaugų teikėjams, kurie nėra įsisteigę ES, bet teikia skaitmenines paslaugas Lietuvos Respublikos teritorijoje, skirti oficialų atstovą ES skaitmeninių paslaugų teikėjo vardu (13 straipsnio 5 dalies 2 punktas). Pastebėtina, kad šios pareigos vykdymą planuojama užtikrinti tiesiogiai neveikiant skaitmeninio paslaugų teikėjo. TIS direktyvoje nustatoma, kad skaitmeninių paslaugų teikėjų atžvilgiu turėtų būti vykdoma negriežta ir reaguojamoji *ex post* priežiūra, todėl atitinkama kompetentinga institucija veiksmų turėtų imtis po įvykusio incidento. Atsižvelgiant į tai, organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose planuojama nustatyti pareigą subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ir ypatingos svarbos informacinės infrastruktūros valdytojams nesinaudoti paslaugomis to skaitmeninių paslaugų teikėjo, kuris neįsteigęs oficialaus atstovo ES.

5. Siekiant išvengti incidentų arba efektyviau valdyti vykstančius incidentus ir įgyvendinant TIS direktyvos nuostatas (16 straipsnio 7 dalis), Kibernetinio saugumo įstatyme siūloma nustatyti pareigą Nacionaliniam kibernetinio saugumo centrui, pasikonsultavus su apie kibernetinį incidentą pranešančiu kibernetinio saugumo subjektu, informuoti visuomenę apie pavienius incidentus arba reikalauti, kad tai padarytų kibernetinio saugumo subjektas (9 straipsnio 2 dalies 10 punktas).

6. Įgyvendinant TIS direktyvos nuostatas (15 straipsnis), siūloma nustatyti Nacionalinio kibernetinio saugumo centro teisę reikalauti, kad kibernetinio saugumo subjektai teiktų informaciją, reikalingą jų ryšių ir informacinių sistemų kibernetiniam saugumui įvertinti ir duoti privalomus nurodymus pašalinti kibernetinio saugumo reikalavimų įgyvendinimo trūkumus (9 straipsnio 2 dalies 2, 4 ir 5 punktai).

Dėl kibernetinio saugumo subjektų pareigos įvertinti kibernetinio saugumo riziką ir taikyti proporcingas įvertintai rizikai kibernetinio saugumo priemones

7. Kibernetinio saugumo įstatymo 3 straipsnio 1 dalies 2 punkte siūloma įtvirtinti naują – kibernetinio saugumo rizikos valdymo principą. Principo esmė, kad taikomos kibernetinio saugumo priemonės turi užtikrinti kibernetinio saugumo subjektų reguliariai įvertinamos rizikos suvaldymą. Kibernetinio saugumo įstatyme papildomų reikalavimų, nustatančių pareigą atlikti rizikos vertinimą ir taikyti juo pagrįstas papildomų techninių ir organizacinių kibernetinio saugumo priemones,

nenumatoma. Tokio pobūdžio reikalavimą siūloma nustatyti organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose.

8. Papildomai prie jau nustatytos kibernetinio saugumo subjektų pareigos užtikrinti šių subjektų valdomų ir tvarkomų ryšių ir informacinių sistemų atitiktį Vyriausybės nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams siūloma nustatyti pareigą atlikti rizikos vertinimą ir, atsižvelgiant į rizikos vertinimo rezultatus, įdiegti kitas naujausiais technikos laimėjimais paremtas ir proporcingas nustatytai rizikai technines ir organizacines kibernetinio saugumo priemones.

Dėl tarptautinio bendradarbiavimo stiprinimo ES lygmeniu

9. Siekiant nustatyti teisinį pagrindą nacionalinių ir tarptautinių organizacijų, kurių narė yra Lietuvos Respublika, krizių valdymo sistemų sąveikai didelio masto kibernetinių incidentų metu, siūloma Kibernetinio saugumo įstatymą papildyti kibernetinio saugumo krizės sąvoka (2 straipsnio 11 dalis) ir nustatyti atsakomybę Vyriausybei vadovauti kibernetinio saugumo krizių valdymui (6 straipsnio 6 punktas), o Krašto apsaugos ministerijai ir nacionaliniam kibernetinio saugumo centrui – dalyvauti valdant kibernetinio saugumo krizes (atitinkamai 7 straipsnio 10 punktas ir 9 straipsnio 2 dalies 9 punktas).

Dėl kibernetinio saugumo principų

10. Įtvirtinant kibernetinio saugumo subjektų pareigą įvertinti kibernetinio saugumo riziką ir taikyti proporcingas įvertintai rizikai kibernetinio saugumo priemones, TIS direktyva skatinama, kad valstybės narės šią pareigą įgyvendintų vienodai (19 straipsnio 1 dalis). Atsižvelgiant į tai, Kibernetinio saugumo įstatymo 3 straipsnyje nustatomi kibernetinio saugumo principai papildomi standartizacijos ir technologinio neutralumo principu, skatinančiu vadovautis nacionaliniais, ES ir kitais tarptautiniais ryšių ir informacinių sistemų kibernetinio saugumo standartais ir specifikacijomis, nereikalaujant taikyti kokios nors konkrečios rūšies technologijos ir nesuteikiant jai pirmenybės.

11. Atsižvelgiant į besikeičiantį kibernetinio saugumo teisinį reguliavimą, kibernetinio saugumo principų sąrašą siūloma papildyti ir subsidiarumo principu, kurio esmė: už ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinį saugumą yra atsakingi šias sistemas valdantys ir paslaugas teikiantys kibernetinio saugumo subjektai, o srityse, kurios priklauso išimtinai kibernetinio saugumo subjektų kompetencijai, kibernetinio saugumo politiką formuojančios ir įgyvendinančios institucijos veiksmų imasi tik tada, kai ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinio saugumo negali užtikrinti šias sistemas valdantys ir paslaugas teikiantys kibernetinio saugumo subjektai.

Dėl subjektų, kuriems taikoma administracinė atsakomybė už administracinius nusižengimus, susijusius su ryšių ir informacinių sistemų atitiktimi kibernetinio saugumo reikalavimams

12. Administracinių nusižengimų kodekso 479 straipsnio 3 dalyje siūloma nustatyti administracinę atsakomybę už informacijos, reikalingos vertinant šių kibernetinio saugumo subjektų ir jų ryšių ir informacinių sistemų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams ir kibernetinio saugumo būklę, nepateikimą visiems kibernetinio saugumo subjektams, kuriems yra duodamas nurodymas pateikti informaciją, ir jie tokios informacijos nepateikia.

13. Siūloma pakeisti Administracinių nusižengimų kodekso 480 straipsnio 4 dalį ir nustatyti administracinę atsakomybę visiems kibernetinio saugumo subjektams už nustatytų organizacinių ir techninių kibernetinio saugumo reikalavimų nesilaikymą.

14. Atsižvelgiant į siūlomus Administracinių nusižengimų kodekso 479 ir 480 straipsnių pakeitimus, siūloma keisti Administracinių nusižengimų kodekso 589 straipsnį, kuriame atsispindėtų 479 ir 480 straipsniuose atliekami pakeitimai.

15. Siūlomomis priemonėmis tikimasi užtikrinti kibernetinio saugumo reikalavimų,

nustatomų kibernetinio saugumo subjektams, laikymąsi.

Dėl perteklinių Kibernetinio saugumo įstatymo nuostatų

16. 2018 m. gegužės 25 d. įsigalioja Bendrasis duomenų apsaugos reglamentas, jam įsigaliojus esamas Kibernetinio saugumo įstatymo reguliavimas dėl Valstybinės duomenų apsaugos inspekcijos įgaliojimų tampa perteklinis, o TIS direktyvos nuostatas būtina įgyvendinti iki 2018 m. gegužės 9 d., taigi susidaro situacija, kad neilgai trukus po įstatymo įsigaliojimo tam tikros Kibernetinio saugumo įstatymo nuostatos taptų perteklinės, nes būtų reguliuojamos tiesioginio taikymo Bendrajame duomenų apsaugos reglamente. Atsižvelgiant į tai, į Kibernetinio saugumo įstatymo pakeitimo projektą siūloma įtraukti papildomas kai kurių įstatymo straipsnių įsigaliojimo nuostatas, kuriomis būtų panaikinti reikalavimai dėl pranešimų priežiūros institucijoms apie asmens duomenų saugumo pažeidimus ir priežiūros institucijų kompetenciją, užduotis ir įgaliojimus.

17. Kibernetinio saugumo įstatymą dėstant nauja redakcija, siūloma atsisakyti Nacionalinio kibernetinio saugumo centro funkcijų, kurios pagal savo svarbą neturėtų būti reguliuojamos įstatymu. Įstatyme siūloma reguliuoti tik nuostatas, susijusias su kibernetinio saugumo užtikrinimo priemonių naudojimu, kibernetinio saugumo subjektų kontrole, asmens duomenų tvarkymu, tarptautiniu bendradarbiavimu ir bendradarbiavimu plėtojant projektus, stiprinančius nacionalinį kibernetinį saugumą.

Dėl kibernetinio saugumo politiką formuojančių ir įgyvendinančių institucijų

18. Kibernetinio saugumo įstatyme siūloma patikslinti teisinį reguliavimą dėl dalyvavimo formuojant kibernetinio saugumo politiką ir nustatyti, kad tai atlieka tik Nacionalinis kibernetinio saugumo centras (5 straipsnio 2 dalis).

19. Atsižvelgiant į tai, kad kibernetinių incidentų tyrimu užsiima Lietuvos kriminalinės policijos biuras, kuris neįeina į Policijos departamento sudėtį, siūloma keisti esamą teisinį reguliavimą dėl kibernetinio saugumo politiką įgyvendinančių institucijų, nustatant, kad tai atlieka ne Policijos departamentas, o policija (5 straipsnio 3 dalis). Lietuvos Respublikos policijos įstatymo 2 straipsnio 4 dalyje nustatyta, kad policija – tai asmens, visuomenės saugumą ir viešąją tvarką užtikrinanti policijos įstaigų ir policijos pareigūnų sistema. Atsižvelgiant į tai, policijos samprata yra platesnė, apimanti visas policijos įstaigas, teisiškai tiksliau būtų laikyti policiją kibernetinio saugumo politiką įgyvendinančia institucija.

20. Atsižvelgiant į tai, kad tipinis kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planas yra metodinė priemonė ypatingos svarbos informacinės infrastruktūros valdytojams rengiant savo kibernetinių incidentų valdymo planus, siūloma tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano tvirtinimą perduoti Krašto apsaugos ministerijai (7 straipsnio 6 punktas).

5. Numatomo teisinio reguliavimo poveikio vertinimo rezultatai (jeigu rengiant įstatymų projektus toks vertinimas turi būti atliktas ir jo rezultatai nepateikiami atskiru dokumentu), galimos neigiamos priimtų įstatymų pasekmės ir kokių priemonių reikėtų imtis, kad tokių pasekmių būtų išvengta

Numatomo teisinio reguliavimo poveikio vertinimas neatliekamas. Priėmus Įstatymų projektus, galima situacija, kad dėl nustatytos pareigos atlikti rizikos vertinimą ir diegti papildomas kibernetinio saugumo priemones išaugs kai kurių kibernetinio saugumo subjektų išlaidos užtikrinant jų valdomų ir (ar) tvarkomų ryšių ir informacinių sistemų kibernetinį saugumą.

6. Kokią įtaką priimti įstatymai turės kriminogeninei situacijai, korupcijai

Įstatymų projektai neturės įtakos kriminogeninei situacijai ir korupcijai.

7. Kaip įstatymų įgyvendinimas atsilieps verslo sąlygoms ir jo plėtrai

Įstatymų įgyvendinimas turės įtakos kuriant saugesnę kibernetinę erdvę Lietuvos Respublikoje, todėl turėtų sukurti palankesnes verslo sąlygas ir skatinti verslo, naudojančio ryšių ir informacines technologijas, plėtrą.

8. Įstatymų pakeitimo projektų inkorporavimas į teisinę sistemą, kokius teisės aktus būtina priimti, kokius galiojančius teisės aktus reikia pakeisti ar pripažinti netekusiais galios

Kartu su Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymo projektu teikiamas ir Lietuvos Respublikos administracinių nusižengimų kodekso 479, 480, 589 straipsnių ir priedo pakeitimo įstatymo projektas.

9. Ar įstatymo projektai parengti laikantis Lietuvos Respublikos valstybinės kalbos, Teisėkūros pagrindų įstatymų reikalavimų, o įstatymų projektų sąvokos ir jas įvardijantys terminai įvertinti Terminų banko įstatymo ir jo įgyvendinamųjų teisės aktų nustatyta tvarka

Įstatymų projektai parengti laikantis Lietuvos Respublikos valstybinės kalbos įstatymo, Lietuvos Respublikos teisėkūros pagrindų įstatymo reikalavimų. Įstatymų projektuose keičiamos ir nustatomos sąvokos yra įvertintos Terminų banko įstatymo ir jo įgyvendinamųjų teisės aktų nustatyta tvarka.

10. Ar įstatymų projektai atitinka Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos nuostatas ir Europos Sąjungos dokumentus

Įstatymų projektai atitinka Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos nuostatas ir ES dokumentus.

11. Jeigu įstatymui įgyvendinti reikia įgyvendinamųjų teisės aktų, – kas ir kada juos turėtų priimti

Įstatymui įgyvendinti Krašto apsaugos ministerija iki 2018 m. gegužės 9 d. parengs šiuos teisės aktų projektus:

1) Lietuvos Respublikos Vyriausybės 2016 m. sausio 25 d. nutarimo Nr. 87 „Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“ pakeitimo projektą;

2) Lietuvos Respublikos Vyriausybės 2016 m. liepos 20 d. nutarimo Nr. 742 „Dėl Ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos patvirtinimo“ pakeitimo projektą;

3) Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimo Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“ pakeitimo projektą;

4) Lietuvos Respublikos Vyriausybės 2016 m. liepos 20 d. nutarimo Nr. 746 „Dėl Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano patvirtinimo“ pripažinimo netekusiu galios projektą;

5) krašto apsaugos ministro įsakymu tvirtinamą Tipinį kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planą.

12. Kiek valstybės, savivaldybių biudžetų ir kitų valstybės įsteigtų fondų lėšų prireiks įstatymams įgyvendinti, ar bus galima sutaupyti (pateikiami prognozuojami rodikliai einamaisiais ir artimiausiais 3 biudžetiniais metais)

Įstatymams įgyvendinti papildomų valstybės biudžeto lėšų nereikės. Įstatymų projektuose siūlomų pakeitimų įgyvendinimas neturės įtakos žmogiškųjų, infrastruktūros ar finansinių išteklių pokyčiams, nes Nacionaliniam kibernetinio saugumo centrui nustatomas funkcijas numatoma vykdyti naudojantis turimais krašto apsaugos sistemos ištekliais.

13. Įstatymų projektų rengimo metu gauti specialistų vertinimai ir išvados

Įstatymų projektų rengimo metu specialistų vertinimų ir išvadų negauta.

14. Reikšminiai žodžiai, kurių reikia šiems projektams įtraukti į kompiuterinę paieškos sistemą, įskaitant Europos žodyno „Eurovoc“ terminus, temas bei sritis

„Kibernetinis saugumas“, „kibernetinis incidentas“, „kibernetinių incidentų valdymas“, „ryšių ir informacinė sistema“, „skaitmeninės paslaugos“.

15. Kiti, iniciatorių nuomone, reikalingi pagrindimai ir paaiškinimai

TIS direktyvos 25 straipsnio 1 dalis nustato, kad valstybės narės ne vėliau kaip 2018 m. gegužės 9 d. priima ir paskelbia įstatymus ir kitus teisės aktus, būtinus, kad būtų laikomasi TIS direktyvos nuostatų, todėl siūloma įstatymo įsigaliojimo data yra 2018 m. balandžio 9 d.

Užsienio reikalų ministras
Linas Linkevičius

Krašto apsaugos viceministras
Vytautas Umbrasas

LIETUVOS RESPUBLIKOS
VYRIAUSYBĖS KANCELIARIJA
Teisės akto projektas
2018-03-13 Nr. TAP-18-357
TAIS Nr. 18-1838(2)

Projektas

LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMO NR. XII-1428 PAKEITIMO ĮSTATYMAS

2018 m. d. Nr.
Vilnius

1 straipsnis. Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 nauja redakcija

Pakeisti Lietuvos Respublikos kibernetinio saugumo įstatymą Nr. XII-1428 ir jį išdėstyti taip:

„LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMAS

I SKYRIUS BENDROSIOS NUOSTATOS

1 straipsnis. Įstatymo paskirtis ir taikymas

1. Šis įstatymas nustato kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, apibrėžia kibernetinio saugumo politiką formuojančias ir įgyvendinančias institucijas, jų kompetenciją, funkcijas, teises ir pareigas, kibernetinio saugumo subjektų pareigas bei atsakomybę ir kibernetinio saugumo užtikrinimo priemones.

2. Įstatymas netaikomas patikimumo užtikrinimo paslaugų teikėjams, kuriems taikomi Reglamento (ES) Nr. 910/2014 19 straipsnyje nustatyti reikalavimai.

3. Šio įstatymo tikslais asmens duomenys tvarkomi vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu.

4. Įstatymo nuostatos suderintos su Europos Sąjungos teisės aktais, nurodytais šio įstatymo priede.

2 straipsnis. Pagrindinės šio įstatymo sąvokos

1. **Debesijos paslaugos** – paslaugos, kurias teikiant šių paslaugų 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. **Paieškos internete paslauga** – paslauga, kuria sudaromos sąlygos naudotojams atlikti paiešką svetainėse, remiantis bet kurio dalyko užklausa, naudojant raktinį žodį, frazę arba kitus įvesties duomenis; atliekant paiešką pateikiamos nuorodos, kuriose gali būti su ieškomu turiniu susijusios informacijos.

5. **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.

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

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

8. **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, trikdyti ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.

9. **Kibernetinių incidentų valdymas** – procedūros, taikomos kibernetiniams incidentams aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei ryšių ir informacinių sistemų veiklai atkurti.

10. **Kibernetinis saugumas** – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų išlaikyti atsparumą veiksniams, 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 jomis teikimui, taip pat įprastinei ryšių ir informacinių sistemų veiklai atkurti.

11. **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 tų tarptautinių organizacijų politiniu lygmeniu.

12. **Kibernetinio saugumo subjektai** – subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjai.

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

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

17. 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 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.

3 straipsnis. Kibernetinio saugumo principai

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

1) kibernetinės erdvės nediskriminavimo – 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 – taikomi teisiniai, organizaciniai ir techniniai kibernetinio saugumo reikalavimai neturi apriboti kibernetinio saugumo subjektų veiklos kibernetinėje erdvėje labiau, negu tai būtina;

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

5) standartizacijos ir technologinio neutralumo – įgyvendinant kibernetinio saugumo užtikrinimo 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 teikiantys kibernetinio saugumo subjektai. Srityse, kurios priklauso išimtinai kibernetinio saugumo subjektų kompetencijai, kibernetinio saugumo politiką formuojančios ir įgyvendinančios institucijos veiksmų imasi tik tada, kai ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinio saugumo negali užtikrinti šias sistemas valdantys ir paslaugas 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.

4 straipsnis. Savanoriškas pranešimas apie kibernetinius incidentus

1. Subjektai, kuriems šiuo įstatymu nėra nustatytos pranešimo apie kibernetinius incidentus jų ryšių ir informacinėse sistemose pareigos, gali savanoriškai informuoti Nacionalinį kibernetinio saugumo centrą apie kibernetinius incidentus, kurie daro didelį neigiamą poveikį jų teikiamų paslaugų tęstinumui, ir taikytas kibernetinių incidentų valdymo priemones. Nacionalinis kibernetinio saugumo centras tokius pranešimus tvarko Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka.

2. Subjektui, savanoriškai pranešusiam apie kibernetinį incidentą, nenustatoma jokių pareigų, kurios jam nebūtų nustatytos, jei jis nebūtų pateikęs pranešimo.

II SKYRIUS
KIBERNETINIO SAUGUMO POLITIKOS FORMAVIMAS IR ĮGYVENDINIMAS

5 straipsnis. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos

1. Kibernetinio saugumo politikos strateginius tikslus, prioritetus ir jiems pasiekti būtinas priemones nustato Lietuvos Respublikos Vyriausybė (toliau – Vyriausybė).

2. Kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija. 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, policija ir kitos institucijos pagal savo kompetenciją.

6 straipsnis. Vyriausybės įgaliojimai kibernetinio saugumo srityje

Vyriausybė:

1) tvirtina Nacionalinę kibernetinio saugumo strategiją;

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

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

4) tvirtina Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašą;

5) tvirtina Nacionalinį kibernetinių incidentų valdymo planą;

6) vadovauja kibernetinio saugumo krizių valdymui.

