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 kibernetinio saugumo įstatymas Nr. XII-1428 (toliau – Kibernetinio saugumo įstatymas)** **2. Lietuvos Respublikos Vyriausybės nutarimo „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ projektas, kuriuo tvirtinami:** **2.1. Ypatingos svarbos informacinės infrastruktūros nustatymo metodika (toliau – YSII nustatymo metodikos projektas);** **2.2. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo projektas);** **2.3. Nacionalinis kibernetinių incidentų valdymo planas (toliau – Kibernetinių incidentų valdymo plano projektas)**	
4 straipsnis. Terminų apibrėžtys Šioje direktyvoje vartojamų terminų apibrėžtys: 9) **rizika** – pagrįstai nustatoma aplinkybė ar įvykis, galintis turėti neigiamą poveikį tinklų ir informacinių sistemų saugumui;	**Kibernetinio saugumo įstatymas** <...> **2 straipsnis. Pagrindinės šio įstatymo sąvokos** <...> 15. **Rizika** – pagrįstai nustatoma aplinkybė ar įvykis, galintis turėti neigiamą poveikį ryšių ir informacinių sistemų saugumui	Visiškas
13) **interneto duomenų srautų mainų taškas (IXP)** – tinklo	**YSII nustatymo metodikos projektas**	Visiškas

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;	**I skyrius. Bendrosios nuostatos** <...> 2. Metodikoje vartojamos sąvokos: 2.6. **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.	
14) **domenų vardų sistema (DNS)** – pagal hierarchiją suskirstyta vardų suteikimo sistema tinkle, kuris persiunčia domenų vardų užklausas;	**YSII nustatymo metodikos projektas** **I skyrius. Bendrosios nuostatos** <...> 2. Metodikoje vartojamos sąvokos: 2.2. **Domenų vardų sistema (DNS)** – pagal hierarchiją suskirstyta vardų suteikimo sistema tinkle, kuris persiunčia domenų vardų užklausas.	Visiškas
15) **DNS paslaugų teikėjas** – subjektas, kuris teikia DNS paslaugas internetu;	**YSII nustatymo metodikos projektas** **I skyrius. Bendrosios nuostatos** <...> 2. Metodikoje vartojamos sąvokos: 2.3. **DNS paslaugų teikėjas** – subjektas, kuris teikia DNS paslaugas internetu.	Visiškas
16) **aukščiausio lygio domenų vardų registras** – subjektas, kuris administruoja ir vykdo interneto domenų vardų registravimą pagal konkretų aukščiausio lygio domeną (ALD);	**YSII nustatymo metodikos projektas** **I skyrius. Bendrosios nuostatos** <...> 2. Metodikoje vartojamos sąvokos: 2.1. **Aukščiausio lygio domenų vardų registras (ALD)** – subjektas, kuris administruoja ir vykdo interneto domenų vardų registravimą pagal konkretų aukščiausio lygio domeną.	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.	**1. Lietuvos Respublikos Vyriausybės nutarimo „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ projektas** <...> 2. Pavesti: 2.1. institucijoms, nurodytoms Metodikos 1 priede, Metodikos nustatyta tvarka peržiūrėti Metodikos 1 priede nustatytus ypatingos svarbos infrastruktūros objektus, nustatytą ypatingos svarbos informacinę infrastruktūrą ir pateikti atnaujintus ypatingos svarbos informacinės infrastruktūros, išdėstytos prioriteto pagal svarbą tvarka, sąrašus Lietuvos Respublikos krašto apsaugos ministerijai; **2. YSII nustatymo metodikos projektas** Ypatingos svarbos informacinės infrastruktūros nustatymo metodikos projekto 1 priedas **YPATINGOS SVARBOS SEKTORIAI, SUBSEKTORIAI, PASLAUGOS IR ATSAKINGOS INSTITUCIJOS** 1. Energetikos sektorius 1.1. Elektros energijos subsektorius 1.2. Naftos ir naftos produktų subsektorius 1.3. Gamtinių dujų subsektorius 1.4. Centralizuoto šildymo subsektorius 2. Transporto ir pašto sektorius 2.1. Oro transporto subsektorius 2.2. Geležinkelių transporto subsektorius 2.3. Vandens transporto subsektorius 2.4. Kelių transporto subsektorius 2.5. Pašto subsektorius 3. Bankininkystės ir finansų sektorius 3.1. Kredito įstaigų subsektorius 3.2. Finansinių rinkų infrastruktūros subsektorius	Visiškas