7 straipsnis. Krašto apsaugos ministerijos įgaliojimai kibernetinio saugumo srityje

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

1) koordinuoja Nacionalinės kibernetinio saugumo strategijos rengimą, teikia ją tvirtinti Vyriausybei;

2) rengia ir teikia Vyriausybei tvirtinti Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašą;

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

4) rengia ir 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 planą;

7) tvirtina ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planą;

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

9) tvirtina techninių kibernetinio saugumo priemonių 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.

8 straipsnis. Kibernetinio saugumo taryba

1. Kibernetinio saugumo taryba yra nuolatinė kolegiali institucija, analizuojanti kibernetinio saugumo užtikrinimo būklę Lietuvos Respublikoje ir teikianti pasiūlymus valstybės institucijoms, formuojančioms ir įgyvendinančioms kibernetinio saugumo politiką, kibernetinio saugumo subjektams, mokslo ir studijų institucijoms ir informacinių technologijų srityje veiklą vykdantiems verslo subjektams (toliau – kibernetinio saugumo dalyviai) dėl šios būklės gerinimo. Kibernetinio saugumo taryba yra sudaroma iš kibernetinio saugumo dalyvių atstovų ir kitų asmenų.

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

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

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

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

9 straipsnis. Nacionalinis kibernetinio saugumo centras

1. Nacionalinio kibernetinio saugumo centro funkcijas vykdo 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 Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatoms priežiūrą ir kibernetinio saugumo būsenos tyrimus;

2) duoda nurodymus kibernetinio saugumo subjektams pateikti informaciją, būtiną kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatoms ir kibernetinio saugumo būsenos 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 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 viešųjų ryšių tinklų ar viešųjų elektroninių ryšių paslaugų saugumo auditą ir pateikti šio audito rezultatus, jei jie Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nustatyta tvarka nepateikia techninės informacijos, reikalingos ryšių ir informacinių sistemų ar jomis teikiamų paslaugų kibernetinio saugumo būsenai įvertinti;

6) gavęs įrodymų iš kibernetinio saugumo subjekto, skaitmeninės paslaugos vartotojo arba kitos valstybės narės, kurioje yra teikiama skaitmeninė paslauga, kompetentingos institucijos, prižiūrinčios skaitmeninių paslaugų teikėjų veiklą kibernetinio saugumo srityje, 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 vykdo rizikos kibernetinėje erdvėje bei kibernetinių incidentų analizę;

8) pagal 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 užtikrinimo 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 informuoja Lietuvos Respublikos ryšių reguliavimo tarnybą;

12) dalyvauja kibernetinio saugumo krizių valdyme;

13) jei 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 incidentus arba reikalauja, kad tai padarytų kibernetinio saugumo subjektas;

14) Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka bendradarbiauja su tarptautinių organizacijų kompetentingomis institucijomis, jų įsteigtomis bendradarbiavimo grupėmis bei užsienio valstybių kompetentingomis institucijomis ir tarnybomis vykdydamas šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje;

15) rengia Ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą;

16) tvarko asmens duomenis, būtinus funkcijoms kibernetinio saugumo užtikrinimo srityje atlikti;

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

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

10 straipsnis. Valstybinės duomenų apsaugos inspekcijos įgaliojimai kibernetinio saugumo srityje

Valstybinė duomenų apsaugos inspekcija įgyvendina kibernetinio saugumo politiką asmens duomenų apsaugos srityje:

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

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

3) nustato kibernetinio saugumo subjektams informacijos apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones pateikimo Valstybinei duomenų apsaugos inspekcijai tvarką;

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

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

11 straipsnis. Policijos įgaliojimai kibernetinio saugumo srityje

Policija, vykdydama kibernetinių incidentų, galimai turinčių nusikalstamos veikos požymių, užkardymą ir tyrimą:

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

2) nustato kibernetinio saugumo subjektams informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veikos 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 nusikalstamoje veikoje, 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, 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. Tokiais atvejais apylinkės teismo pirmininkui ar jo įgaliotam teisėjui pateikiamas teikimas dėl veiksmų teisėtumo ar pagrįstumo patvirtinimo motyvuota nutartimi. Jeigu terminas baigiasi poilsio ar švenčių dieną, teikimas pateikiamas ne vėliau kaip kitą darbo dieną po poilsio ar švenčių dienos. Jeigu teisėjas nepatvirtina nurodytų veiksmų teisėtumo ar pagrįstumo motyvuota nutartimi, nurodymas nedelsiant stabdomas;

4) turi teisę duoti nurodymą viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų teikėjui ir skaitmeninių paslaugų teikėjui išsaugoti informaciją, susijusią su jų teikiamomis paslaugomis, 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 ir, kai yra motyvuota teismo nutartis, gauti paslaugų gavėjo srauto duomenis ir kontroliuoti perduodamos informacijos turinį.

III SKYRIUS
KIBERNETINIO SAUGUMO SUBJEKTŲ PAREIGOS

12 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 Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatoms;

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

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

4) teikia Valstybinei duomenų apsaugos inspekcijai informaciją apie jų valdomose ir (arba) tvarkomose arba viešosioms elektroninių ryšių paslaugoms, elektroninės informacijos prieglobos paslaugoms ir skaitmeninėms paslaugoms teikti naudojamose ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones šios institucijos nustatyta tvarka;

5) policijos generalinio komisaro nustatyta tvarka teikia policijai informaciją, reikalingą teisės pažeidimams, turintiems nusikalstamos veikos 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;

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

7) vykdo Nacionalinio kibernetinio saugumo centro nurodymus, duotus šio įstatymo nustatytais pagrindais.

2. Šiame straipsnyje nustatytos pareigos netaikomos mažoms ir labai mažoms įmonėms, teikiančioms skaitmenines paslaugas Lietuvos Respublikoje ir (arba) kitoje Europos Sąjungos valstybėje narėje.

13 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, parengia, patvirtina ir Nacionaliniam kibernetinio saugumo centrui pateikia kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus;

2) Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka informuoja skaitmeninių paslaugų teikėjus 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 metus išbando kibernetinių incidentų valdymo planų veikimą, o 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 svetainėje ar kitomis visuomenės informavimo priemonėmis paslaugų gavėjams rekomendacijas apie priemones 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 svetainėje ar kitomis visuomenės informavimo priemonėmis elektroninės informacijos prieglobos paslaugų gavėjams rekomendacijas apie priemones kibernetiniam saugumui užtikrinti naudojantis elektroninės informacijos prieglobos paslaugomis.

5. Skaitmeninių paslaugų teikėjai:

1) viešai skelbia savo interneto svetainėje ar kitomis visuomenės informavimo priemonėmis paslaugų gavėjams rekomendacijas apie priemones kibernetiniam saugumui užtikrinti naudojantis skaitmeninių paslaugų teikėjų teikiamomis paslaugomis;

2) skiria atstovą veikti Europos Sąjungoje skaitmeninių paslaugų teikėjo vardu. Atstovas skiriamas, jei skaitmeninių paslaugų teikėjas nėra įsisteigęs Europos Sąjungos valstybėje narėje. Atstovas turi būti fizinis arba juridinis asmuo, įsisteigęs vienoje iš tų valstybių narių, kuriose yra teikiamos skaitmeninės paslaugos. Kibernetinio saugumo politiką įgyvendinančios institucijos turi teisę kreiptis į skaitmeninių paslaugų teikėjo atstovą dėl šiuo įstatymu nustatytų skaitmeninių paslaugų teikėjo pareigų vykdymo. Laikoma, kad skaitmeninių paslaugų teikėjas priklauso valstybės narės, kurioje yra įsisteigęs jo atstovas, jurisdikcijai.

6. Šiame straipsnyje nustatytos pareigos netaikomos mažoms ir labai mažoms įmonėms, teikiančioms skaitmenines paslaugas Lietuvos Respublikoje ir (arba) kitoje Europos Sąjungos valstybėje narėje.

IV SKYRIUS

TARPINSTITUCINIS BENDRADARBIAVIMAS, KEITIMOSI INFORMACIJA TVARKA IR ATSAKOMYBĖ UŽ KIBERNETINIO SAUGUMO REIKALAVIMŲ PAŽEIDIMUS

14 straipsnis. Kibernetinio saugumo informacinis tinklas

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

2. Kibernetinio saugumo informaciniu tinklu gali naudotis tik tie 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.

15 straipsnis. Tarpinstitucinis bendradarbiavimas tiriant kibernetinius incidentus

1. Nacionalinis kibernetinio saugumo centras ir policija konsultuojasi ir bendradarbiauja tiriant kibernetinius incidentus, keičiasi su kibernetinių incidentų tyrimais susijusia informacija, reikalinga pagal kompetenciją institucijų vykdomoms funkcijoms atlikti. Prireikus apie kibernetinių incidentų tyrimą gali būti informuojami kiti kriminalinės žvalgybos subjektai ir (arba) žvalgybos institucijos.

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

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

16 straipsnis. Informacijos apsauga

Kibernetinio saugumo politiką įgyvendinančios institucijos kibernetinio saugumo subjektų pateikta informacija, įskaitant ir konfidencialią informaciją, keičiasi tik tiek, kiek tai yra būtina institucijų pagal kompetenciją vykdomoms funkcijoms atlikti, ir užtikrina gautos informacijos apsaugą.

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

Už šio įstatymo ar jo įgyvendinamųjų teisės aktų nustatytų reikalavimų pažeidimus kibernetinio saugumo subjektų administracijos vadovai atsako Lietuvos Respublikos administracinių nusižengimų kodekso nustatyta tvarka.“

2 straipsnis. Įstatymo įsigaliojimas ir įgyvendinimas

1. Šis įstatymas, išskyrus šio straipsnio 2 dalį, įsigalioja 2018 m. balandžio 9 d.

2. Vyriausybė ir krašto apsaugos ministras iki 2018 m. balandžio 9 d. priima šio įstatymo įgyvendinamuosius teisės aktus.

3. 2018 m. gegužės 5 d. įsigalioja tokia šiuo įstatymu patvirtinto Kibernetinio saugumo įstatymo 9 straipsnio redakcija:

„10 straipsnis. Valstybinės duomenų apsaugos inspekcijos įgaliojimai kibernetinio saugumo srityje

Valstybinė duomenų apsaugos inspekcija įgyvendina kibernetinio saugumo politiką asmens duomenų apsaugos srityje ir vykdo 2016 m. balandžio 27 d. Europos Parlamento ir

Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) jai pavestas užduotis.“

4. 2018 m. gegužės 25 d. įsigalioja tokia šiuo įstatymu patvirtinto Kibernetinio saugumo įstatymo 12 straipsnio redakcija:

„12 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 Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatoms;

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

3) Nacionaliniame kibernetinių incidentų valdymo plane nustatytomis sąlygomis ir tvarka informuoja kibernetinio saugumo instituciją 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 nusikalstamos veikos 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 paskirto asmens ar padalinio kontaktinę informaciją;

6) vykdo Nacionalinio kibernetinio saugumo centro nurodymus, duotus šio įstatymo nustatytais pagrindais.

2. Šiame straipsnyje nustatytos pareigos netaikomos mažoms ir labai mažoms įmonėms, teikiančioms skaitmenines paslaugas Lietuvos Respublikoje ir (arba) kitoje Europos Sąjungos valstybėje narėje.“

Skelbiu šį Lietuvos Respublikos Seimo priimtą įstatymą.

Respublikos Prezidentas

Užsienio reikalų ministras
Linas Linkevičius

KAM AD
Dokumentų administravimo skyriaus vyr. specialistė
Jurgita Kulitienė

Krašto apsaugos ministerijos
Teisės departamento direktorė
Judita Nazienė

Krašto apsaugos viceministras
Vytautas Umbrasas

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 (OL 2016 L 194, p. 1-30).

2. 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).

Užsienio reikalų ministras
Linas Linkevičius

Krašto apsaugos viceministras
Vytautas Umbrasas

KAM AD
Dokumentų administravimo
skyriaus vyr. specialistė
Jurgita Kulikienė

Krašto apsaugos ministerijos
Teisės departamento direktorė
Judita Nacienė

LIETUVOS RESPUBLIKOS
VYRIAUSYBĖS KANCELIARIJA
Teisės akto projektas
2018-03-13 Nr. TAP-18-356
TAIS Nr. 18-1839(2)

Projektas

LIETUVOS RESPUBLIKOS ADMINISTRACINIŲ NUSIŽENGIMŲ KODEKSO 479, 480, 589 STRAIPSNIŲ IR PRIEDO PAKEITIMO ĮSTATYMAS

2018 m. d. Nr.
Vilnius

1 straipsnis. 479 straipsnio pakeitimas

1. Pakeisti 479 straipsnio 3 dalį ir ją išdėstyti taip:

„3. Nacionalinio kibernetinio saugumo centro nurodymų pateikti informaciją, būtiną kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatoms ir kibernetinio saugumo būsenai įvertinti, nevykdymas laiku

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.“

2. Pakeisti 479 straipsnio 4 dalį ir ją išdėstyti taip:

„4. Informacijos apie kibernetinius incidentus, galimai turinčius nusikalstamos veikos požymių, nepateikimas policijai arba šios informacijos teikimo tvarkos pažeidimas

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.“

2 straipsnis. 480 straipsnio pakeitimas

Pakeisti 480 straipsnio 4 dalį ir ją išdėstyti taip:

„4. Nustatytų Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatų kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų kibernetiniam saugumui užtikrinti nevykdymas

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki vieno tūkstančio keturių šimtų eurų.“

3 straipsnis. 589 straipsnio pakeitimas

1. Pakeisti 589 straipsnio 29 punktą ir jį išdėstyti taip:

„29) Valstybinės duomenų apsaugos inspekcijos – dėl šio kodekso 82, 83 straipsniuose, 224 straipsnio 1 dalyje, 505, 507 straipsniuose numatytų administracinių nusižengimų;“.

2. Pakeisti 589 straipsnio 46 punktą ir jį išdėstyti taip:

„46) Nacionalinio kibernetinio saugumo centro – dėl šio kodekso 479 straipsnio 1, 2, 4 dalyse, 480, 507 straipsniuose numatytų administracinių nusižengimų;“.

3. Pakeisti 589 straipsnio 49 punktą ir jį išdėstyti taip:

„49) policijos – dėl šio kodekso 48, 62, 63, 65, 69, 71, 72, 73, 74 straipsniuose, 75 straipsnio 1 dalyje, 76, 77, 78, 80, 88, 89, 95 straipsniuose, 98 straipsnio 1 dalyje, 108, 109, 115, 122, 125, 127, 130, 131, 133, 134, 137, 142, 143, 150, 151, 152, 153, 154, 155, 159, 160, 161, 162, 163, 164, 166, 167, 168, 169, 170, 171 straipsniuose, 172 straipsnio 1, 2 dalyse, 173, 174, 176, 182, 183, 192, 206, 207, 208, 209, 214, 219, 220, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 234^1, 234^2 straipsniuose, 281 straipsnio 1, 2 dalyse, 282, 290, 306, 307, 321, 336, 339, 340, 342, 346, 366, 367, 368 straipsniuose, 369 straipsnio 5, 6 dalyse, 414, 415, 416, 417, 420, 421, 422, 423, 424 straipsniuose, 426 straipsnio 1, 2, 3, 5 dalyse, 427, 428, 429, 430, 431, 432, 433 straipsniuose, 434 straipsnio 1, 3 dalyse, 436, 438 straipsniuose, 439 straipsnio 2 dalyje, 450, 451, 452, 453, 454, 455, 456, 458, 459, 460, 461, 462, 463, 473, 474 straipsniuose,

479 straipsnio 3, 4 dalyse, 481, 482, 483, 484, 484[1], 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495 straipsniuose, 496 straipsnio 1, 2 dalyse, 506 straipsnio 1, 2, 4, 5, 6 dalyse, 507, 508, 511, 512, 513, 518, 519, 520, 521, 523, 524, 527, 528, 530, 532, 534, 535, 538, 539, 540, 541 straipsniuose, 542 straipsnio 1, 2, 3 dalyse, 543, 546, 553 straipsniuose numatytų administracinių nusižengimų;".

4 straipsnis. Kodekso priedo pakeitimas

Papildyti Kodekso priedą nauju 95 punktu:

„95. 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. 1–30).“

5 straipsnis. Įstatymo įsigaliojimas

1. Šis įstatymas, išskyrus šio įstatymo 3 straipsnį, įsigalioja 2018 m. balandžio 9 d.

2. Šio įstatymo 3 straipsnis įsigalioja 2018 m. gegužės 25 d.

3. 2018 m. gegužės 25 d. įsigalioja tokia šiuo įstatymu patvirtinto Administracinių nusižengimų kodekso 479 straipsnio redakcija:

„479 straipsnis. Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytos informacijos teikimo pareigos atlikimo pažeidimai

1. Informacijos apie kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones nepateikimas Nacionaliniam kibernetinio saugumo centrui arba šios informacijos teikimo tvarkos pažeidimas

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.

2. Nacionalinio kibernetinio saugumo centro nurodymų kibernetinio saugumo subjektams pateikti informaciją, būtiną kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams ir kibernetinio saugumo būsenai įvertinti, nevykdymas laiku

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.

3. Informacijos apie kibernetinius incidentus, galimai turinčius nusikalstamos veikos požymių, nepateikimas policijai arba šios informacijos teikimo tvarkos pažeidimas

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.

4. Šio straipsnio 1, 2, 3 dalyse numatyti administraciniai nusižengimai, padaryti pakartotinai,

užtraukia baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trijų šimtų iki vieno tūkstančio keturių šimtų keturiasdešimt eurų.“

Skelbiu šį Lietuvos Respublikos Seimo priimtą įstatymą.

Respublikos Prezidentas

Užsienio reikalų ministras
Linas Linkevičius

Krašto apsaugos viceministras
Vytautas Umbrasas

KAM AD
Dokumentų administravimo skyriaus vyr. specialistė
Jurgita Kulitienė

Krašto apsaugos ministerijos
Teisės departamento direktorė
Judita Nagienė

Projekto
lyginamasis variantas

LIETUVOS RESPUBLIKOS ADMINISTRACINIŲ NUSIŽENGIMŲ KODEKSO 479, 480, 589 STRAIPSNIŲ IR PRIEDO PAKEITIMO ĮSTATYMAS

2018 m. d. Nr.
Vilnius

1 straipsnis. 479 straipsnio pakeitimas

1. Pakeisti 479 straipsnio 3 dalį ir ją išdėstyti taip:

„3. ~~Informacijos, reikalingos vertinti viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir (arba) elektroninės informacijos prieglobos paslaugų kibernetinio saugumo būseną, nepateikimas Nacionaliniam kibernetinio saugumo centrui arba šios informacijos pateikimo tvarkos pažeidimas~~ **Nacionalinio kibernetinio saugumo centro nurodymų pateikti informaciją, būtiną kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties** Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatoms **ir kibernetinio saugumo būsenai įvertinti, nevykdymas laiku**

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.“

2. Pakeisti 479 straipsnio 4 dalį ir ją išdėstyti taip:

„4. Informacijos apie kibernetinius incidentus, galimai turinčius nusikalstamos veikos požymių, nepateikimas ~~Policijos departamentui prie Vidaus reikalų ministerijos~~ **policijai** arba šios informacijos teikimo tvarkos pažeidimas

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.“

2 straipsnis. 480 straipsnio pakeitimas

Pakeisti 480 straipsnio 4 dalį ir ją išdėstyti taip:

„4. Nustatytų ~~organizacinių~~ **Organizacinių** ir techninių **kibernetinio saugumo** reikalavimų, **taikomų kibernetinio saugumo subjektams, aprašo nuostatų kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų kibernetiniam saugumui užtikrinti nevykdymas** ~~ypatingos svarbos informacinei infrastruktūrai arba elektroninės informacijos prieglobos paslaugų kibernetiniam saugumui užtikrinti nesilaikymas~~

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki vieno tūkstančio keturių šimtų eurų.“

3 straipsnis. 589 straipsnio pakeitimas

1. Pakeisti 589 straipsnio 29 punktą ir jį išdėstyti taip:

„29) Valstybinės duomenų apsaugos inspekcijos – dėl šio kodekso 82, 83 straipsniuose, 224 straipsnio 1 dalyje, ~~479 straipsnio 2, 5 dalyse,~~ 505, 507 straipsniuose numatytų administracinių nusižengimų;“.

2. Pakeisti 589 straipsnio 46 punktą ir jį išdėstyti taip:

„46) Nacionalinio kibernetinio saugumo centro – dėl šio kodekso 479 straipsnio 1, ~~32~~, ~~54~~ dalyse, 480, 507 straipsniuose numatytų administracinių nusižengimų;“.