	4. Sveikatos priežiūros sektorius 4.1. Sveikatos priežiūros infrastruktūros subsektorius 5. Geriamo vandens tiekimo, paskirstymo ir tvarkymo sektorius 5.1. Geriamojo vandens subsektorius 5.2. Nuotekų subsektorius 6. Informacinių technologijų ir elektroninių ryšių sektorius 6.1. Skaitmeninės infrastruktūros subsektorius 6.2. Elektroninių ryšių subsektorius 6.3. Informacinių technologijų subsektorius	
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 nustatymo metodikos projektas** **III skyrius. Ypatingos svarbos informacinės infrastruktūros nustatymas** <...> 6.2. Atsakinga institucija kreipiasi į instituciją, įstaigą, įmonę ar jos struktūrinį padalinį, kurie yra infrastruktūros objektai, ar į infrastruktūros objekto valdytoją, kai infrastruktūros objektas yra įrenginys ar įrenginio dalis (toliau – Atsakingas valdytojas), prašydama Atsakingo valdytojo atlikti visų jo valdomų 6.1 papunkčio nustatyta tvarka nustatytų infrastruktūros objektų svarbos vertinimą ir užpildyti Metodikos 2 priede pateiktą klausimyną (toliau – Klausimynas). Jeigu Atsakinga institucija ir Atsakingas valdytojas yra tas pats subjektas, Klausimyną pildo Atsakinga institucija. **YSII nustatymo metodikos projekto 2 ir 3 priedai.**	Visiškas
3. 1 dalies tikslais kiekviena valstybė narė sudaro 2 dalies a punkte nurodytų paslaugų sąrašą.	**YSII nustatymo metodikos projektas** **II skyrius. Ypatingos svarbos infrastruktūros objektų nustatymas** <...> 6. Ypatingos svarbos infrastruktūros objektai nustatomi šia tvarka: 6.1. Atsakinga institucija nustato visus jos veiklos srityje	Visiškas

	veikiančius infrastruktūros objektus, turinčius reikšmės teikiant ypatingos svarbos paslaugas. 6.2. Atsakinga institucija kreipiasi į instituciją, įstaigą, įmonę ar jos struktūrinį padalinį, kurie yra infrastruktūros objektai, ar į infrastruktūros objekto valdytoją, kai infrastruktūros objektas yra įrenginys ar įrenginio dalis (toliau – Atsakingas valdytojas), prašydama Atsakingo valdytojo atlikti visų jo valdomų 6.1 papunkčio nustatyta tvarka nustatytų infrastruktūros objektų svarbos vertinimą ir užpildyti Metodikos 2 priede pateiktą klausimyną (toliau – Klausimynas). Jeigu Atsakinga institucija ir Atsakingas valdytojas yra tas pats subjektas, Klausimyną pildo Atsakinga institucija. 6.3. Atsakingas valdytojas ne vėliau kaip per 20 darbo dienų nuo 6.2 papunktyje nurodyto prašymo gavimo užpildo Klausimyną ir teikia jį raštu Atsakingai institucijai. 6.4. Atsakinga institucija įvertina Atsakingo valdytojo pateiktą Klausimyną ir prireikus teikia Atsakingam valdytojui pastabas ir pasiūlymus, kartu nurodydama terminą, kurio reikia Klausimynui patikslinti. Atsakinga institucija turi teisę prašyti Atsakingo valdytojo papildomos informacijos, kuri reikalinga Klausimynui patikslinti, taip pat turi teisę Klausimyne papildomai nustatyti ir įvertinti jos veiklos srities sektoriaus specifinius kriterijus, galinčius turėti įtakos jos veiklos srityje veikiančių Atsakingų valdytojų veiklai. 6.5. Infrastruktūros objektų, kurie, atsižvelgiant į Atsakingos institucijos vertinimą ir Klausimyno kriterijus, įvertinami 16 ar daugiau balų, teikiamų paslaugų sutrikdymo neigiamas poveikis yra didelis, todėl šie infrastruktūros objektai nustatomi kaip ypatingos svarbos infrastruktūros objektai.	
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	**YSII nustatymo metodikos projektas** **III skyrius. Ypatingos svarbos informacinės infrastruktūros nustatymas**	Visiškas