3. Pakeisti 589 straipsnio 49 punktą ir jį išdėstyti taip:

„49) policijos – dėl šio kodekso 48, 62, 63, 65, 69, 71, 72, 73, 74 straipsniuose, 75 straipsnio 1 dalyje, 76, 77, 78, 80, 88, 89, 95 straipsniuose, 98 straipsnio 1 dalyje, 108, 109, 115, 122, 125, 127, 130, 131, 133, 134, 137, 142, 143, 150, 151, 152, 153, 154, 155, 159, 160, 161, 162, 163, 164, 166, 167, 168, 169, 170, 171 straipsniuose, 172 straipsnio 1, 2 dalyse, 173, 174,

176, 182, 183, 192, 206, 207, 208, 209, 214, 219, 220, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 234^1, 234^2 straipsniuose, 281 straipsnio 1, 2 dalyse, 282, 290, 306, 307, 321, 336, 339, 340, 342, 346, 366, 367, 368 straipsniuose, 369 straipsnio 5, 6 dalyse, 414, 415, 416, 417, 420, 421, 422, 423, 424 straipsniuose, 426 straipsnio 1, 2, 3, 5 dalyse, 427, 428, 429, 430, 431, 432, 433 straipsniuose, 434 straipsnio 1, 3 dalyse, 436, 438 straipsniuose, 439 straipsnio 2 dalyje, 450, 451, 452, 453, 454, 455, 456, 458, 459, 460, 461, 462, 463, 473, 474 straipsniuose, 479 straipsnio **43**, ~~54~~ dalyse, 481, 482, 483, 484, 484^1, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495 straipsniuose, 496 straipsnio 1, 2 dalyse, 506 straipsnio 1, 2, 4, 5, 6 dalyse, 507, 508, 511, 512, 513, 518, 519, 520, 521, 523, 524, 527, 528, 530, 532, 534, 535, 538, 539, 540, 541 straipsniuose, 542 straipsnio 1, 2, 3 dalyse, 543, 546, 553 straipsniuose numatytų administracinių nusižengimų;“.

4 straipsnis. Kodekso priedo pakeitimas

Papildyti Kodekso priedą nauju 95 punktu:

„95. 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. 1-30)“

5 straipsnis. Įstatymo įsigaliojimas

1. Šis įstatymas, išskyrus šio įstatymo 3 straipsnį, įsigalioja 2018 m. balandžio 9 d.

2. Šio įstatymo 3 straipsnis įsigalioja 2018 m. gegužės 25 d.

3. 2018 m. gegužės 25 d. įsigalioja tokia šiuo įstatymu patvirtinto Administracinių nusižengimų kodekso 479 straipsnio redakcija:

~~479 straipsnis. Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytos informacijos teikimo pareigos atlikimo pažeidimai~~

~~1. Informacijos apie kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones nepateikimas Nacionaliniam kibernetinio saugumo centrui arba šios informacijos teikimo tvarkos pažeidimas~~

~~užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.~~

~~2. Informacijos apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones nepateikimas Valstybinei duomenų apsaugos inspekcijai arba šios informacijos teikimo tvarkos pažeidimas~~

~~užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.~~

~~3. Nacionalinio kibernetinio saugumo centro nurodymų pateikti informaciją, būtiną kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatoms ir kibernetinio saugumo būsenai įvertinti, nevykdymas laiku užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.~~

~~4. Informacijos apie kibernetinius incidentus, galimai turinčius nusikalstamos veikos požymių, nepateikimas policijai arba šios informacijos teikimo tvarkos pažeidimas~~

~~užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.~~

~~5. Šio straipsnio 1, 2, 3, 4 dalyse numatyti administraciniai nusižengimai, padaryti pakartotinai,~~

~~užtraukia baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trijų šimtų iki vieno tūkstančio keturių šimtų keturiasdešimt eurų.~~

„479 straipsnis. Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytos informacijos teikimo pareigos atlikimo pažeidimai

1. Informacijos apie kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones nepateikimas Nacionaliniam kibernetinio saugumo centrui arba šios informacijos teikimo tvarkos pažeidimas

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.

2. Nacionalinio kibernetinio saugumo centro nurodymų kibernetinio saugumo subjektams pateikti informaciją, būtiną kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams ir kibernetinio saugumo būsenai įvertinti, nevykdymas laiku

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.

3. Informacijos apie kibernetinius incidentus, galimai turinčius nusikalstamos veikos požymių, nepateikimas policijai arba šios informacijos teikimo tvarkos pažeidimas

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.

4. Šio straipsnio 1, 2, 3 dalyse numatyti administraciniai nusižengimai, padaryti pakartotinai,

užtraukia baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trijų šimtų iki vieno tūkstančio keturių šimtų keturiasdešimt eurų.“

Skelbiu šį Lietuvos Respublikos Seimo priimtą įstatymą.

Respublikos Prezidentas

Užsienio reikalų ministras
Linas Linkevičius

Krašto apsaugos viceministras
Vytautas Umbrasas

2016 M. LIEPOS 6 D. EUROPOS PARLAMENTO IR TARYBOS DIREKTYVOS (ES) 2016/1148 DĖL PRIEMONIŲ AUKŠTAM BENDRAM TINKLŲ IR INFORMACINIŲ SISTEMŲ SAUGUMO LYGIUI VISOJE SĄJUNGOJE UŽTIKRINTI IR NACIONALINIŲ TEISĖS AKTŲ ATITIKTIES LENTELĖ

Direktyvos (kito Europos Sąjungos (ES) teisės akto) pavadinimas ir numeris	**Lietuvos Respublikos nacionalinio teisės akto (teisės akto projekto) pavadinimas**	**Direktyvos (kito ES teisės akto) perkėlimo (įgyvendinimo) lygis (visiškas, dalinis)**
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 (toliau – Direktyva)	**1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas Nr. X-1444 (toliau – ADTAĮ)** **2. Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymo projektas (toliau – Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas)** **3. Lietuvos Respublikos elektroninių ryšių įstatymas Nr. IX-2135** **4. Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas Nr. X-614** **5. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo Nr. XI-1807 pakeitimo įstatymo projektas** **6. Administracinių nusižengimų kodekso pakeitimo įstatymo projektas (toliau – ANKPĮ projektas)** **7. Lietuvos Respublikos Vyriausybės nutarimo „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“ projektas (toliau – Strategijos projektas)** **8. Lietuvos Respublikos Vyriausybės nutarimo „Dėl Lietuvos Respublikos Vyriausybės 2016 m. liepos 20 d. nutarimo Nr. 742 „Dėl Ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos patvirtinimo“**	

	pakeitimo“ projektas (toliau – YSII identifikavimo metodikos projektas) **9. Lietuvos Respublikos Vyriausybės nutarimo „Dėl Lietuvos Respublikos Vyriausybės 2016 m. sausio 25 d. nutarimo Nr. 87 „Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“ pakeitimo“ projektas (toliau – Kibernetinių incidentų valdymo plano projektas)** **10. Lietuvos Respublikos Vyriausybės nutarimo „Dėl Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimo Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“ pakeitimo“ projektas (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo projektas)** **11. Lietuvos Respublikos smulkiojo ir vidutinio verslo plėtros įstatymas Nr. VIII-935**	
1 straipsnis. Dalykas ir taikymo sritis 1. Šioje direktyvoje nustatomos priemonės aukštam bendram tinklų ir informacinių sistemų saugumo lygiui Sąjungoje užtikrinti, kad būtų pagerintas vidaus rinkos veikimas.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
2. Tuo tikslu šia direktyva: a) visoms valstybėms narėms nustatomos pareigos priimti nacionalinę tinklų ir informacinių sistemų saugumo strategiją; b) sukuriama Bendradarbiavimo grupė, kad būtų remiamas ir lengvinamas valstybių narių strateginis bendradarbiavimas ir keitimasis informacija, taip pat didinama jų atsakomybė ir tarpusavio pasitikėjimas; c) sukuriamas Reagavimo į kompiuterinius saugumo incidentus tarnybų tinklas (toliau – CSIRT tinklas), kad būtų prisidedama prie valstybių narių atsakomybės ir tarpusavio pasitikėjimo didinimo ir skatinamas greitas bei veiksmingas operatyvinis	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	

bendradarbiavimas; d) nustatomi saugumo ir pranešimo reikalavimai esminių paslaugų operatoriams ir skaitmeninių paslaugų teikėjams; e) nustatomos valstybių narių pareigos paskirti nacionalines kompetentingas institucijas, bendruosius informacinius centrus ir CSIRT, kuriems pavedamos užduotys, susijusios su tinklų ir informacinių sistemų saugumu.		
3. Šioje direktyvoje numatyti saugumo ir pranešimo reikalavimai netaikomi įmonėms, kurioms taikomi Direktyvos 2002/21/EB 13a ir 13b straipsniuose nustatyti reikalavimai, ir patikimumo užtikrinimo paslaugų teikėjams, kuriems taikomi Reglamento (ES) Nr. 910/2014 19 straipsnyje nustatyti reikalavimai.	**1. Kibernetinio saugumo įstatymas iš dalies įgyvendina ir Direktyvos 2002/21/EB 13s ir 13b straipsnių nuostatas dėl saugumo ir pranešimų reikalavimų** **2. Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **1 straipsnis. Įstatymo paskirtis ir taikymas** <...> 2. Įstatymas netaikomas patikimumo užtikrinimo paslaugų teikėjams, kuriems taikomi Reglamento (ES) Nr. 910/2014 19 straipsnyje nustatyti reikalavimai.	Visiškas
4. Ši direktyva taikoma nedarant poveikio Tarybos direktyvai 2008/114/EB (14) ir Europos Parlamento ir Tarybos direktyvoms 2011/93/ES (15) ir 2013/40/ES (16).	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
5. Nedarant poveikio SESV 346 straipsniui, informacija, kuri yra konfidenciali pagal Sąjungos ir nacionalines taisykles, kaip antai taisykles dėl verslo konfidencialumo, turi būti keičiamasi su Komisija ir kitomis atitinkamomis institucijomis tik kai toks keitimasis yra būtinas šios direktyvos taikymui. Keičiamasi tik tokia informacija, kuri atitinka keitimosi tikslą ir yra svarbi tam tikslui pasiekti. Keičiantis tokia informacija turi būti saugomas tos informacijos konfidencialumas, ir esminių paslaugų operatorių bei skaitmeninių paslaugų teikėjų saugumo ir komerciniai interesai.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **16 straipsnis. Informacijos apsauga** Kibernetinio saugumo politiką įgyvendinančios institucijos kibernetinio saugumo subjektų pateikta informacija, įskaitant ir konfidencialią informaciją, keičiasi tik tiek, kiek tai yra būtina institucijų pagal kompetenciją vykdomoms funkcijoms atlikti, ir užtikrina gautos informacijos apsaugą.	

6. Šia direktyva **nedaromas poveikis veiksmams**, kurių valstybės narės **imasi siekdamos apsaugoti** savo esmines valstybines funkcijas, visų pirma užtikrinti nacionalinį saugumą, įskaitant veiksmus, **skirtus informacijai**, kurios atskleidimas, valstybių narių nuomone, prieštarautų gyvybiniams jų saugumo interesams, **apsaugoti**, taip pat palaikyti viešąją tvarką, visų pirma sudaryti sąlygas tirti ir išaiškinti nusikalstamas veikas, ir už jas patraukti baudžiamojon atsakomybėn.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
7. Kai pagal konkrečiam sektoriui taikomą Sąjungos teisės aktą reikalaujama, kad esminių paslaugų operatoriai arba skaitmeninių paslaugų teikėjai užtikrintų savo tinklų ir informacinių sistemų saugumą arba praneštų apie incidentus, jei tokių reikalavimų poveikis yra bent lygiavertis šioje direktyvoje nustatytų pareigų poveikiui, taikomos tos minėto konkrečiam sektoriui taikomo Sąjungos teisės akto nuostatos.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
2 straipsnis. Asmens duomenų tvarkymas 1. Asmens duomenų tvarkymas pagal šią direktyvą vykdomas laikantis Direktyvos 95/46/EB. 2. Sąjungos institucijos ir įstaigos asmens duomenis pagal šią direktyvą tvarko laikydamosi Reglamento (EB) Nr. 45/2001.	**Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas Nr. I-1374** **Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo priedas** **ĮGYVENDINAMI EUROPOS SĄJUNGOS TEISĖS AKTAI** 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL *2004 m. specialusis leidimas,* 13 skyrius, 15 tomas, p. 355).	Visiškas
3 straipsnis. Minimalus suderinimas Nedarant poveikio 16 straipsnio 10 daliai ir valstybių narių pareigoms pagal Sąjungos teisę, valstybės narės gali priimti ar palikti galioti nuostatas aukštesniam tinklų ir informacinių sistemų saugumo lygiui užtikrinti.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
4 straipsnis. Terminų apibrėžtys Šioje direktyvoje vartojamų terminų apibrėžtys:	**1. Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas**	Visiškas

1) **tinklų ir informacinė sistema** – tai: a) elektroninių ryšių tinklas, kaip apibrėžta Direktyvos 2002/21/EB 2 straipsnio a punkte; b) bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba c) skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami a ir b punktuose nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;	**2 straipsnis. Pagrindinės šio įstatymo sąvokos:** <...> 9. **Informacinė sistema** – techninių ir programinių priemonių visuma, naudojama informacijai kurti, siųsti, priimti, išsaugoti ar kitaip tvarkyti elektroniniu būdu. <...> **2. Lietuvos Respublikos elektroninių ryšių įstatymas Nr. IX-2135** **3 straipsnis.** <...> 16. **Elektroninių ryšių tinklas** – perdavimo sistemos ir (arba) komutavimo bei maršruto parinkimo įranga, kitos priemonės, įskaitant pasyviuosius tinklo elementus, leidžiančios perduoti signalus laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis, įskaitant palydovinius tinklus, fiksuotuosius (kanalų ir paketų komutavimo, įskaitant internetą) ir judriuosius antžeminius tinklus, elektros perdavimo kabelines sistemas (kiek jos naudojamos signalams perduoti), tinklus, naudojamus radijo ir (arba) televizijos programoms transliuoti (retransliuoti), ir kabelinės televizijos bei mikrobangų daugiakanalės televizijos tinklus neatsižvelgiant į perduodamos informacijos pobūdį. **3. Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> 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.	
2) **tinklų ir informacinių sistemų saugumas** – tinklų ir informacinių sistemų pajėgumas **tam tikru patikimumo lygiu išlikti atsparus** bet kuriems veiksmams, keliantiems pavojų saugomų, perduodamų ar tvarkomų duomenų, arba atitinkamų teikiamų ar per tas tinklų ir informacines sistemas gaunamų paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui;	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> 10. **Kibernetinis saugumas** – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų išlaikyti atsparumą veiksniams, 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 jomis teikimui, taip pat įprastinei ryšių ir informacinių sistemų veiklai atkurti.	Visiškas
3) **nacionalinė tinklų ir informacinių sistemų saugumo strategija** – sistema, kurioje nustatomi strateginiai tikslai ir prioritetai dėl tinklų ir informacinių sistemų saugumo nacionaliniu lygmeniu;	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **5 straipsnis. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos** 1. Kibernetinio saugumo politikos strateginius tikslus, prioritetus ir jiems pasiekti būtinas priemones nustato Lietuvos Respublikos Vyriausybė (toliau – Vyriausybė). <...> **6 straipsnis. Vyriausybės įgaliojimai kibernetinio saugumo srityje** Vyriausybė: 1) tvirtina Nacionalinę kibernetinio saugumo strategiją; <...>	Visiškas
4) **esminių paslaugų operatorius** – viešojo arba privačiojo sektoriaus subjektas, kurio rūšis yra nurodyta II priede ir kuris tenkina 5 straipsnio 2 dalyje nustatytus kriterijus;	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...>	Visiškas

	6. **Ypatingos svarbos informacinės infrastruktūros valdytojas** – asmuo, valdantis ypatingos svarbos informacinę infrastruktūrą.	
5) **skaitmeninė paslauga** – paslauga, kaip apibrėžta Europos Parlamento ir Tarybos direktyvos (ES) 2015/1535 1 straipsnio 1 dalies b punkte, kuri yra vienos iš III priede išvardytų rūšių;	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> 15. **Skaitmeninė paslauga** – ryšių ir informacinėmis technologijomis grindžiama paslaugų grupė, apimanti elektroninės prekyvietės ir (arba) paieškos internete, ir (arba) debesijos paslaugas.	Visiškas
6) **skaitmeninių paslaugų teikėjas** – juridinis asmuo, kuris teikia skaitmenines paslaugas;	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> 16. **Skaitmeninių paslaugų teikėjas** – juridinis asmuo, teikiantis skaitmenines paslaugas Lietuvoje ir (arba) kitose Europos Sąjungos valstybėse narėse.	Visiškas
7) **incidentas** – įvykis, turintis faktinį neigiamą poveikį tinklų ir informacinių sistemų saugumui;	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> 8. **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, trikdyti ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.	Visiškas
8) **incidentų valdymas** – visos procedūros, padedančios nustatyti, ištirti bei suvaldyti incidentą ir į jį reaguoti;	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...>	Visiškas

	9. **Kibernetinių incidentų valdymas** – procedūros, taikomos kibernetiniams incidentams aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei ryšių ir informacinių sistemų veiklai atkurti.	
9) **rizika** – pagrįstai nustatoma aplinkybė ar įvykis, galintis turėti neigiamą poveikį tinklų ir informacinių sistemų saugumui;	**Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo projektas**	Visiškas
10) **atstovas** – Sąjungoje įsisteigęs fizinis arba juridinis asmuo, aiškiai paskirtas veikti skaitmeninių paslaugų teikėjo, kuris nėra įsisteigęs Sąjungoje, vardu ir į kurį vietoj skaitmeninių paslaugų teikėjo gali kreiptis nacionalinė kompetentinga institucija arba CSIRT dėl pagal šią direktyvą nustatytų to skaitmeninių paslaugų teikėjo pareigų;	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **13 straipsnis. Specialiosios kibernetinio saugumo subjektų pareigos** 5. Skaitmeninių paslaugų teikėjai: <...> 2) skiria atstovą veikti Europos Sąjungoje skaitmeninių paslaugų teikėjo vardu. Atstovas skiriamas, jei skaitmeninių paslaugų teikėjas nėra įsisteigęs Europos Sąjungos valstybėje narėje. Atstovas turi būti fizinis arba juridinis asmuo, įsisteigęs vienoje iš tų valstybių narių, kuriose yra teikiamos skaitmeninės paslaugos. Kibernetinio saugumo politiką įgyvendinančios institucijos turi teisę kreiptis į skaitmeninių paslaugų teikėjo atstovą dėl šiuo įstatymu nustatytų skaitmeninių paslaugų teikėjo pareigų vykdymo. Laikoma, kad skaitmeninių paslaugų teikėjas priklauso valstybės narės, kurioje yra įsisteigęs jo atstovas, jurisdikcijai.	Visiškas
11) **standartas** – standartas, kaip apibrėžta Reglamento (ES) Nr. 1025/2012 2 straipsnio 1 punkte;	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> 17. 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	Visiškas

	žvalgybos įstatyme, Lietuvos Respublikos kriminalinės žvalgybos įstatyme, Lietuvos Respublikos viešojo administravimo įstatyme, Lietuvos Respublikos nesąžiningos komercinės veiklos vartotojams draudimo įstatyme, Lietuvos Respublikos smulkiojo ir vidutinio verslo plėtros 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.	
12) **specifikacija** – techninė specifikacija, kaip apibrėžta Reglamento (ES) Nr. 1025/2012 2 straipsnio 4 punkte;	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> 17. 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 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,	Visiškas

	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.	
13) **interneto duomenų srautų mainų taškas (IXP)** – tinklo įrenginys, kuris sudaro sąlygas sujungti daugiau nei dvi nepriklausomas autonomines sistemas, visų pirma siekiant palengvinti interneto duomenų srautų mainus; IXP sujungia tik autonomines sistemas; IXP atveju nėra būtina, kad interneto duomenų srautai, perduodami tarp bet kurių naudojamų autonominių sistemų porų, būtų perduodami per bet kurią trečią autonominę sistemą; be to, jis nekeičia tokių srautų ar kitokiu būdu jų netrikdo;	**Ši sąvoka bus perkelta į YSII identifikavimo metodikos pakeitimo projektą.**	
14) **domenų vardų sistema (DNS)** – pagal hierarchiją suskirstyta vardų suteikimo sistema tinkle, kuris persiunčia domenų vardų užklausas;	**Ši sąvoka bus perkelta į YSII identifikavimo metodikos pakeitimo projektą.**	
15) **DNS paslaugų teikėjas** – subjektas, kuris teikia DNS paslaugas internetu;	**Ši sąvoka bus perkelta į YSII identifikavimo metodikos pakeitimo projektą.**	
16) **aukščiausio lygio domenų vardų registras** – subjektas, kuris administruoja ir vykdo interneto domenų vardų registravimą pagal konkretų aukščiausio lygio domeną (ALD);	**Ši sąvoka bus perkelta į YSII identifikavimo metodikos pakeitimo projektą.**	
17) **elektroninė prekyvietė** – skaitmeninė paslauga, kuria sudaromos sąlygos vartotojams ir (arba) komercinės veiklos subjektams, apibrėžtiems atitinkamai Europos Parlamento ir Tarybos direktyvos 2013/11/ES (18) 4 straipsnio 1 dalies a punkte ir b punkte, 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;	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> 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.	Visiškas
18) **interneto paieškos sistema** – skaitmeninė paslauga, kuria sudaromos sąlygos naudotojams vykdyti paiešką iš esmės visose	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas**	Visiškas

svetainėse arba svetainėse konkrečia kalba, remiantis bet kurio dalyko užklausa, naudojant raktinį žodį, frazę arba kitus įvesties duomenis; šioje sistemoje pateikiamos nuorodos, kuriose gali būti su ieškomu turiniu susijusios informacijos;	**2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> 4. **Paieškos internete paslauga** – paslauga, kuria sudaromos sąlygos naudotojams atlikti paiešką svetainėse, remiantis bet kurio dalyko užklausa, naudojant raktinį žodį, frazę arba kitus įvesties duomenis; atliekant paiešką pateikiamos nuorodos, kuriose gali būti su ieškomu turiniu susijusios informacijos.	
19) **debesijos kompiuterijos paslauga** – skaitmeninė paslauga, kuri suteikia prieigą prie kintamo masto pritaikomos bendrų kompiuterijos išteklių bazės.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> **1. Debesijos paslaugos** – paslaugos, kurias teikiant šių paslaugų gavėjai nuotoliniu būdu naudojasi šių paslaugų teikėjų valdoma ryšių ir informacinių sistemų infrastruktūra.	Visiškas
5 straipsnis. Esminių paslaugų operatorių identifikavimas 1. Ne vėliau kaip 2018 m. lapkričio 9 d. valstybės narės kiekviename iš II priede nurodytų sektorių ir subsektorių identifikuoja esminių paslaugų operatorius, kurie yra įsisteigę jų teritorijoje.	**Ši Direktyvos nuostata bus perkelta į YSII identifikavimo metodikos pakeitimo projektą.**	
2. Esminių paslaugų operatorių identifikavimo kriterijai, kaip nurodyta 4 straipsnio 4 punkte, yra šie: a) subjektas teikia paslaugą, kuri yra būtina siekiant užtikrinti ypatingos svarbos visuomeninės ir (arba) ekonominės veiklos vykdymą; b) tos paslaugos teikimas priklauso nuo tinklų ir informacinių sistemų, ir c) incidentas turėtų didelį trikdomąjį poveikį tos paslaugos teikimui.	**YSII identifikavimo metodika** **IV skyrius. Ypatingos svarbos informacinės infrastruktūros identifikavimas** <...> 12. Kriterijai, pagal kuriuos vertinama, kuri informacinė infrastruktūra būtina ypatingos svarbos paslaugos nenutrūkstamam teikimui užtikrinti: 12.1. ypatingos svarbos infrastruktūros objekto teikiama ypatingos svarbos paslauga priklauso nuo šio objekto informacinės infrastruktūros tinkamo veikimo;	Visiškas

	12.2. kibernetinis incidentas ypatingos svarbos infrastruktūros objekto informacinėje infrastruktūroje turėtų esminį poveikį šio objekto teikiamos ypatingos svarbos paslaugos sutrikdymui; 12.3. sutrikus ypatingos svarbos infrastruktūros objekto informacinei infrastruktūrai, nėra kitų alternatyvų šio objekto veikimui užtikrinti teikiant ypatingos svarbos paslaugą.	
3. 1 dalies tikslais kiekviena valstybė narė sudaro 2 dalies a punkte nurodytų paslaugų sąrašą.	**Ši Direktyvos nuostata bus perkelta į YSII identifikavimo metodikos pakeitimo projektą, papildant šios metodikos II skyriaus 4 punkte nustatomą ypatingos svarbos sektorių, jų subsektorių ir ypatingos svarbos paslaugų sąrašą.**	
4. 1 dalies tikslais, kai subjektas teikia 2 dalies a punkte nurodytą paslaugą dviejose ar daugiau valstybių narių, tos valstybės narės konsultuojasi tarpusavyje. Tokios konsultacijos vyksta prieš priimant sprendimą dėl identifikavimo.	**Ši Direktyvos nuostata bus perkelta į YSII identifikavimo metodikos pakeitimo projektą.**	
5. Valstybės narės reguliariai ir ne rečiau kaip kas dvejus metus nuo 2018 m. gegužės 9 d. peržiūri ir prireikus atnaujina identifikuotų esminių paslaugų operatorių sąrašą.	**YSII identifikavimo metodika** **IV skyrius. Ypatingos svarbos informacinės infrastruktūros identifikavimas** <...> 19. Atsakingos institucijos ypatingos svarbos infrastruktūros objektų ir apibendrintus sąrašus atnaujina kas dvejus metus arba atsiradus esminių ypatingos svarbos infrastruktūros objektų ir ypatingos svarbos informacinės infrastruktūros pokyčių (likvidavimas, reorganizavimas, svarbos pokytis, naujos infrastruktūros steigimas ir panašiai). Nurodyti sąrašai atnaujinami atliekant Metodikos III ir IV skyriuose nurodytus veiksmus.	Visiškas
6. Bendradarbiavimo grupės vaidmuo, atsižvelgiant į 11 straipsnyje nurodytas užduotis, yra padėti valstybėms narėms esminių paslaugų operatorių identifikavimo procese laikytis nuoseklaus požiūrio.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
7. 23 straipsnyje nurodytos peržiūros tikslais ir ne vėliau kaip	**1. Kibernetinio saugumo įstatymo pakeitimo įstatymo**	

2018 m. lapkričio 9 d., o vėliau – kas dvejus metus, valstybės narės pateikia Komisijai būtiną informaciją, kad ji galėtų įvertinti šios direktyvos įgyvendinimą, visų pirma, požiūrio, kurio laikosi valstybės narės identifikuodamos esminių paslaugų operatorius, nuoseklumą. Turi būti pateikiama bent ši informacija: a) nacionalinės priemonės, kuriomis sudaromos sąlygos identifikuoti esminių paslaugų operatorius; b) 3 dalyje nurodytų paslaugų sąrašas; c) kiekviename II priede nurodytame sektoriuje identifikuotų esminių paslaugų operatorių skaičius ir jų svarba tam sektoriui; d) ribos, jei jų esama, siekiant nustatyti atitinkamą tiekimo lygį atsižvelgiant į naudotojų, kurie priklauso nuo tos paslaugos, kaip nurodyta 6 straipsnio 1 dalies a punkte, skaičių arba to konkretaus esminių paslaugų operatoriaus svarbą, kaip nurodyta 6 straipsnio 1 dalies f punkte. Siekdama prisidėti prie palyginamos informacijos teikimo, Komisija, kuo įmanoma labiau atsižvelgdama į ENISA nuomonę, gali priimti atitinkamas technines gaires dėl parametrų, taikomų šioje dalyje nurodytai informacijai.	**projektas** **9 straipsnis. Nacionalinis kibernetinio saugumo centras** <...> 2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką: <...> 14) Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka bendradarbiauja su tarptautinių organizacijų kompetentingomis institucijomis, jų įsteigtomis bendradarbiavimo grupėmis bei užsienio valstybių kompetentingomis institucijomis ir tarnybomis vykdydamas šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje; <...> **2. Ši Direktyvos nuostata bus perkelta į YSII identifikavimo metodikos pakeitimo projektą, nustatant informacijos teikimo Komisijai reikalavimus.**	
6 straipsnis. Didelis trikdomasis poveikis 1. Nustatydamos, ar trikdomasis poveikis yra didelis, kaip nurodyta 5 straipsnio 2 dalies c punkte, valstybės narės atsižvelgia bent į šiuos tarpsektorinius veiksnius: a) naudotojų, kurie priklauso nuo atitinkamo subjekto teikiamos paslaugos, skaičių; b) kitų II priede nurodytų sektorių priklausomybę nuo to subjekto teikiamos paslaugos; c) poveikį, kurį incidentai dėl savo masto ir trukmės galėtų daryti ekonominei ir visuomeninei veiklai arba viešajam saugumui; d) to subjekto užimamą rinkos dalį;	**YSII identifikavimo metodika** **III skyrius. Ypatingos svarbos infrastruktūros objektų nustatymas** <...> 7. Infrastruktūros objektų svarba nustatoma įvertinus potencialią žalą, kurią patirtų valstybė, jeigu infrastruktūros objektas būtų sunaikintas, sugadintas ar sutriktų jo veikla. Infrastruktūros objekto svarba vertinama remiantis šiais bendraisiais potencialios žalos, padarytos sunaikinus, sugadinus infrastruktūros objektą ar sutrikus jo veiklai, kriterijais: 7.1. įtaka ypatingos svarbos paslaugos teikimo sutrikdymui;	Visiškas

e) geografinę teritorijos, kurią galėtų paveikti incidentas, aprėptį; f) subjekto svarbą pakankamam paslaugos lygiui išlaikyti, atsižvelgiant į esamas tos paslaugos teikimo alternatyvas. 2. Siekdamos nustatyti, ar incidentas turėtų didelį trikdomąjį poveikį, valstybės narės taip pat prireikus atsižvelgia į konkretiems sektoriams būdingus veiksnius.	7.2. pavojus gyventojų gyvybei ir sveikatai; 7.3. ekonominė žala valstybei; 7.4. žala aplinkai; 7.5. įtaka gyventojų pasitikėjimui valstybe; 7.6. infrastruktūros objekto įtaka kito infrastruktūros objekto, užtikrinančio tos pačios ypatingos svarbos paslaugos teikimą, nepertraukiamam funkcionavimui; 7.7. infrastruktūros objekto įtaka kito infrastruktūros objekto, užtikrinančio kitų ypatingos svarbos paslaugų teikimą, nepertraukiamam funkcionavimui; 7.8. įtaka viešojo saugumo užtikrinimui; 7.9. žala kitoms Europos Sąjungos valstybėms narėms; 7.10. įtaka valstybės integracijos į europines ir transatlantines institucijas stiprinimui ir tarptautinių saugumo garantijų užsitikrinimui; 7.11. infrastruktūros objekto užimamą rinkos dalį. 8. Atsakinga institucija pagal poreikį papildomai nustato ir įvertina jos veiklos srities sektoriaus specifinius kriterijus, galinčius turėti įtakos jos veiklos srityje veikiančių infrastruktūros objektų veiklai. <...> **IV skyrius. Ypatingos svarbos informacinės infrastruktūros identifikavimas** <...> 12. Kriterijai, pagal kuriuos vertinama, kuri informacinė infrastruktūra būtina ypatingos svarbos paslaugos nenutrūkstamam teikimui užtikrinti: 12.1. ypatingos svarbos infrastruktūros objekto teikiama ypatingos svarbos paslauga priklauso nuo šio objekto informacinės infrastruktūros tinkamo veikimo; 12.2. kibernetinis incidentas ypatingos svarbos infrastruktūros objekto informacinėje infrastruktūroje turėtų esminį poveikį šio	

	objekto teikiamos ypatingos svarbos paslaugos sutrikdymui; 12.3. sutrikus ypatingos svarbos infrastruktūros objekto informacinei infrastruktūrai, nėra kitų alternatyvų šio objekto veikimui užtikrinti teikiant ypatingos svarbos paslaugą. **YSII identifikavimo metodikos 1 ir 2 priedai**	
7 straipsnis. Nacionalinė tinklų ir informacinių sistemų saugumo strategija 1. Kiekviena valstybė narė priima nacionalinę tinklų ir informacinių sistemų saugumo strategiją, kurioje apibrėžiami strateginiai tikslai ir tinkamos politikos bei reguliavimo priemonės aukšto lygio tinklų ir informacinių sistemų saugumui pasiekti ir išlaikyti, ir kuri apima bent II priede nurodytus sektorius ir III priede nurodytas paslaugas. Nacionalinėje tinklų ir informacinių sistemų saugumo strategijoje visų pirma nagrinėjami šie klausimai: a) nacionalinės tinklų ir informacinių sistemų saugumo strategijos tikslai ir prioritetai; b) valdymo sistema, skirta nacionalinės tinklų ir informacinių sistemų saugumo strategijos tikslams ir prioritetams įgyvendinti, įskaitant valdžios įstaigų ir kitų atitinkamų subjektų vaidmenis ir įsipareigojimus; c) parengties, reagavimo ir atkūrimo priemonių, įskaitant viešojo ir privačiojo sektorių bendradarbiavimą, nustatymas; d) švietimo, informuotumo didinimo ir mokymo programų, susijusių su nacionaline tinklų ir informacinių sistemų saugumo strategija, nurodymas; e) mokslinių tyrimų ir plėtros planų, susijusių su nacionaline tinklų ir informacinių sistemų saugumo strategija, nurodymas; f) rizikos vertinimo planas, skirtas rizikai nustatyti; g) įvairių subjektų, dalyvaujančių įgyvendinant nacionalinę tinklų ir informacinių sistemų saugumo strategiją, sąrašas.	**1. Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **5 straipsnis. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos** 1. Kibernetinio saugumo politikos strateginius tikslus, prioritetus ir jiems pasiekti būtinas priemones nustato Lietuvos Respublikos Vyriausybė (toliau – Vyriausybė). <...> **6 straipsnis. Vyriausybės įgaliojimai kibernetinio saugumo srityje** Vyriausybė: 1) tvirtina Nacionalinę kibernetinio saugumo strategiją; <...> **2. Strategijos projektas**	

2. Valstybės narės gali prašyti ENISA padėti parengti nacionalines tinklų ir informacinių sistemų saugumo strategijas. 3. Valstybės narės pateikia Komisijai nacionalines tinklų ir informacinių sistemų saugumo strategijas per tris mėnesius nuo jų priėmimo. Tai darydamos valstybės narės gali nepranešti apie su nacionaliniu saugumu susijusius strategijos elementus.		
8 straipsnis. Nacionalinės kompetentingos institucijos ir bendrasis informacinis centras 1. Kiekviena valstybė narė paskiria vieną ar daugiau nacionalinių tinklų ir informacinių sistemų saugumo kompetentingų institucijų (toliau – kompetentinga institucija), kurių veikla apima bent II priede nurodytus sektorius ir III priede nurodytas paslaugas. Valstybės narės gali paskirti šį vaidmenį esamai institucijai arba institucijoms.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **5 straipsnis. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos** <...> 2. Kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija (toliau – 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, policija ir kitos institucijos pagal savo kompetenciją.	Visiškas
2. Kompetentingos institucijos stebi šios direktyvos taikymą nacionaliniu lygmeniu.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **5 straipsnis. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos** <...> 2. Kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija (toliau – Krašto apsaugos ministerija). Nacionalinis kibernetinio saugumo centras formuojant kibernetinio saugumo politiką dalyvauja tiek, kiek šiame įstatyme nustatytoms funkcijoms atlikti reikia nustatyti	Visiškas

	kibernetinio saugumo subjektų veiklos teisinį reguliavimą. 3. Kibernetinio saugumo politiką įgyvendina Nacionalinis kibernetinio saugumo centras, Valstybinė duomenų apsaugos inspekcija, policija ir kitos institucijos pagal savo kompetenciją.	
3. Kiekviena valstybė narė paskiria **nacionalinį bendrąjį tinklų ir informacinių sistemų saugumo informacinį centrą** (toliau – bendrasis informacinis centras). Valstybės narės gali paskirti šį vaidmenį esamai institucijai. Kai valstybė narė paskiria tik vieną kompetentingą instituciją, ta kompetentinga institucija taip pat vykdo bendrojo informacinio centro funkcijas.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **9 straipsnis. Nacionalinis kibernetinio saugumo centras** 2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką: <...> 14) Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka bendradarbiauja su tarptautinių organizacijų kompetentingomis institucijomis, jų įsteigtomis bendradarbiavimo grupėmis bei užsienio valstybių kompetentingomis institucijomis ir tarnybomis vykdydamas šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje; <...>.	Visiškas
4. Bendrasis informacinis centras atlieka ryšių palaikymo funkciją, kad būtų užtikrintas tarpvalstybinis valstybių narių institucijų bendradarbiavimas ir bendradarbiavimas su kitų valstybių narių atitinkamomis institucijomis, 11 straipsnyje nurodyta Bendradarbiavimo grupe ir 12 straipsnyje nurodytu CSIRT tinklu.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **9 straipsnis. Nacionalinis kibernetinio saugumo centras** 2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką: <...> 14) Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka bendradarbiauja su tarptautinių organizacijų kompetentingomis institucijomis, jų įsteigtomis bendradarbiavimo grupėmis bei užsienio valstybių kompetentingomis institucijomis ir tarnybomis vykdydamas šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje; <...>	Visiškas

5. Valstybės narės užtikrina, kad kompetentingos institucijos ir bendrieji informaciniai centrai turėtų tinkamų išteklių, kad efektyviai ir veiksmingai vykdytų jiems pavestas užduotis ir taip įgyvendintų šios direktyvos tikslus. Valstybės narės užtikrina efektyvų, veiksmingą ir saugų į **Bendradarbiavimo grupę** paskirtų atstovų bendradarbiavimą.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
6. Kompetentingos institucijos ir bendrasis informacinis centras prireikus ir pagal nacionalinę teisę konsultuojasi ir bendradarbiauja su atitinkamomis nacionalinėmis teisėsaugos institucijomis ir nacionalinėmis duomenų apsaugos institucijomis.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **15 straipsnis. Tarpinstitucinis bendradarbiavimas tiriant kibernetinius incidentus** 1. Nacionalinis kibernetinio saugumo centras ir policija konsultuojasi ir bendradarbiauja tiriant kibernetinius incidentus, keičiasi su kibernetinių incidentų tyrimais susijusia informacija, reikalinga pagal kompetenciją institucijų vykdomoms funkcijoms atlikti. Prireikus apie kibernetinių incidentų tyrimą gali būti informuojami kiti kriminalinės žvalgybos subjektai ir (arba) žvalgybos institucijos. 2. Nacionalinis kibernetinio saugumo centras ir Valstybinė duomenų apsaugos inspekcija bendradarbiauja tiriant kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, keičiasi informacija, reikalinga teisės aktų nustatytoms funkcijoms, susijusioms su kibernetinių incidentų, pažeidžiančių asmens duomenų saugumą, tyrimu, atlikti. 3. Tarpinstitucinio bendradarbiavimo valdant ir tiriant kibernetinius incidentus tvarka nustatoma Nacionaliniame kibernetinių incidentų valdymo plane.	Visiškas
7. Kiekviena valstybė narė nedelsdama praneša Komisijai apie kompetentingos institucijos ir bendrojo informacinio centro paskyrimą, jų užduotis ir visus vėlesnius jų pakeitimus. Kiekviena valstybė narė viešai paskelbia apie kompetentingos institucijos ir bendrojo informacinio centro paskyrimą. Komisija paskelbia paskirtų bendrųjų informacinių centrų sąrašą.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	

9 straipsnis. Reagavimo į kompiuterinius saugumo incidentus tarnybos (CSIRT) 1. Kiekviena valstybė narė paskiria vieną ar daugiau CSIRT, atitinkančią I priedo 1 punkte nustatytus reikalavimus, kurios veikla apima bent II priede nurodytus sektorius ir III priede nurodytas paslaugas, ir kuri yra atsakinga už rizikos bei incidentų valdymą vadovaujantis tiksliai apibrėžtu procesu. CSIRT gali būti įsteigta kompetentingoje institucijoje.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **9 straipsnis. Nacionalinis kibernetinio saugumo centras** 2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką: 7) nacionaliniu lygmeniu stebi kibernetinius incidentus ir vykdo rizikos kibernetinėje erdvėje bei kibernetinių incidentų analizę; <...> 9) nacionaliniu lygmeniu organizuoja kibernetinių incidentų kibernetinio saugumo subjektų ryšių ir informacinėse sistemose valdymą; <...> 12) dalyvauja kibernetinio saugumo krizių valdyme; <...>	Visiškas
2. Valstybės narės užtikrina, kad CSIRT turėtų tinkamų išteklių, kad galėtų efektyviai vykdyti savo užduotis, nustatytas I priedo 2 punkte. Valstybės narės užtikrina efektyvų, veiksmingą ir saugų jų CSIRT bendradarbiavimą 12 straipsnyje nurodytame CSIRT tinkle.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
3. Valstybės narės užtikrina, kad jų CSIRT turėtų prieigą prie tinkamos, saugios ir atsparios nacionalinio lygmens ryšių ir informacinės infrastruktūros.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
4. Valstybės narės informuoja Komisiją apie jų CSIRT incidentų valdymo proceso mastą ir pagrindinius elementus.	**1. Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **9 straipsnis. Nacionalinis kibernetinio saugumo centras** 2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką: <...> 14) Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka bendradarbiauja su tarptautinių organizacijų	

	kompetentingomis institucijomis, jų įsteigtomis bendradarbiavimo grupėmis bei užsienio valstybių kompetentingomis institucijomis ir tarnybomis vykdydamas šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje; <...> **2. Šio direktyvos straipsnio nuostata dėl Komisijos informavimo bus perkelta į Kibernetinių incidentų valdymo plano projektą.**	
5. Valstybės narės gali paprašyti ENISA padėti kurti nacionalines CSIRT.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
10 straipsnis. Bendradarbiavimas nacionaliniu lygmeniu 1. Kai tos pačios valstybės narės kompetentinga institucija, bendrasis informacinis centras ir CSIRT yra atskiri, jie *bendradarbiauja*, kad vykdytų šioje direktyvoje nustatytas pareigas.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia, nes kompetentinga institucija, bendrasis informacinis centras ir CSIRT yra ta pati institucija.**	
2. Valstybės narės užtikrina, kad kompetentingos institucijos arba CSIRT gautų pagal šią direktyvą pateiktus pranešimus apie incidentus. Kai valstybė narė nusprendžia, kad CSIRT neturi gauti pranešimų, minėtai CSIRT, kiek tai būtina jos užduotims vykdyti, suteikiama prieiga prie duomenų apie incidentus, apie kuriuos pranešė esminių paslaugų operatoriai pagal 14 straipsnio 3 ir 5 dalis arba skaitmeninių paslaugų teikėjai pagal 16 straipsnio 3 ir 6 dalis.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **12 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos** 1. Kibernetinio saugumo subjektai: <...> 3) Nacionaliniame kibernetinių incidentų valdymo plane nustatytomis sąlygomis ir tvarka informuoja Nacionalinį kibernetinio saugumo centrą apie jų valdomose ir (arba) tvarkomose ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones. <...>	Visiškas

3. Valstybės narės užtikrina, kad kompetentingos institucijos arba CSIRT informuotų bendruosius informacinius centrus apie pagal šią direktyvą pateiktus pranešimus apie incidentus. Ne vėliau kaip 2018 m. rugpjūčio 9 d. ir po to kiekvienais metais bendrasis informacinis centras Bendradarbiavimo grupei pateikia suvestinę ataskaitą apie gautus pranešimus, kurioje, be kita ko, nurodomas pranešimų skaičius ir incidentų, apie kuriuos pranešta, pobūdis, taip pat veiksmai, kurių buvo imtasi pagal 14 straipsnio 3 ir 5 dalis bei 16 straipsnio 3 ir 6 dalis.	**1. Direktyvos nuostatos dėl bendrojo informacijos centro informavimo į nacionalinę teisę perkelti nereikia, nes kompetentinga institucija, bendrasis informacinis centras ir CSIRT yra ta pati institucija.** **2. Šio direktyvos straipsnio nuostata dėl Bendradarbiavimo grupės informavimo bus perkelta į Kibernetinių incidentų valdymo plano projektą.**	
11 straipsnis. Bendradarbiavimo grupė 1. Siekiant remti ir palengvinti valstybių narių strateginį bendradarbiavimą ir keitimąsi informacija, didinti atsakomybę bei tarpusavio pasitikėjimą ir užtikrinti aukštą bendrą tinklų ir informacinių sistemų saugumo lygį Sąjungoje, įsteigiama **Bendradarbiavimo grupė**. Bendradarbiavimo grupė vykdo savo užduotis remdamasi dvimetėmis darbo programomis, nurodytomis 3 dalies antroje pastraipoje. 2. Bendradarbiavimo grupę sudaro valstybių narių, Komisijos ir ENISA atstovai. Prireikus Bendradarbiavimo grupė gali pakviesti atitinkamų suinteresuotųjų subjektų atstovų dalyvauti jos darbe. Komisija teikia sekretoriato paslaugas. 3. Bendradarbiavimo grupė vykdo šias užduotis: a) teikia strategines gaires dėl CSIRT tinklo, įsteigto pagal 12 straipsnį, veiklos; b) keičiasi geriausia keitimosi informacija, susijusia su pranešimu apie incidentus, kaip nurodyta 14 straipsnio 3 ir 5 dalyse bei 16 straipsnio 3 ir 6 dalyse, srityje, praktika; c) keičiasi valstybių narių geriausia praktika ir, bendradarbiaudama su ENISA, padeda valstybėms narėms stiprinti gebėjimus tinklų ir informacinių sistemų saugumo	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	

srityje; d) aptaria valstybių narių pajėgumus bei parengtį ir savanoriškai vertina nacionalines tinklų ir informacinių sistemų saugumo strategijas ir CSIRT veiksmingumą, taip pat nustato geriausią praktiką; e) keičiasi informacija ir geriausia informuotumo didinimo ir mokymo srities praktika; f) keičiasi informacija ir geriausia praktika tinklų ir informacinių sistemų saugumo mokslinių tyrimų ir plėtros srityje; g) prireikus keičiasi patirtimi su tinklų ir informacinių sistemų saugumu susijusiais klausimais su atitinkamomis Sąjungos institucijomis, įstaigomis, tarnybomis ir agentūromis; h) aptaria 19 straipsnyje nurodytus standartus ir specifikacijas su atitinkamų Europos standartizacijos organizacijų atstovais; i) renka geriausią praktiką, susijusią su rizika ir incidentais; j) kasmet nagrinėja 8 straipsnio 8 dalies antroje pastraipoje nurodytas suvestines ataskaitas; k) aptaria darbą, vykdomą pratybų, susijusių su tinklų ir informacinių sistemų saugumu, švietimo programų ir mokymo srityje, įskaitant ENISA atliekamą darbą; l) padedant ENISA keičiasi geriausia praktika, susijusia su valstybių narių vykdomu esminių paslaugų operatorių identifikavimu, be kita ko, susijusiu su valstybių tarpusavio priklausomybe rizikos ir incidentų atveju; m) aptaria pranešimų apie incidentus, kaip nurodyta 14 ir 16 straipsniuose, teikimo tvarką. Bendradarbiavimo grupė ne vėliau kaip 2018 m. vasario 9 d., o vėliau – kas dvejus metus, parengia darbo programą dėl veiksmų, kurių reikia imtis siekiant įgyvendinti tikslus ir užduotis, kurie turi atitikti šios direktyvos tikslus. 4. 23 straipsnyje nurodytos peržiūros tikslais ir ne vėliau kaip 2018 m. rugpjūčio 9 d., o vėliau – kas pusantrų metų,		

Bendradarbiavimo grupė parengia ataskaitą, kurioje įvertina patirtį, įgytą vykdant strateginį bendradarbiavimą pagal šį straipsnį. 5. Komisija priima įgyvendinimo aktus, kuriais nustatoma procedūrinė tvarka, būtina Bendradarbiavimo grupės veikimui užtikrinti. Tie įgyvendinimo aktai priimami laikantis 22 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros. Pirmos pastraipos taikymo tikslais Komisija pateikia pirmąjį įgyvendinimo akto projektą 22 straipsnio 1 dalyje nurodytam komitetui ne vėliau kaip 2017 m. vasario 9 d.		
12 straipsnis. CSIRT tinklas 1. Siekiant prisidėti prie valstybių narių tarpusavio pasitikėjimo bei atsakomybės didinimo ir skatinti greitą bei veiksmingą operatyvinį bendradarbiavimą, įsteigiamas nacionalinių CSIRT tinklas. 2. CSIRT tinklą sudaro valstybių narių CSIRT ir ES CERT atstovai. Komisija dalyvauja CSIRT tinklo veikloje stebėtojos teisėmis. ENISA teikia sekretoriato paslaugas ir aktyviai remia CSIRT tarpusavio bendradarbiavimą. 3. CSIRT tinklas vykdo šias užduotis: a) keičiasi informacija apie CSIRT paslaugas, operacijas ir bendradarbiavimo pajėgumus; b) valstybės narės, kurią galėjo paveikti incidentas, CSIRT atstovo prašymu keičiasi skelbtina komercine informacija, susijusia su tuo incidentu bei susijusia rizika, ir ją aptaria; tačiau bet kurios valstybės narės CSIRT gali atsisakyti prisidėti prie tos diskusijos, jei kyla rizika, kad bus pakenkta incidento tyrimui; c) savanoriškai keičiasi skelbtina informacija apie pavienius incidentus ir ją skelbia; d) valstybės narės CSIRT atstovo prašymu aptaria ir, kai įmanoma, apibrėžia koordinuotus tos valstybės narės jurisdikcijai priklausančius reagavimo į incidentą, kuris buvo	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	

nustatytas, veiksmus; e) padeda valstybėms narėms šalinti tarpvalstybinius incidentus remiantis savanoriško valstybių narių savitarpio pagalbos teikimo principu; f) aptaria, nagrinėja ir nustato tolesnes operatyvinio bendradarbiavimo formas, be kita ko, susijusias su: i) rizikos ir incidentų kategorijomis, ii) išankstiniais įspėjimais, iii) savitarpio pagalba, iv) koordinavimo principais ir tvarka tuo atveju, kai valstybės narės reaguoja į tarpvalstybinę riziką ir incidentus; g) informuoja Bendradarbiavimo grupę apie savo veiklą ir tolesnes operatyvinio bendradarbiavimo formas, aptartas pagal f punktą, ir prašo tuo klausimu rekomendacijų; h) aptaria per pratybas, susijusias su tinklų ir informacinių sistemų saugumu, įskaitant per ENISA rengtas pratybas, įgytą patirtį; i) atskiros CSIRT prašymu aptaria tos CSIRT pajėgumus ir parengtį; j) teikia gaires siekiant palengvinti operatyvinės praktikos konvergenciją taikant šio straipsnio nuostatas dėl operatyvinio bendradarbiavimo. 4. 23 straipsnyje nurodytos peržiūros tikslais ir ne vėliau kaip 2018 m. rugpjūčio 9 d., o vėliau – kas pusantrų metų, CSIRT tinklas parengia ataskaitą, įskaitant išvadas ir rekomendacijas, kurioje įvertina patirtį, įgytą vykdant operatyvinį bendradarbiavimą pagal šį straipsnį. Ta ataskaita taip pat pateikiama Bendradarbiavimo grupei. 5. CSIRT tinklas nustato savo darbo tvarkos taisykles.		
13 straipsnis. Tarptautinis bendradarbiavimas Pagal SESV 218 straipsnį Sąjunga gali sudaryti tarptautinius susitarimus su trečiosiomis šalimis ar tarptautinėmis	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	

organizacijomis, pagal kuriuos joms būtų leidžiama dalyvauti tam tikroje Bendradarbiavimo grupės veikloje ir toks dalyvavimas būtų organizuojamas. Tokiuose susitarimuose atsižvelgiama į poreikį užtikrinti tinkamą duomenų apsaugą.		
14 straipsnis. Saugumo reikalavimai ir pranešimas apie incidentus 1. Valstybės narės užtikrina, kad esminių paslaugų operatoriai imtųsi tinkamų ir proporcingų techninių ir organizacinių priemonių, kad galėtų valdyti riziką, kylančią tinklų ir informacinių sistemų, kuriais jie naudojasi vykdydami savo veiklą, saugumui. Remiantis naujausiais technikos laimėjimais, tomis priemonėmis turi būti užtikrinamas toks tinklų ir informacinių sistemų saugumo lygis, kuris atitinka atsiradusią riziką.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **12 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 Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatoms; 2) Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nustatyta tvarka atlieka rizikos vertinimą ir įdiegia kitas, naujausiais technikos laimėjimais paremtas ir proporcingas nustatytai rizikai suvaldyti, technines ir organizacines kibernetinio saugumo priemones; <...>	Visiškas
2. Valstybės narės užtikrina, kad esminių paslaugų operatoriai imtųsi tinkamų priemonių, kad būtų išvengta incidentų, paveikiančių tinklų ir informacinių sistemų, naudojamų tokių esminių paslaugų teikimui, saugumą, poveikio ir jis būtų kuo labiau sumažintas, siekiant užtikrinti tų paslaugų tęstinumą.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **12 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 Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatoms; 2) Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nustatyta tvarka atlieka rizikos vertinimą ir įdiegia kitas, naujausiais	Visiškas

	technikos laimėjimais paremtas ir proporcingas nustatytai rizikai suvaldyti, technines ir organizacines kibernetinio saugumo priemones; <...> 6) paskiria kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, ir Nacionaliniam kibernetinio saugumo centrui pateikia paskirto asmens ar padalinio kontaktinę informaciją; <...> **13 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, parengia, patvirtina ir Nacionaliniam kibernetinio saugumo centrui pateikia kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus; <...> 3) ne rečiau kaip kartą per metus išbando kibernetinių incidentų valdymo planų veikimą, o 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.	

	<...>	
3. Valstybės narės užtikrina, kad esminių paslaugų operatoriai be nepagrįsto delsimo praneštų kompetentingai institucijai arba CSIRT apie incidentus, kurie turi didelį poveikį jų teikiamų esminių paslaugų tęstinumui. Pranešimuose pateikiama informacija, kuria remdamasi kompetentinga institucija arba CSIRT galėtų nustatyti tarpvalstybinį incidento poveikį. Pranešančiajai šaliai dėl to netenka didesnė atsakomybė.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **12 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos** 1. Kibernetinio saugumo subjektai: <...> 3) Nacionaliniame kibernetinių incidentų valdymo plane nustatytomis sąlygomis ir tvarka informuoja Nacionalinį kibernetinio saugumo centrą apie jų valdomose ir (arba) tvarkomose ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones. <...>	Visiškas
4. Siekiant nustatyti incidento poveikio mastą, visų pirma atsižvelgiama į šiuos parametrus: a) naudotojų, kuriuos paveikė esminės paslaugos sutrikdymas, skaičių; b) incidento trukmę; c) geografinę teritorijos, kurią paveikė incidentas, aprėptį.	**Šio Direktyvos straipsnio nuostata bus perkelta į Kibernetinių incidentų valdymo plano projektą.**	
5. Remdamasi esminių paslaugų operatoriaus pranešime pateikta informacija, kompetentinga institucija arba CSIRT informuoja kitą (-as) paveiktą (-as) valstybę (-es) narę (-es), ar incidentas daro didelį poveikį esminių paslaugų tęstinumui toje valstybėje narėje. Tai darydama kompetentinga institucija arba CSIRT, laikydamosi Sąjungos teisės arba Sąjungos teisę atitinkančių nacionalinės teisės aktų, saugo esminių paslaugų operatoriaus saugumo ir komercinius interesus, taip pat jo pranešime pateiktos informacijos konfidencialumą. Atsižvelgdamos į aplinkybes, kompetentinga institucija arba CSIRT pranešančiajam esminių paslaugų operatoriui pateikia atitinkamą informaciją apie tolesnę veiklą, susijusią su jo	**Šio Direktyvos straipsnio nuostata bus perkelta į Kibernetinių incidentų valdymo plano projektą.**	

pranešimu, kaip antai informaciją, kuria remiantis incidentas būtų veiksmingai valdomas. Kompetentingos institucijos arba CSIRT prašymu bendrasis informacinis centras perduoda pirmoje pastraipoje nurodytus pranešimus kitų paveiktų valstybių narių bendriesiems informaciniams centrams.		
6. Pasikonsultavusi su pranešančiuoju esminių paslaugų operatoriumi, kompetentinga institucija arba CSIRT gali informuoti visuomenę apie pavienius incidentus, jei būtina informuoti visuomenę siekiant išvengti incidento arba valdyti vykstantį incidentą.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **9 straipsnis. Nacionalinis kibernetinio saugumo centras** <...> 2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką: <...> 13) jei 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 incidentus arba reikalauja, kad tai padarytų kibernetinio saugumo subjektas; <...>	Visiškas
7. Kompetentingos institucijos, veikdamos kartu su Bendradarbiavimo grupe, gali parengti ir priimti gaires dėl aplinkybių, kuriomis esminių paslaugų operatoriai privalo pranešti apie incidentus, įskaitant apie parametrus, pagal kuriuos būtų nustatytas incidento poveikio mastas, kaip nurodyta 4 dalyje.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
15 straipsnis. Įgyvendinimas ir vykdymo užtikrinimas 1. Valstybės narės užtikrina, kad kompetentingos institucijos turėtų reikiamus įgaliojimus ir priemones įvertinti, ar esminių paslaugų operatoriai vykdo savo pareigas pagal 14 straipsnį, ir kokį poveikį tai daro tinklų ir informacinių sistemų saugumui.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **9 straipsnis. Nacionalinis kibernetinio saugumo centras** 2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką: <...>	Visiškas

	1) atlieka kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatoms priežiūrą ir kibernetinio saugumo būsenos tyrimus: <...> 2) duoda nurodymus kibernetinio saugumo subjektams pateikti informaciją, būtiną kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatoms ir kibernetinio saugumo būsenos įvertinimui atlikti; <...>	
2. Valstybės narės užtikrina, kad kompetentingos institucijos turėtų įgaliojimus ir priemones reikalauti, kad esminių paslaugų operatoriai pateiktų: a) informaciją (įskaitant dokumentus apie saugumo politiką), kuri yra būtina norint įvertinti jų tinklų ir informacinių sistemų saugumą; b) įrodymus, kad saugumo politika veiksmingai įgyvendinama, kaip antai, kompetentingos institucijos ar kvalifikuoto auditoriaus atlikto saugumo audito rezultatus, ir pastaruoju atveju jo rezultatus, įskaitant pagrindinius įrodymus, pateiktų kompetentingai institucijai. Prašydama tokios informacijos ar įrodymų, kompetentinga institucija nurodo prašymo tikslą ir kokios informacijos prašoma.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **9 straipsnis. Nacionalinis kibernetinio saugumo centras** 2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką: <...> 2) duoda nurodymus kibernetinio saugumo subjektams pateikti informaciją, būtiną kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatoms ir kibernetinio saugumo būsenos įvertinimui atlikti; <...>	Visiškas
3. Įvertinusi 2 dalyje nurodytą informaciją arba saugumo auditų rezultatus, kompetentinga institucija gali pateikti privalomus nurodymus esminių paslaugų operatoriams ištaisyti nustatytus trūkumus.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **9 straipsnis. Nacionalinis kibernetinio saugumo centras** <...> 2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:	Visiškas

	<...> 4) duoda nurodymus, susijusius su kibernetinio saugumo užtikrinimu ir nustatytų kibernetinio saugumo trūkumų pašalinimu, nustato 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; <...>	
4. Kompetentinga institucija, nagrinėdama incidentus, dėl kurių pažeidžiamas asmens duomenų saugumas, glaudžiai bendradarbiauja su duomenų apsaugos institucijomis.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **15 straipsnis. Tarpinstitucinis bendradarbiavimas tiriant kibernetinius incidentus** <...> 2. Nacionalinis kibernetinio saugumo centras ir Valstybinė duomenų apsaugos inspekcija bendradarbiauja tiriant kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, keičiasi informacija, reikalinga teisės aktų nustatytoms funkcijoms, susijusioms su kibernetinių incidentų, pažeidžiančių asmens duomenų saugumą, tyrimu, atlikti.	Visiškas
16 straipsnis. Saugumo reikalavimai ir pranešimas apie incidentus 1. Valstybės narės užtikrina, kad skaitmeninių paslaugų teikėjai nustatytų tinkamas ir proporcingas technines ir organizacines priemones ir jų imtųsi, kad galėtų valdyti riziką, kylančią tinklų ir informacinių sistemų, kuriais jie naudojasi teikdami III priede nurodytas paslaugas Sąjungoje, saugumui. Remiantis naujausiais technikos laimėjimais, tomis priemonėmis užtikrinamas toks tinklų ir informacinių sistemų saugumo lygis, kuris atitinka atsiradusią riziką, ir atsižvelgiama į šiuos elementus: a) sistemų ir įrenginių saugumą;	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **12 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos** 1. Kibernetinio saugumo subjektai: <...> 2) Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nustatyta tvarka atlieka rizikos vertinimą ir įdiegia kitas, naujausiais technikos laimėjimais paremtas ir proporcingas nustatytai rizikai suvaldyti, technines ir organizacines kibernetinio saugumo	Visiškas

b) incidentų valdymą; c) veiklos tęstinumo valdymą; d) stebėseną, auditą ir bandymus; e) atitiktį tarptautiniams standartams.	priemones; <...>	
2. Valstybės narės užtikrina, kad skaitmeninių paslaugų teikėjai imtųsi priemonių, kad būtų išvengta incidentų, darančių poveikį jų tinklų ir informacinių sistemų saugumui, poveikio III priede nurodytoms Sąjungoje teikiamoms paslaugoms ir jis būtų kuo labiau sumažintas, siekiant užtikrinti tų paslaugų tęstinumą.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **12 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 Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatoms; <...>	Visiškas
3. Valstybės narės užtikrina, kad skaitmeninių paslaugų teikėjai be nepagrįsto delsimo praneštų kompetentingai institucijai arba CSIRT apie incidentą, kuris turi didelį poveikį III priede nurodytos paslaugos, kurią jie teikia Sąjungoje, teikimui. Pranešimuose pateikiama informacija, kuria remdamasi kompetentinga institucija arba CSIRT galėtų nustatyti tarpvalstybinio poveikio mastą. Pranešančiajai šaliai dėl to netenka didesnė atsakomybė.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **12 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos** 1. Kibernetinio saugumo subjektai: <...> 3) Nacionaliniame kibernetinių incidentų valdymo plane nustatytomis sąlygomis ir tvarka informuoja Nacionalinį kibernetinio saugumo centrą apie jų valdomose ir (arba) tvarkomose ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones. <...>	Visiškas
4. Siekiant nustatyti, ar incidentas sukelia didelį poveikį, visų pirma atsižvelgiama į šiuos parametrus: a) naudotojų, kuriuos paveikė incidentas, skaičių, visų pirma naudotojų, kurių pačių paslaugų teikimas priklauso nuo tos paslaugos;	**1. Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **12 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos**	

b) incidento trukmę; c) geografinę teritorijos, kurią paveikė incidentas, aprėptį; d) paslaugos veikimo sutrikdymo mastą; e) poveikio ekonominei ir visuomeninei veiklai mastą. Pareiga pranešti apie incidentą taikoma tik tuo atveju, kai skaitmeninių paslaugų teikėjas gali naudotis informacija, kuri reikalinga įvertinti incidento poveikį atsižvelgiant į pirmoje pastraipoje nurodytus parametrus.	1. Kibernetinio saugumo subjektai: <...> 3) Nacionaliniame kibernetinių incidentų valdymo plane nustatytomis sąlygomis ir tvarka informuoja Nacionalinį kibernetinio saugumo centrą apie jų valdomose ir (arba) tvarkomose ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones. <...> **2. Šio Direktyvos straipsnio nuostatos dėl incidento poveikio nustatymo parametrų bus perkeltos į Nacionalinio kibernetinių incidentų valdymo plano pakeitimo projektą.**	
5. Kai esminių paslaugų teikėjas priklauso nuo trečiosios šalies skaitmeninių paslaugų teikėjo teikdamas paslaugą, kuri yra būtina siekiant užtikrinti ypatingos svarbos visuomeninės ir ekonominės veiklos vykdymą, tas operatorius praneša apie bet kokį didelį poveikį esminių paslaugų tęstinumui, kurį padarė incidentas, paveikęs skaitmeninių paslaugų teikėją.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **13 straipsnis. Specialiosios kibernetinio saugumo subjektų pareigos** 1. Ypatingos svarbos informacinės infrastruktūros valdytojai: <...> 2) Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka informuoja skaitmeninių paslaugų teikėjus apie neigiamą poveikį ypatingos svarbos informacinės infrastruktūros veiklai, kurį lėmė skaitmeninių paslaugų teikėjų ryšių ir informacinėse sistemose įvykę sutrikimai; <...>	Visiškas
6. Atitinkamais atvejais, ir visų pirma jei 3 dalyje nurodytas incidentas susijęs su dviem ar daugiau valstybių narių, kompetentinga institucija arba CSIRT informuoja kitas paveiktas valstybes nares. Tai darydamos kompetentingos institucijos, CSIRT ir bendrieji informaciniai centrai, laikydamiesi Sąjungos teisės arba Sąjungos teisę atitinkančių nacionalinės teisės aktų, saugo skaitmeninių paslaugų teikėjo saugumo ir komercinius interesus, taip pat pateiktos informacijos konfidencialumą.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **9 straipsnis. Nacionalinis kibernetinio saugumo centras** 2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką: <...> 14) Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka bendradarbiauja su tarptautinių organizacijų	Visiškas

	kompetentingomis institucijomis, jų įsteigtomis bendradarbiavimo grupėmis bei užsienio valstybių kompetentingomis institucijomis ir tarnybomis vykdydamas šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje; <...>	
7. Pasikonsultavusi su atitinkamu skaitmeninių paslaugų teikėju, kompetentinga institucija arba CSIRT ir, prireikus, kitų atitinkamų valstybių narių institucijos arba CSIRT gali informuoti visuomenę apie pavienius incidentus arba reikalauti, kad tai padarytų skaitmeninių paslaugų teikėjas, jei būtina informuoti visuomenę siekiant išvengti incidento ar valdyti vykstantį incidentą arba jei incidento atskleidimas kitais atvejais atitinka viešąjį interesą.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **9 straipsnis. Nacionalinis kibernetinio saugumo centras** <...> 2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką: <...> 13) jei 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 incidentus arba reikalauja, kad tai padarytų kibernetinio saugumo subjektas; <...>	Visiškas
8. Komisija priima įgyvendinimo aktus, kuriais toliau apibrėžiami šio straipsnio 1 dalyje nurodyti elementai ir 4 dalyje išvardyti parametrai. Tie įgyvendinimo aktai priimami laikantis 22 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros ne vėliau kaip 2017 m. rugpjūčio 9 d.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
9. Komisija gali priimti įgyvendinimo aktus, kuriais nustato pranešimo reikalavimams taikytinus formatus ir procedūras. Tie įgyvendinimo aktai priimami laikantis 22 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
10. Nedarant poveikio 1 straipsnio 6 daliai, valstybės narės nenustato jokių papildomų saugumo ar pranešimo reikalavimų skaitmeninių paslaugų teikėjams.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	

11. V skyrius netaikomas mikroįmonėms ir mažosioms įmonėms, kaip apibrėžta Komisijos rekomendacijoje 2003/361/EB.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **12 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos** <...> 2. Šiame straipsnyje nustatytos pareigos netaikomos mažoms ir labai mažoms įmonėms, teikiančioms skaitmenines paslaugas Lietuvos Respublikoje ir (arba) kitoje Europos Sąjungos valstybėje narėje. **13 straipsnis. Specialiosios kibernetinio saugumo subjektų pareigos** <...> 6. Šiame straipsnyje nustatytos pareigos netaikomos mažoms ir labai mažoms įmonėms, teikiančioms skaitmenines paslaugas Lietuvos Respublikoje ir (arba) kitoje Europos Sąjungos valstybėje narėje.	Visiškas
17 straipsnis. Įgyvendinimas ir vykdymo užtikrinimas 1. Valstybės narės užtikrina, kad kompetentingos institucijos imtųsi veiksmų, jei būtina, vykdydamos *ex post* priežiūros priemones, kai gauna įrodymų, kad skaitmeninių paslaugų teikėjas neatitinka 16 straipsnyje nustatytų reikalavimų. Tokius įrodymus gali pateikti kitos valstybės narės, kurioje paslauga teikiama, kompetentinga institucija. 2. 1 dalies taikymo tikslais kompetentingos institucijos turi būtinus įgaliojimus ir priemones reikalauti, kad skaitmeninių paslaugų teikėjai: a) pateiktų informaciją (įskaitant saugumo politikos dokumentus), kuri reikalinga jų tinklų ir informacinių sistemų saugumui įvertinti; b) ištaisytų 16 straipsnyje nustatytų reikalavimų vykdymo pažeidimus.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **9 straipsnis. Nacionalinis kibernetinio saugumo centras** <...> 2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką: <...> 6) gavęs įrodymų iš skaitmeninių paslaugų teikėjo, subjekto, skaitmeninės paslaugos vartotojo arba kitos valstybės narės, kurioje yra teikiama skaitmeninė paslauga, kompetentingos institucijos, prižiūrinčios skaitmeninių paslaugų teikėjų veiklą kibernetinio saugumo srityje, 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	Visiškas

3. Jei skaitmeninių paslaugų teikėjo pagrindinė verslo vieta arba atstovas yra valstybėje narėje, bet jo tinklų ir informacinės sistemos yra vienoje ar daugiau kitų valstybių narių, valstybės narės, kurioje yra pagrindinė verslo vieta arba atstovas, kompetentinga institucija ir tų kitų valstybių narių kompetentingos institucijos prireikus bendradarbiauja ir padeda viena kitai. Tokia pagalba ir bendradarbiavimas gali apimti keitimąsi informacija tarp atitinkamų kompetentingų institucijų ir prašymus vykdyti 2 dalyje nurodytas priežiūros priemones.	saugumo reikalavimų įgyvendinimo trūkumus; <...> 14) Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka bendradarbiauja su tarptautinių organizacijų kompetentingomis institucijomis, jų įsteigtomis bendradarbiavimo grupėmis bei užsienio valstybių kompetentingomis institucijomis ir tarnybomis vykdydamas šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje;	
18 straipsnis. Jurisdikcija ir teritoriškumas 1. Šios direktyvos tikslais laikoma, kad skaitmeninių paslaugų teikėjas priklauso valstybės narės, kurioje yra jo pagrindinė verslo vieta, jurisdikcijai. Laikoma, kad skaitmeninių paslaugų teikėjo pagrindinė verslo vieta yra valstybėje narėje, kai jo pagrindinė buveinė yra toje valstybėje narėje. 2. Skaitmeninių paslaugų teikėjas, kuris nėra įsisteigęs Sąjungoje, bet teikia III priede nurodytas paslaugas Sąjungoje, paskiria atstovą Sąjungoje. Atstovas turi būti įsisteigęs vienoje iš tų valstybių narių, kuriose teikiamos paslaugos. Laikoma, kad skaitmeninių paslaugų teikėjas priklauso valstybės narės, kurioje yra įsisteigęs jo atstovas, jurisdikcijai. 3. Skaitmeninių paslaugų teikėjo atstovo skyrimas nedaro poveikio teisiniams veiksmams, kurie gali būti inicijuoti prieš patį skaitmeninių paslaugų teikėją.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **13 straipsnis. Specialiosios kibernetinio saugumo subjektų pareigos** <...> 5. Skaitmeninių paslaugų teikėjai: <...> 2) skiria atstovą veikti Europos Sąjungoje skaitmeninių paslaugų teikėjo vardu. Atstovas skiriamas, jei skaitmeninių paslaugų teikėjas nėra įsisteigęs Europos Sąjungos valstybėje narėje. Atstovas turi būti fizinis arba juridinis asmuo, įsisteigęs vienoje iš tų valstybių narių, kuriose yra teikiamos skaitmeninės paslaugos. Kibernetinio saugumo politiką įgyvendinančios institucijos turi teisę kreiptis į skaitmeninių paslaugų teikėjo atstovą dėl šiuo įstatymu nustatytų skaitmeninių paslaugų teikėjo pareigų vykdymo. Laikoma, kad skaitmeninių paslaugų teikėjas priklauso valstybės narės, kurioje yra įsisteigęs jo atstovas, jurisdikcijai.	Visiškas
19 straipsnis. Standartizacija 1. Siekdamos skatinti vienodą 14 straipsnio 1 ir 2 dalių bei 16 straipsnio 1 ir 2 dalių įgyvendinimą, valstybės narės, nereikalaudamos taikyti kokios nors konkrečios rūšies technologijos ir nesuteikdamos jai pirmenybės, skatina naudotis	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **3 straipsnis. Kibernetinio saugumo principai** 1. Kibernetinis saugumas grindžiamas bendraisiais teisės principais, elektroninių ryšių veiklos reguliavimo principais ir	Visiškas

europiniais ar tarptautiniu mastu pripažintais standartais ir specifikacijomis, kurie yra svarbūs tinklų ir informacinių sistemų saugumui. 2. ENISA, bendradarbiaudama su valstybėmis narėmis, parengia rekomendacijas ir gaires dėl techninių sričių, kurios turi būti apsvarstytos 1 dalies atžvilgiu, taip pat dėl jau galiojančių standartų, be kita ko, valstybių narių nacionalinių standartų, kuriuose būtų numatyta įtraukti tas sritis.	šiais kibernetinio saugumo principais: <...> 5) standartizacijos ir technologinio neutralumo – įgyvendinant kibernetinio saugumo užtikrinimo 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.	
20 straipsnis. Savanoriškas pranešimas 1. Nedarant poveikio 3 straipsniui, subjektai, kurie nebuvo identifikuoti kaip esminių paslaugų operatoriai ir kurie nėra skaitmeninių paslaugų teikėjai, gali savanoriškai pranešti apie incidentus, kurie daro didelį poveikį jų teikiamų paslaugų tęstinumui. 2. Tvarkydamos tokius pranešimus valstybės narės veikia pagal 14 straipsnyje nustatytą procedūrą. Valstybės narės gali teikti pirmenybę privalomų pranešimų tvarkymui, lyginant su savanoriškais pranešimais. Savanoriški pranešimai tvarkomi tik tuo atveju, jei dėl tokio tvarkymo atitinkamoms valstybėms narėms neužkraunama neproporcinga arba netinkama našta. Dėl savanoriško pranešimo pranešančiajam subjektui nenustatoma jokių pareigų, kurios jam nebūtų buvusios nustatytos, jei jis nebūtų pateikęs to pranešimo.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **4 straipsnis. Savanoriškas pranešimas apie kibernetinius incidentus** 1. Subjektai, kuriems šiuo įstatymu nėra nustatytos pranešimo apie kibernetinius incidentus jų ryšių ir informacinėse sistemose pareigos, gali savanoriškai informuoti Nacionalinį kibernetinio saugumo centrą apie kibernetinius incidentus, kurie daro didelį neigiamą poveikį jų teikiamų paslaugų tęstinumui, ir taikytas kibernetinių incidentų valdymo priemones. Nacionalinis kibernetinio saugumo centras tokius pranešimus tvarko Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka. 2. Subjektui, savanoriškai pranešusiam apie kibernetinį incidentą, nenustatoma jokių pareigų, kurios jam nebūtų nustatytos, jei jis nebūtų pateikęs pranešimo.	Visiškas

21 straipsnis. Sankcijos Valstybės narės nustato sankcijų, taikomų pažeidus pagal šią direktyvą priimtas nacionalines nuostatas, taisykles ir būtinų priemonių užtikrinti, kad šios sankcijos būtų įgyvendinamos. Numatytos sankcijos turi būti *veiksmingos, proporcingos ir atgrasomos.* Valstybės narės praneša apie tas taisykles ir tas priemones Komisijai ne vėliau kaip 2018 m. gegužės 9 d. ir jai praneša apie visus vėlesnius joms įtakos turinčius pakeitimus.	**1. Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **17 straipsnis. Atsakomybė už šio įstatymo ir jo įgyvendinamųjų teisės aktų pažeidimus** Už šio įstatymo ar jo įgyvendinamųjų teisės aktų nustatytų reikalavimų pažeidimus kibernetinio saugumo subjektų administracijos vadovai atsako Lietuvos Respublikos administracinių nusižengimų kodekso nustatyta tvarka. **2. ANKPĮ projektas** **479 straipsnis. Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytos informacijos teikimo pareigos atlikimo pažeidimai** 3. Nacionalinio kibernetinio saugumo centro nurodymų pateikti informaciją, būtiną kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatoms ir kibernetinio saugumo būsenai įvertinti, nevykdymas laiku užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų. **480 straipsnis. Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytų kibernetinio saugumo užtikrinimo pareigų atlikimo pažeidimai** 1. Teisėtų Nacionalinio kibernetinio saugumo centro nurodymų, susijusių su kibernetinio saugumo užtikrinimu, neįvykdymas laiku užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar	

	kitiems atsakingiems asmenims nuo dviejų šimtų penkiasdešimt iki trijų tūkstančių eurų. 2. Kibernetinių incidentų valdymo ypatingos svarbos informacinėje infrastruktūroje plano neparengimas ar nepatvirtinimas arba nepateikimas Nacionaliniam kibernetinio saugumo centrui užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo dviejų šimtų penkiasdešimt iki trijų tūkstančių eurų. 3. Nustatytų Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatų kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų kibernetiniam saugumui užtikrinti nevykdymas užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo dviejų šimtų penkiasdešimt iki trijų tūkstančių keturių šimtų eurų. 4. Šio straipsnio 1, 2, 3 dalyse numatyti administraciniai nusižengimai, padaryti pakartotinai, užtraukia baudą juridinių asmenų vadovams ar kitiems asmenims nuo dviejų tūkstančių iki šešių tūkstančių eurų.	
22 straipsnis. Komiteto procedūra 1. Komisijai padeda Tinklų ir informacinių sistemų saugumo komitetas. Tas komitetas – tai komitetas, kaip nustatyta Reglamente (ES) Nr. 182/2011. 2. Kai daroma nuoroda į šią dalį, taikomas Reglamento (ES) Nr. 182/2011 5 straipsnis.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
23 straipsnis. Peržiūra 1. Ne vėliau kaip 2019 m. gegužės 9 d. Komisija pateikia Europos Parlamentui ir Tarybai ataskaitą, kurioje įvertina požiūrio, kurio laikosi valstybės narės identifikuodamos esminių paslaugų operatorius, nuoseklumą.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	

2. Komisija periodiškai peržiūri šios direktyvos taikymą ir teikia ataskaitą Europos Parlamentui ir Tarybai. Šiuo tikslu ir siekiant tolesnės pažangos vykdant strateginį ir operatyvinį bendradarbiavimą, Komisija atsižvelgia į Bendradarbiavimo grupės ir CSIRT tinklo ataskaitas apie patirtį, įgytą strateginiu ir operatyviniu lygmeniu. Atlikdama peržiūrą Komisija taip pat įvertina II ir III prieduose pateiktus sąrašus ir esminių paslaugų operatorių bei paslaugų II priede nurodytuose sektoriuose identifikavimo nuoseklumą. Pirmoji ataskaita pateikiama ne vėliau kaip 2021 m. gegužės 9 d.		
24 straipsnis. Pereinamojo laikotarpio priemonės 1. Nedarant poveikio 25 straipsniui ir siekiant suteikti valstybėms narėms papildomų tinkamo bendradarbiavimo galimybių direktyvos perkėlimo į nacionalinę teisę laikotarpiu, Bendradarbiavimo grupė ir CSIRT tinklas pradeda atlikti užduotis, nustatytas atitinkamai 11 straipsnio 3 dalyje ir 12 straipsnio 3 dalyje, ne vėliau kaip 2017 m. vasario 9 d. 2. Laikotarpiu nuo 2017 m. vasario 9 d. iki 2018 m. lapkričio 9 d. bei siekiant remti valstybes nares, kad jos esminių paslaugų operatorių identifikavimo procese laikytųsi nuoseklaus požiūrio, Bendradarbiavimo grupė aptaria nacionalinių priemonių, kuriomis sudaromos sąlygos identifikuoti esminių paslaugų operatorius konkrečiame sektoriuje remiantis 5 ir 6 straipsniuose nustatytais kriterijais, taikymo procesą, turinį ir rūšį. Bendradarbiavimo grupė, valstybės narės prašymu, taip pat aptaria konkrečius tos valstybės narės nacionalinių priemonių projektus, kuriais sudaromos sąlygos identifikuoti esminių paslaugų operatorius konkrečiame sektoriuje remiantis 5 ir 6 straipsniuose nustatytais kriterijais. 3. Valstybės narės ne vėliau kaip 2017 m. vasario 9 d. ir šio straipsnio tikslais užtikrina, kad būtų tinkamai atstovaujama Bendradarbiavimo grupėje ir CSIRT tinkle.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	

25 straipsnis. Perkėlimas į nacionalinę teisę 1. Valstybės narės ne vėliau kaip 2018 m. gegužės 9 d. priima ir paskelbia įstatymus ir kitus teisės aktus, būtinus, kad būtų laikomasi šios direktyvos. Apie tai jos nedelsdamos praneša Komisijai. Tas nuostatas jos taiko nuo 2018 m. gegužės 10 d. Valstybės narės, priimdamos tas nuostatas, daro jose nuorodą į šią direktyvą arba tokia nuoroda daroma jas oficialiai skelbiant. Tokios nuorodos darymo tvarką nustato valstybės narės. 2. Valstybės narės pateikia Komisijai šios direktyvos taikymo srityje priimtų nacionalinės teisės aktų pagrindinių nuostatų tekstus.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **2 straipsnis. Įstatymo įsigaliojimas ir įgyvendinimas** 1. Šis įstatymas, išskyrus šio straipsnio 2 dalį, įsigalioja 2018 m. balandžio 9 d. **Kibernetinio saugumo įstatymo pakeitimo įstatymo projekto 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 (OL 2016 L 194, p. 1-30).	Visiškas
26 straipsnis. Įsigaliojimas Ši direktyva įsigalioja dvidešimtą dieną po jos paskelbimo Europos Sąjungos oficialiajame leidinyje.	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
27 straipsnis. Adresatai Ši direktyva skirta valstybėms narėms. Priimta Strasbūre 2016 m. liepos 6 d. Europos Parlamento vardu Pirmininkas M. SCHULZ Tarybos vardu Pirmininkas I. KORČOK	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	
1 priedas. Reagavimo į kompiuterinius saugumo incidentus tarnyboms (CSIRT) keliami reikalavimai ir jų užduotys CSIRT keliami reikalavimai ir jų užduotys yra tinkamai ir aiškiai apibrėžti ir grindžiami nacionaline politika ir (arba) taisyklėmis. Juos sudaro: 1) CSIRT keliami reikalavimai a) CSIRT užtikrina, kad jų ryšio paslaugos būtų lengvai prieinamos išvengiant kritinių funkcionavimo trikties taškų, taip	**Šio Direktyvos straipsnio į nacionalinę teisę perkelti nereikia.**	

pat nustato keletą būdų, kaip bet kuriuo metu susisiekti su jomis ir kitais subjektais. Be to, ryšio kanalai yra aiškiai apibrėžti ir gerai žinomi klientams ir bendradarbiavimo partneriams. b) CSIRT biurai ir pagalbinės informacinės sistemos veikia saugiose vietose. c) Veiklos tęstinumas: i) CSIRT aprūpinamos tinkama prašymų valdymo ir nukreipimo sistema, siekiant palengvinti perdavimą; ii) CSIRT turi pakankamai darbuotojų, kad būtų užtikrintas pasiekiamumas bet kuriuo metu; iii) CSIRT turi infrastruktūrą, kurios tęstinumas yra užtikrintas. Tuo tikslu sukuriamos rezervinių komponentų sistemos ir atsarginės darbo patalpos. d) CSIRT, kai jos to pageidauja, turi galimybę dalyvauti tarptautiniuose bendradarbiavimo tinkluose.		
2) CSIRT užduotys: a) CSIRT užduotys yra bent šios: i) stebėti incidentus nacionaliniu lygmeniu; ii) teikti su įvairia rizika ir incidentais susijusius išankstinius įspėjimus, perspėjimus, skelbimus ir skleisti apie juos informaciją atitinkamiems suinteresuotiesiems subjektams; iii) reaguoti į incidentus; iv) užtikrinti operatyvią rizikos bei incidentų analizę ir informuotumą apie padėtį; v) dalyvauti CSIRT tinkle. b) CSIRT užmezga bendradarbiavimo santykius su privačiuoju sektoriumi. c) Siekiant palengvinti bendradarbiavimą, CSIRT skatina priimti ir naudoti bendrus ar standartizuotus metodus dėl: i) incidentų ir rizikos valdymo procedūrų; ii) incidentų, rizikos ir informacijos klasifikavimo sistemų.	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **9 straipsnis. Nacionalinis kibernetinio saugumo centras** 2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką: 1) atlieka kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo nuostatoms priežiūrą ir kibernetinio saugumo būsenos tyrimus; <...> 7) nacionaliniu lygmeniu stebi kibernetinius incidentus ir vykdo rizikos kibernetinėje erdvėje bei kibernetinių incidentų analizę; <...> 9) nacionaliniu lygmeniu organizuoja kibernetinių incidentų kibernetinio saugumo subjektų ryšių ir informacinėse sistemose valdymą;	Visiškas

	<...> 13) jei 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 incidentus arba reikalauja, kad tai padarytų kibernetinio saugumo subjektas; <...> 14) Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka bendradarbiauja su tarptautinių organizacijų kompetentingomis institucijomis, jų įsteigtomis bendradarbiavimo grupėmis bei užsienio valstybių kompetentingomis institucijomis ir tarnybomis vykdydamas šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje; 17) kartu su verslo subjektais, mokslo ir studijų institucijomis ir kibernetinio saugumo subjektais plėtoja nacionalinį kibernetinį saugumą stiprinančius projektus; <...>	
2 priedas. Subjektų rūšys 4 straipsnio 4 punkto taikymo tikslais 7. Skaitmeninė infrastruktūra — IXP — DNS paslaugų teikėjai — ALD vardų registrai	**Šio Direktyvos priedo nuostatos bus perkeltos į YSII identifikavimo metodikos projektą.**	
3 priedas. Skaitmeninių paslaugų rūšys 4 straipsnio 5 punkto taikymo tikslais 1. Elektroninė prekyvietė 2. Interneto paieškos sistema 3. Debesijos kompiuterijos paslauga	**Kibernetinio saugumo įstatymo pakeitimo įstatymo projektas** **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> 15. **Skaitmeninė paslauga** – ryšių ir informacinėmis	Visiškas

	technologijomis grindžiama paslaugų grupė, apimanti elektroninės prekyvietės ir (arba) paieškos internete, ir (arba) debesijos paslaugas.	

Užsienio reikalų ministras
Linas Linkevičius

Krašto apsaugos viceministras
Vytautas Umbrasas

LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMO NR. XII-1428 PAKEITIMO ĮSTATYMO IR LIETUVOS RESPUBLIKOS ADMINISTRACINIŲ NUSIŽENGIMŲ KODEKSO 479, 480, 589 STRAIPSNIŲ IR PRIEDO PAKEITIMO ĮSTATYMO PROJEKTŲ DERINIMO PAŽYMA

Institucijos pavadinimas, rašto data ir numeris	Pastabos ir pasiūlymai	Argumentai, kodėl neatsižvelgta arba tik iš dalies atsižvelgta į suinteresuotų institucijų ir asmenų pastabas ir pasiūlymus
Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymo projekto		
Europos teisės departamento prie Lietuvos Respublikos teisingumo ministerijos 2018-02-23 išvada Nr. NR-120	6. Įgyvendinant Direktyvos (ES) 2016/1148 8 straipsnio 5 dalį, 9 straipsnio 2, 3 dalis KSĮ projektas arba kitas nacionalinės teisės aktas turėtų nustatyti Nacionalinio kibernetinio saugumo centro veiklos garantijas, kurios pagal Direktyvą (ES) 2016/1148 yra šios: pakankami ištekliai užduočių atlikimui, prieiga prie tinkamos infrastruktūros. Tačiau nei KSĮ projektas, nei kiti teisės aktų projektai, remiantis atitikties lentele, neužtikrina minėtų nuostatų įgyvendinimo.	**Neatsižvelgta.** Nurodytos Direktyvos (ES) 2016/1148 8 straipsnio 5 dalies, 9 straipsnio 2, 3 dalių nuostatomis dėl Nacionalinio kibernetinio saugumo centro veiklos garantijų yra sukuriama pareiga valstybėms narėms užtikrinti, kad Nacionalinis kibernetinio saugumo centras turėtų pakankamai išteklių užduotims atlikti. Šią pareigą valstybė atlieka kiekvienais metais priimdama biudžeto įstatymą, kuriuo ir yra sukuriamos prielaidos veiklos garantijų užtikrinimui. Įstatyme sukuriant formuluotę, kurios esmė, kad institucijai turi būti skiriami pakankami ištekliai, tikslas nebūtų pasiektas. Visų pirma, kiltų klausimas, kas yra *pakankami ištekliai*. Antra, būtų sukuriama dviprasmiška situacija, kad, jeigu tam tikros institucijos atžvilgiu įstatyme nėra įtvirtinama panaši formuluotė, tai reiškia, kad jai pakankami ištekliai neturi būti skiriami. Trečia, valstybė pati sau sukurtų pareiga, kurios įgyvendinimas niekaip nebūtų užtikrinamas. Atsižvelgiant į tai, Krašto apsaugos ministerijos nuomone, tokių Direktyvos (ES) 2016/1148 nuostatų perkėlimas į nacionalinę teisę nesukurtų pridėtinės vertės.
	8. Nesutinkame su atitikties lentelėje pateikta nuomone, kad Direktyvos (ES) 2016/1148 1 priedas nereikalauja įgyvendinančių priemonių. Šiame priede reagavimo į kompiuterinius saugumo	**Neatsižvelgta.** Krašto apsaugos ministerijos nuomone, Direktyvos (ES) 2016/1148 1 priedo 1 dalyje nustatyti reikalavimai (atkreiptinas dėmesys, kad 1 priedo 2 dalyje nustatytas užduotis siūloma perkelti į nacionalinę teisę nustatant Nacionalinio

	incidentus tarnyboms nustatomi atitinkami reikalavimai ir užduotys. Pagal KSĮ projektą Nacionalinis kibernetinio saugumo centras atliks nacionalinės reagavimo į kompiuterinius saugumo incidentus tarnybos funkcijas, todėl jis turi atitikti Direktyvos (ES) 2016/1148 1 priedo reikalavimus. Be to, šie reikalavimai, mūsų nuomone, turėtų būti nustatyti įstatymu.	kibernetinio saugumo centro kompetenciją) yra pakankamai bendro pobūdžio, neapibrėžti, todėl, laikantis nacionalinių teisėkūros taisyklių, atskirai teisės aktuose nėra nustatomi. Be to, Direktyvos (ES) 2016/1148 1 priede nustatoma, kad šie reikalavimai yra grindžiami nacionaline politika ir (arba) taisyklėmis, todėl keičiantis nacionalinei politikai Direktyvos (ES) 2016/1148 1 priede nustatytų reikalavimų reikšmė taip pat gali kisti. Manome, kad šie reikalavimai turėtų būti užtikrinami individualaus pobūdžio teisės aktais, todėl tokios nuostatos į norminio pobūdžio nacionalinės teisės aktus neturėtų būti perkeliamos. Atsižvelgiant į tai, teisės aktuose siūlytina neįvesti deklaratyvių, pridėtinės vertės nekuriančių formuluočių.
Asociacijos „Infobalt“ 2018-02-27 raštas Nr. 20180227/02	**Kibernetinio saugumo įstatymo 2 straipsnio 12 punktas:** Kibernetinio saugumo subjektai – subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai, elektroninės informacijos prieglobos paslaugų teikėjai ir skaitmeninių paslaugų teikėjai. **Siūlymas:** Siūlome praplėsti taikymo sritį ir įvardinti, kad įstatymas galioja ir savivaldybėms, savivaldybių įmonėms ir t.t. nes traktuojama, kad VIIVĮ savivaldybėms netaikomas, nes VII kurti ne iš valstybės biudžeto lėšų, o savivaldybės. Kas pagal Biudžeto sandaros įstatymą yra du skirtingi objektai. Savivaldybių įmonėse biudžetai dar labiau ne	Atkreiptinas dėmesys, kad Valstybės informacinių išteklių įstatymas taikomas toms valstybės ir savivaldybių įmonėms, savivaldybių įstaigoms ir viešosioms įstaigoms ir tais atvejais, jeigu apdorojant informaciją informacinių technologijų priemonėmis per valstybės informacinių sistemų ar registrų sąveiką reikia gauti duomenis iš valstybės informacinių sistemų ir (arba) registrų (1 straipsnio 3 dalis), todėl sieti valstybės informacinius išteklius vien per tai, ar jie parengti iš valstybės biudžeto, ar ne, būtų netikslu. Suprantama, kad ne visos savivaldybės, savivaldybių įmonės valdo valstybės informacinius išteklius, kas lemia, kad ne visos savivaldybės, savivaldybių įmonės yra laikomos kibernetinio saugumo subjektais. Tačiau visų jų priskirti kibernetinio saugumo subjektams nėra poreikio, todėl pasirenkami kriterijai, kuriuos atitinkantys bet kokie subjektai būtų laikomi kibernetinio saugumo subjektais, t. y. valstybės informacinių išteklių valdymas ir (arba) tvarkymas ir priskyrimas ypatingos svarbos informacinės infrastruktūros valdytojams.

	valstybiniai, o teikiamos paslaugos gal ir ne YSII, bet kai kurios turi strateginę reikšmę nacionaliniam saugumui (vandentiekis, šildymas).	
	Kibernetinio saugumo įstatymo 11 straipsnio 3 punktas: turi teisę, kai paslaugų gavėjas galimai dalyvauja ar jo naudojama ryšių ir informacinių technologijų įranga galimai yra naudojama nusikalstamoje veikoje, 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, 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. Tokiais atvejais apylinkės teismo pirmininkui ar jo įgaliotam teisėjui pateikiamas teikimas dėl veiksmų teisėtumo ar pagrįstumo patvirtinimo motyvuota nutartimi. Jeigu terminas baigiasi poilsio ar švenčių dieną, teikimas pateikiamas ne vėliau kaip kitą darbo dieną po poilsio ar švenčių dienos. Jeigu teisėjas nepatvirtina nurodytų veiksmų teisėtumo ar pagrįstumo motyvuota nutartimi, nurodymas nedelsiant stabdomas; **Siūlymas:** Nėra aišku kaip elgtis vykdytojams jei terminas baigiasi poilsio ar švenčių dienomis.	**Neatsižvelgta.** Nurodymas be teismo sprendimo apriboti paslaugų teikimą gali būti nustatomas ne ilgiau kaip 48 valandų terminui. Ši teisė neturi išimčių, nepriklausomai nuo to, kada baigiasi terminas. Kitaip tariant, jeigu 48 valandų terminas baigiasi poilsio ar švenčių dienomis, o teismų sprendimo vis dar nėra, kibernetinio saugumo subjektui nelieka pareigos apriboti paslaugų teikimą.

	Punkte reikia išaiškinti kaip elgtis vykdytojams. Jei palikti tai iki kada.	
	Kibernetinio saugumo įstatymo 11 straipsnio 4 punktas: turi teisę duoti nurodymą viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų teikėjui ir skaitmeninių paslaugų teikėjui išsaugoti informaciją, susijusią su jų teikiamomis paslaugomis, 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 ir, kai yra motyvuota teismo nutartis, gauti paslaugų gavėjo srauto duomenis ir kontroliuoti perduodamos informacijos turinį. **Siūlymas:** Labai viskas neapibrėžta. Turėtų būti paruošta tvarka, kurioje būtų aprašyta pvz. už kokį laikotarpį gali prašyti išsaugoti duomenis ir pan. Tada šiame punkte rašyti, kad duodami nurodymai pagal tam tikrą tvarką. Arba duoti nuorodą į jau egzistuojančias tvarkas.	Nurodymas išsaugoti informaciją yra neatsiejamas nuo teisės ją gauti ir, esant motyvuotai teismo nutarčiai, paslaugų gavėjo srauto duomenų gavimo ir perduodamos informacijos kontrolės. Ne visa informacija, esanti ryšių aparatūros įrengimo vietoje, yra automatiškai išsaugoma. Siekdama ją gauti, policija turi turėti teisę duoti nurodymą pradėti išsaugoti nurodytą informaciją ir tik ją surinkus būtų galima reikalauti ją perduoti. Kitas svarbus aspektas yra tai, kad aplinkybės, kurios yra pagrindas reikalauti informacijos, atsiranda anksčiau, nei išduodama teismo nutartis. Atsižvelgiant į tai ir siekiant neprarasti informacijos per tą laiką, kol gaunama teismo nutartis, policijai ir suteikiama teisė duoti nurodymą išsaugoti nurodytą informaciją.
	12 straipsnio 1 dalies 5 punktas: policijos generalinio komisaro nustatyta tvarka teikia policijai informaciją, reikalingą teisės pažeidimams, turintiems nusikalstamos veikos	**Neatsižvelgta.** Šia norma teikiamas prioritetas visuomenės saugumui. Galimos situacijos, kai, siekiant išvengti nepageidaujamų pasekmių, reikėtų reaguoti išties greitai, todėl policija turi turėti galimybę reaguoti kaip įmanoma greičiau, nepriklausomai nuo to, ar

	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; **Siūlymas:** Šio punkto įgyvendinimas užkrauna finansinę ir administracinę naštą, nes jo įgyvendinimui subjektai privalės užtikrinti personalo darbą 24x7 režimu. Siūlome tikslinti punktą ir rašyti „privaloma įvykdyti ne vėliau kaip per 8 darbo valandas“	incidentas įvyko darbo, ar nedarbo valandų metu (ypač poilsio ar šventinėmis dienomis).

Užsienio reikalų ministras
Linas Linkevičius

Krašto apsaugos viceministras
Vytautas Umbrasas

LIETUVOS RESPUBLIKOS VYRIAUSYBĖS KANCELIARIJA
TEISĖS GRUPĖ

IŠVADA

DĖL LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMO NR. XII-1428 PAKEITIMO ĮSTATYMO PROJEKTO (toliau- Projektas Nr.1) IR LIETUVOS RESPUBLIKOS ADMINISTRACINIŲ NUSIŽENGIMŲ KODEKSO 479, 480, 589 STRAIPSNIŲ IR PRIEDO PAKEITIMO ĮSTATYMO PROJEKTO (toliau – Projektas Nr.2, toliau kartu – Projektai)) (TAP-18-356–18-358) (TAIS NR.18-2648)

2018-03-21 Nr.NV-748

Vilnius

Įvertinę Projektų atitiktį įstatymams bei teisės technikos reikalavimams teikiame šias pastabas ir pasiūlymus:

1. Siūlome tikslinti Projektu Nr.1 nauja redakcija dėstomo Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymo (toliau – Kibernetinio saugumo įstatymas) 1 straipsnio 1 dalyje nustatomą įstatymo reguliavimo sritį, kuri šiuo atveju apibrėžiama netiksliai, nes įstatymo turinys neatitinka 1 dalyje nurodytos įstatymo reguliavimo srities, pavyzdžiui, vartojama „kibernetinio saugumo sistemos“ sąvoka, kuri šiame įstatyme nėra apibrėžta ir jos turinys nėra atskleidžiamas; kibernetinio saugumo politiką formuojančių ar įgyvendinančių institucijų funkcijos turėtų būti institucijų veiklos nuostatų reguliavimo dalykas; šio įstatymo III skyriuje reguliuojamos kibernetinio saugumo subjektų pareigos, bet ne teisės; siūlomas atsakomybės reguliavimas yra fragmentiškas ir perteklinis Lietuvos Respublikos administracinių nusižengimų kodekso atžvilgiu ir pan.

2. Pastebėtina, kad Kibernetinio saugumo įstatymo nuostatų formuluotėse skirtingų sąvokų „kibernetinio saugumo užtikrinimo priemonės“ (pavyzdžiui, 1 straipsnio 1 dalis) ir „kibernetinio saugumo priemonės“ (pavyzdžiui, 3 straipsnio 1 dalies 2 punktas) vartojimas sukelia neaiškumą dėl jų turinio bei taikymo aplinkybių, todėl turi būti sistemiškai peržiūrėtas ir tikslinamas.

3. Pastebėtina, kad Kibernetinio saugumo įstatymo 1 straipsnio 2 dalyje turėtų būti nurodomas ir Europos Sąjungos teisės akto pavadinimas, kadangi šis teisės aktas nenurodomas įstatymo priede, bei pateikiama nuoroda į paskelbimo šaltinį. Šiuo aspektu tikslintina ir Kibernetinio saugumo įstatymo 2 straipsnio 17 dalis. Be to, tikslinga tikslinti ir 1 straipsnio 3 dalies formuluotę dėl asmens duomenų tvarkymo pagrindo, nes pastebėtina, kad asmens duomenų tvarkymo pagrindimas įstatymo tikslais, kurie nėra konkrečiai apibrėžti, nelaikytinas tinkamai reglamentuojančiu duomenų tvarkymo teisėtumą.

4. Siekiant aiškumo ir dėstymo nuoseklumo, Kibernetinio saugumo įstatymo 1 straipsnyje siūlome suderinti nuostatų „šis įstatymas“ ir „įstatymas“ vartojimą.

5. Kibernetinio saugumo įstatymo 2 straipsnyje teikiamų visų naujų sąvokų apibrėžtys turi būti suderintos (aprobuotos) Terminų banko įstatymo ir jo įgyvendinamųjų teisės aktų nustatyta tvarka (Teisės aktų projektų rengimo rekomendacijų, patvirtintų teisingumo ministro 2013 m. gruodžio 23

d. įsakymu Nr.1R-298 (toliau – Rekomendacijos), 6.5 papunktis) iki Projekto Nr.1 pateikimo Lietuvos Respublikos Seimui. Įvertinus šio įstatymo 2 straipsnio 3 ir 4 dalyse teikiamų sąvokų apibrėžtis, pastebėtina, kad skirtingų sąvokų „vartotojai“ ir „naudotojai“ vartojimas, arba šio straipsnio 5 ir 11 dalyse nustatomų sąvokų apibrėžtyse vertinamojo pobūdžio nuostatų „neigiamas poveikis“ ir „didelis neigiamas poveikis“ vartojimas, kai jų turinys nėra atskleistas ir nenurodoma, kokiuose teisės aktuose tai būtų reglamentuojama, sudaro neaiškumą bei galimybę interpretuoti teikiamas sąvokas. Taipogi, siūlytina įvertinti, ar 2 straipsnio 3 ir 4 dalyse neturėtų būti vartojamas terminas „interneto svetainė“ (vietoj žodžio „svetainė“).

6. Siūlytina peržiūrėti Kibernetinio saugumo įstatymo 2 straipsnio 11 dalies apibrėžtį, ypač neapibrėžtas nuostatas „tokio masto“, „politinės reikšmės“ „iškyla poreikis *koordinuoti politiką* (kokią?) ir *reaguoti tų tarptautinių organizacijų politiniu lygmeniu*“, suteikiant norminį pobūdį, nes priešingu atveju siūloma apibrėžtis neatitinka aiškumo ir tikslumo reikalavimo.

7. Atsižvelgiant į 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyvos (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (toliau – Direktyva (ES) 2016/1148) 4 straipsnio 4 punkto bei 5 straipsnio 2 dalies a papunktį, manytina, kad siekiant išvengti netikslumų, Kibernetinio saugumo įstatymo 2 straipsnio 6 dalyje, apibrėžiant ypatingos svarbos informacinės infrastruktūros valdytoją, turėtų būti detaliau apibrėžiama, koks asmuo turimas mintyje šiuo atveju, pavyzdžiui, kad tai fizinis ar juridinis asmuo, veikiantis viešajame ar privačiame sektoriuje, o taip pat nurodoma ir nuostatos „valdantis“ apimtis.

8. Siūlome įvertinti, ar Kibernetinio saugumo įstatymo 2 straipsnio 9 dalyje, apibrėžiant kibernetinių incidentų valdymo sąvoką, neturėtų būti nurodytos procedūros, apimančios ir incidentų prevenciją, kaip viena iš rizikos valdymo priemonių, nurodytų Direktyvos (ES) 2016/1148 preambulės 46 punkte. Be to, manome, kad siekiant reguliavimo aiškumo, Kibernetinio saugumo įstatymo 2 straipsnis pildytinas „rizikos“ sąvoka, priešingu atveju, Kibernetinio saugumo įstatymo nuostatos, kuriose minima rizika bei jos valdymas, pavyzdžiui, 3 straipsnio 1 dalies 2 punkto, 9 straipsnio 2 dalies 7 punkto, 12 straipsnio 1 dalies 2 punkto ir kt., lieka neaiškios, nors būtent įstatymuose, o ne jų įgyvendinamuosiuose teisės aktuose, ir turi būti apibrėžiamos įstatymuose vartojamos sąvokos (Rekomendacijų 6.5 papunktis.). Kartu pastebėtina, kad šio straipsnio 9 ir 10 dalyse procedūroms bei priemonėms apibūdinti vartojama tapati nuostata „įprastinei ryšių informacinių sistemų veiklai atkurti“ sudaro neaiškumą dėl skirtingų sąvokų dubliavimosi.

9. Kibernetinio saugumo įstatymo 2 straipsnio 16 dalyje turėtų būti nurodyta „Lietuvos Respublikoje“.

10. Atsižvelgiant į Kibernetinio saugumo įstatymo 3 straipsnio pavadinimą bei reguliavimo turinį, siūlytina 1 dalyje atsisakyti nuorodos į bendruosius teisės principus bei elektroninių ryšių veiklos principus kaip perteklinio reguliavimo. Be to, Kibernetinio saugumo įstatymo 3 straipsnio 1 dalies 3 punkte siūlome vietoj nuostatos „kibernetinio saugumo reikalavimai“ vartoti nuostatą „kibernetinio saugumo priemonės“, kaip tai yra nustatyta „kibernetinio saugumo“ sąvokoje.

11. Kibernetinio saugumo įstatymo 4 straipsnis ir jame nustatytas reguliavimas vertintinas kaip ne šio skyriaus reguliavimo dalykas, nes reguliuoja ir Nacionalinio kibernetinio saugumo centro veiksmus. Siūlytina įvertinti galimybę šiomis nuostatomis pildyti Kibernetinio saugumo įstatymo III skyrių, atitinkamai papildant ir šio skyriaus pavadinimą.

12. Siūlytina tikslinti Kibernetinio saugumo įstatymo 4 straipsnio 2 dalyje siūlomą reguliavimą, tiksliai apibrėžiant subjektų, kuriems taikytina ši nuostata, ratą, t.y., suvienodinant subjektų sąvoką, jeigu tai yra subjektai, nurodyti šio straipsnio 1 dalyje, arba atskleidžiant subjekto, savanoriškai pranešusio apie kibernetinį incidentą, taikymo apimtį: ar taikytina kibernetinio saugumo subjektams, nurodytiems 12 straipsnio 2 dalyje, kuriems netaikomos 12 straipsnyje nustatytos kibernetinio saugumo subjektų pareigos. Taipogi, siūlome tikslinti vertinamo straipsnio 1 dalies nuostatą „gali savanoriškai informuoti“, suteikiant asmeniui *teisę savanoriškai pranešti* apie kibernetinį incidentą. Pastebėtina ir tai, kad vertinama 4 straipsnio 2 dalies nuostata tikslintina kaip stokojanti loginio ryšio, nes nenustatant „jokių“ pareigų, nurodytos sąlygos negalėtų būti tenkinamos.

13. Siūlytina apibrėžtumo stokojančią Kibernetinio saugumo įstatymo 5 straipsnio 3 dalies nuostatą „ir kitos institucijos pagal savo kompetenciją“ keisti nuostata „ir kitos institucijos, kurių vykdomos funkcijos, susijusios su kibernetiniu saugumu“ ar pan.

14. Kibernetinio saugumo įstatymo II skyriuje „Kibernetinio saugumo politikos formavimas ir įgyvendinimas“ nustatomi įgaliojimai institucijoms parengti konkrečius teisės aktus ar juos priimti. Mūsų nuomone, Kibernetinio saugumo įstatyme minimi konkretūs planavimo dokumentų pavadinimai ir konkretūs poįstatyminio teisės akto pavadinimai riboja Vyriausybės ar jos įgaliotos institucijos diskreciją spręsti, kokius konkrečius teisės aktus (ir kokios formos) būtina priimti. Be to, aukštesnės galios teisės akte turėtų būti vengiama nuorodų į konkrečius žemesnės galios teisės aktus (Rekomendacijų 13 punktas). Taip pat, atkreipiame dėmesį, kad įgaliojimas Vyriausybei tvirtinti Nacionalinę kibernetinio saugumo strategiją, neatitinka Lietuvos Respublikos Vyriausybės 2002 m. birželio 6 d. nutarimu Nr.827 patvirtintos Strateginio planavimo metodikos ir joje nustatytos strateginio planavimo sistemos, nes ilgos trukmės planavimo dokumentus – strategijas tvirtina Lietuvos Respublikos Seimas.

15. Siūlytina atsisakyti Kibernetinio saugumo įstatymo 7 straipsnio pirmosios pastraipos nuostatos kaip atkartojančios 5 straipsnio 2 dalies pirmojo sakinio nuostatą.

16. Siūlytina pildyti Kibernetinio saugumo įstatymo 8 straipsnį, aiškiai apibrėžiant Kibernetinio saugumo tarybos teisinį statusą ir atskleidžiant nuostatos „nuolatinė“ turinį, pavyzdžiui, ar tai nepriklausoma institucija, vykdanti stebėsenos ar patariamosios institucijos funkciją, ar tai institucija, veikianti prie Krašto apsaugos ministerijos, ar pan. Be to, siekiant aiškesnio šios tarybos sudarymo ir veiklos reguliavimo, tikslinga tikslinti Kibernetinio saugumo įstatymo 6 straipsnio 2 punktą, o taip pat ir 8 straipsnio 1 dalį, vienam subjektui – krašto apsaugos ministrui, pavesti nustatyti Kibernetinio saugumo tarybos sudarymo tvarką, patvirtinti jos veiklos nuostatus bei personalinę sudėtį. Taipogi, siūlytume 8 straipsnio 1 dalyje atsisakyti neapibrėžtumą

sąlygojančios nuostatos „kitų asmenų“ (neaišku, kokie kiti asmenys galėtų būti šios tarybos sudėtyje) ir 4 dalies 2 punkte – vertinamojo pobūdžio nuostatos „platesnio“.

17. Atsižvelgiant į Kibernetinio saugumo įstatymo 9 straipsnyje siūlomą reguliavimą, pažymėtina, kad Lietuvos Respublikos Vyriausybės įstatymo 22 straipsnio 9 punkte Vyriausybei pavesta tvirtinti ministerijų, Vyriausybės įstaigų ir įstaigų prie ministerijų nuostatus. Vyriausybė, įgyvendindama šiuos įgaliojimus, yra kompetentinga nustatyti ministerijų, įstaigų prie ministerijų veiklos sritis ir funkcijas, spręsti su Vyriausybės ir jai atskaitingų įstaigų veiklos organizavimu susijusius klausimus. Todėl manome, kad įstaigų prie ministerijų veiklos funkcijos (išskyrus tas, kurioms reikalingas įstatyminis pagrindas) apskritai neturėtų būti įtvirtintos įstatymuose, tokiu būdu sukuriant situaciją, kai tam tikros funkcijos turinys gali būti keičiamas ar funkcija gali būti perduodama kitai įstaigai, tik atitinkamai koreguojant įstatymus. Civilinio kodekso 2.46 straipsnyje, Biudžetinių įstaigų įstatymo 6 straipsnyje numatyta, jog juridiniai asmenys savo veikloje vadovaujasi įstatais (nuostatais), Civilinio kodekso 2.47 straipsnyje, Biudžetinių įstaigų įstatymo 6 straipsnyje įtvirtinta, kad būtent įstatuose (nuostatuose) turėtų būti nurodomi juridinio asmens veiklos tikslai, biudžetinės įstaigos veiklos tikslai ir funkcijos. Atsižvelgiant į tai, manytume, kad, būtų tikslinga įvertinti ir Kibernetinio saugumo įstatymo 9 straipsnyje numatytų detalių Nacionalinio kibernetinio saugumo centro funkcijų nustatymo įstatyme poreikį bei jų atsisakymo galimybę, nes nurodytos funkcijos gali būti numatytos įgyvendinamuosiuose teisės aktuose. Be to, tokiu būdu būtų užtikrinta ir teisės aktų hierarchija ir ekonomiškumo principą atitinkanti teisėkūra. Taipogi, šiuo atveju būtų tikslinga pakartotinai įvertinti Europos teisės departamento prie Teisingumo ministerijos išvadoje dėl Projektų pateiktą 8 pastabą dėl reikalavimų, kurie taikytini Nacionalinio kibernetinio saugumo centrui pagal Direktyvą (ES) 2016/1148, nustatymo įstatyme tikslingumą.

18. Pastebime, kad Kibernetinio saugumo įstatymo 9 straipsnyje 2 dalies 1 punkte, 8 punkte vartojamos įstatyme neapibrėžtos nuostatos „kibernetinio saugumo būsena“ bei „diegimo planas“, todėl siūlome atskleisti jų turinį, nurodyti subjektą, kuris tvirtintų planą, arba, siekiant aiškumo, siūlomą reguliavimą susieti su šio įstatymo 7 straipsnio 9 punkto nuostata. Kartu tikslintina ir 9 straipsnio 2 dalies 6 punkto nuostata „valstybės narės“ (turėtų būti „Europos Sąjungos valstybės narės“, įrašant atitinkamai ir kituose šio įstatymo straipsniuose, pavyzdžiui, 13 straipsnio 5 dalies 2 punkte) bei 2 dalies 11 punkte – nurodytinas nustatyto termino pradžios momentas, o 17 punkte - vietoj nurodytų subjektų įrašytinas 8 straipsnio 1 dalyje įvestas trumpinys „kibernetinio saugumo dalyviai“.

19. Kibernetinio saugumo įstatymo 12 straipsnio 1 dalies 7 punkto formuluotė tikslintina, nes nėra aiškiai nustatyta, kokie pagrindai (kuriame straipsnyje nustatyti) šiuo atveju turi būti taikomi.

20. Kibernetinio saugumo įstatymo 13 straipsnio 1 dalies 1 punkte siūlome atsisakyti nuostatos „parengia“, o 3 punkte nurodytą terminą skaičiuoti kalendoriniais metais.

21. Tikslinga įvertinti Kibernetinio saugumo įstatymo 13 straipsnio 5 dalies 2 punkte siūlomo reguliavimo pakankamumą bei nuostatos „veikti“ aiškumą.

22. Manome, kad tikslinga keisti Kibernetinio saugumo įstatymo IV skyriaus pavadinimą, pavyzdžiui, „Tarpinstitucinis bendradarbiavimas“, nes vertiname skyriuje nėra nustatoma keitimosi informacija tvarka, o siūlomas atsakomybės reguliavimas šiuo atveju laikytinas pertekliniu.

Taipogi, pažymime, kad Teisės grupės 2018-02-19 išvadoje Nr. NV-435 dėl Lietuvos Respublikos Vyriausybės nutarimo „Dėl Lietuvos Respublikos Vyriausybės 2016 m. sausio 25 d. nutarimo Nr. 87 „Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“ pakeitimo“ projekto buvo pateikta 1 pastaba, kuria siūloma į Kibernetinio saugumo įstatymą įtraukti nuostatos, aiškiai apibrėžiančios Nacionalinio kibernetinių incidentų valdymo plano (toliau – Planas) turinį (reguliuojamų santykių apimtį), kadangi pagal šiuo metu galiojančio Kibernetinio saugumo įstatymo 18 straipsnio 3 dalį Nacionaliniame kibernetinių incidentų valdymo plane nustatoma tarpinstitucinio bendradarbiavimo tiriant kibernetinius incidentus tvarka ir kibernetinių incidentų klasifikavimo tvarka, tuo tarpu Plano turinys apima ne tik tuos aspektus, bet ir institucijų veiksmus, atliekamus siekiant suvaldyti kibernetinius incidentus, galinčius sutrikdyti ar sutrikdančius valstybės informacinių išteklių, ypatingos svarbos informacinės infrastruktūros ir (ar) kitų elektroninių ryšių tinklų ir paslaugų ir (ar) informacinių sistemų darbą, taip pat tarpinstitucinę kibernetinių incidentų valdymo sąveiką. Taigi, siekiant išvengti įgyvendinamųjų teisės aktų įstatyminio pagrindo problemų, siūlytume įvertinti šią pastabą ir tikslinti Kibernetinio saugumo įstatymo IV skyriuje siūlomą teisinį reguliavimą. Pavyzdžiui, ar nebūtų tikslinga tikslinti Kibernetinio saugumo įstatymo 15 straipsnio pavadinimą bei straipsnio nuostatas, kuriuose nustatomas bendradarbiavimas ne tik tiriant, bet ir valdant kibernetinius incidentus, ir, atsižvelgiant į kibernetinių incidentų valdymo sąvoką, nustatant tarpinstitucinio bendradarbiavimo valdant kibernetinius incidentus reguliavimą.

23. Siūlome tikslinti Kibernetinio saugumo įstatymo 16 straipsnio nuostatą, nes formuluotėje nėra tiksliai apibrėžta, kokiems subjektams ši nuostata taikytina, kokias pareigas subjektams siūloma nustatyti.

24. Siūlome Projekto Nr.1 2 straipsnio 1 dalyje nurodytą įsigaliojimo terminą tikslinti, nustatant realų įsigaliojimo terminą, įvertinant teisės aktų projektų svarstymo ir priėmimo Lietuvos Respublikos Seime procedūras bei terminus, bei tai, jog pakeitimams įgyvendinti turi būti priimami ir įgyvendinamieji teisės aktai. Atitinkama pastaba taikytina ir Projektui Nr.2.

25. Siūlome Projekto Nr.1 2 straipsnio nuostatas tikslinti teisės technikos aspektu: 1 dalies išimtyje nurodyti ne tik 2, bet ir 3 ir 4 dalis; 2 dalyje nurodyti pilnus oficialius institucijų ir pareigų pavadinimus „Lietuvos Respublikos Vyriausybė ir Lietuvos Respublikos krašto apsaugos ministras“; 3 dalyje tikslinti įsigaliojimo datą, be to, vietoj nuostatos „šiuo įstatymo patvirtinto Kibernetinio saugumo įstatymo 9 straipsnio“ siūlytina įrašyti nuostatą „šio įstatymo 1 straipsnyje išdėstyto Lietuvos Respublikos kibernetinio saugumo įstatymo 10 straipsnio“; analogiškai siūlytina formuluoti ir 4 dalies pakeitimo esmę.

26. Atsižvelgiant į tai, kad Kibernetinio saugumo įstatymo priedas dėl įgyvendinamų Europos Sąjungos teisės aktų yra nauja redakcija dėstomo įstatymo, o ne Įstatymo projekto Nr.1 dalis, šis priedas turi būti dėstomas prieš Įstatymo projekto Nr. 2 straipsnį. Be to, pagal Europos Sąjungos teisės aktų nuorodų pateikimo įstatymuose ir kituose teisės aktuose rekomendacijų, patvirtintų Europos teisės departamento prie Lietuvos Respublikos teisingumo ministerijos generalinio direktoriaus 2006 m. rugsėjo 25 d. įsakymo Nr.129kkk, 17 punktą, Kibernetinio saugumo įstatymo priede įgyvendinami Europos Sąjungos teisės aktai turi būti nurodomi chronologine tvarka, pradedant nuo anksčiausiai priimto teisės akto, todėl siūlytina priedą tikslinti. Taipogi, vadovaujantis šių rekomendacijų 12.2 papunkčiu, nuorodoje į Direktyvos (ES) 2016/1148 oficialų paskelbimo šaltinį vietoj nuorodos į puslapį „p.1-30“ turi būti nustatyta nuoroda į puslapį, kuriame prasideda teisės aktas, t. y., „p.1“ (atitinkamai ši pastaba taikytina ir Projekto Nr.2 4 straipsniui).

27. Atkreipiame dėmesį, kad Teisingumo ministerija yra parengusi Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 4, 11, 13, 14, 15 ir 18 straipsnių pakeitimo įstatymo projektą ir Lietuvos Respublikos administracinių nusižengimų kodekso 79, 479 ir 589 straipsnių pakeitimo ir 82 straipsnio pripažinimo netekusiu galios įstatymo projektą, kurie jau buvo teikti svarstyti Vyriausybei (TAIS Nr. 17-7650(2) ir yra grąžinti rengėjams tobulinti. Atsižvelgiant į tai, kad nurodytais projektais yra keičiami tie patiės Kibernetinio saugumo įstatymo bei Lietuvos Respublikos administracinių nusižengimų kodekso (toliau – ANK) straipsniai bei numatoma ta pati jų įsigaliojimo data, keičiamos nuostatos turi būti suderintos tarpusavyje, nesudarant situacijos, kai siekiant pasirengti tiesiogiai taikyti Bendrąjį duomenų apsaugos reglamentą, siūlomos skirtingos tą pačią dieną įsigaliojančių įstatymų pakeitimų nuostatos.

28. Dėl Projekto Nr.2 pastebėtina, kad 1 straipsnyje teikiamo ANK 479 straipsnio pakeitimų, galiosiančių tik iki 2018 m. gegužės 25 d., tikslingumas kelia pagrįstų abejonių, nes galiojantis ANK 479 straipsnis nustato atsakomybę dėl Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytos informacijos teikimo pareigos atlikimo pažeidimų, be to, galiojanti šio straipsnio 3 dalies nuostata yra taikytina subjektų, kurie laikytini kibernetinio saugumo subjektais, atžvilgiu. Analogiškai vertintinas ir Projekto Nr.2 2 straipsnyje teikiamas ANK 480 straipsnio pakeitimas. Kartu pastebėtina, kad aukštesnės galios teisės aktuose nuorodų į žemesnės galios konkrečius teisės aktus pateikimas neatitinka teisės aktų rengimo rekomendacijų, todėl ANK 479 straipsnio 3 dalies pakeitimas, o taip pat ir teikiamas ANK 480 straipsnio 4 dalies pakeitimas, tikslintini ir šiuo aspektu. Taipogi, siūlytina tikslinti ir Projekto Nr.2 lyginamąjį variantą, kuriame netiksliai pateikiamas siūlomas ANK 479 straipsnio 3 dalies pakeitimas.

29. Projekto Nr.2 1 straipsnyje teikiamo ANK 479 straipsnio3 dalies pakeitime vartojama „kibernetinio saugumo būsenos“ sąvoka, kuri Kibernetinio saugumo įstatyme nėra apibrėžta, todėl normos dispozicija tampa neaiški.

30. Projekto Nr.2 5 straipsnyje siūlytina braukti 2 dalies nuostatą kaip perteklinę.

31. Siūlome tikslinti nutarime, kuriuo Projektai teikiami Seimui, nurodytą skubos motyvą. Manome, kad šiuo atveju prašymą svartyti Projektus skubos tvarka būtų tikslingiau pagrįsti nurodant ne Direktyvos (ES) 2016/1148 įsigaliojimo datą, o siekį laiku į nacionalinę teisę perkelti minėtos direktyvos nuostatas.

32. Siūlytina tikslinti Projektų aiškinamojo rašto 3 dalies 2 ir 3 punkte teikiamas netikslias nuorodas į Kibernetinio saugumo įstatymo 2 straipsnyje dėstomas sąvokas, o 9 punkte atsisakyti netikslios ir klaidinančios nuostatos „nustatyti atsakomybę Vyriausybei vadovauti“ ir formuluoti kitaip, pavyzdžiui, suteikti įgaliojimus, pavesti ar pan.

Teisės grupės patarėja Tatjana Knyzienė

Teisės grupės vyresnioji patarėja Eglė Gasiūnaitė

Tatjana Knyzienė, tel. 870663862, el. p. tatjana.knyziene@lrv.lt