vyksta prieš priimant sprendimą dėl identifikavimo.	<...> 8.5. Jeigu užpildytame Klausimyne, Lentelėje, Sąraše nurodyta, kad ypatingos svarbos paslauga teikiama dviejose ar daugiau Europos Sąjungos valstybėse narėse, Atsakinga institucija prieš priimdama sprendimą dėl ypatingos svarbos informacinės infrastruktūros nustatymo konsultuojasi su Europos Sąjungos valstybių narių institucijomis, kurių veiklos sritys apima užpildytame Klausimyne, Lentelėje, Sąraše nurodytus ypatingos svarbos sektorius, subsektorius ir juose teikiamas ypatingos svarbos paslaugas.	
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 nustatymo metodikos projektas** **V skyrius. Baigiamos nuostatos** <...> 12. Atsakingas valdytojas, atsiradus ypatingos svarbos infrastruktūros objekto, ypatingos svarbos informacinės infrastruktūros ir (arba) jos valdymo pokyčių arba kai steigiama nauja infrastruktūra, skirta ypatingos svarbos paslaugoms teikti, kurios funkcionavimas pagrįstas informacine infrastruktūra, nedelsdamas, bet ne vėliau kaip per 10 darbo dienų apie tai informuoja Atsakingą instituciją. 13. Atsakinga institucija, gavusi 12 punkte nurodytą informaciją, nustato ypatingos svarbos infrastruktūros objektus, nustato ypatingos svarbos informacinę infrastruktūrą, ją įvertina ir teikia tvirtinti Metodikos II, III ir IV skyriuose nustatyta tvarka. 14. Jeigu per dvejus metus neįvyksta ypatingos svarbos infrastruktūros objekto, ypatingos svarbos informacinės infrastruktūros ir (arba) jos valdymo pokyčių, Atsakinga institucija inicijuoja turimos informacijos peržiūrą ir prireikus atnaujina informaciją ir teikia ją tvirtinti Metodikos II, III ir IV skyriuose nustatyta tvarka.	Visiškas
7. 23 straipsnyje nurodytos peržiūros tikslais ir ne vėliau kaip 2018 m. lapkričio 9 d., o vėliau – kas dvejus metus, valstybės	**1. Kibernetinio saugumo įstatymas** <...>	Visiškas

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 techninės gaires dėl parametrų, taikomų šioje dalyje nurodytai informacijai.	**8 straipsnis. Nacionalinis kibernetinio saugumo centras** <...> 2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką: <...> 14) bendradarbiauja su tarptautinių organizacijų kompetentingomis institucijomis, jų įsteigtomis bendradarbiavimo grupėmis ir užsienio valstybių kompetentingomis institucijomis ir tarnybomis, turi teisę jas pasitelkti kartu atliekant šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje; <...> **2. YSII nustatymo metodikos projektas** **V skyrius. Baigiamosios nuostatos** <...> 16. Krašto apsaugos ministerija kas dvejus metus teikia informaciją Europos Komisijai apie nacionalines ypatingos svarbos informacinės infrastruktūros nustatymo priemones, ypatingos svarbos paslaugų sąrašą, 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 (OL 2016 L 194, p. 1) II priede nurodytuose sektoriuose nustatytos informacinės infrastruktūros valdytojų skaičių ir vartotojų skaičiaus, nustatant ypatingos svarbos informacinę infrastruktūrą, kriterijus.	
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;	**YSII nustatymo metodikos projektas** **II skyrius. Ypatingos svarbos infrastruktūros objektų nustatymas** <...> 6. Ypatingos svarbos infrastruktūros objektai nustatomi šia tvarka:	Visiškas

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; 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.	6.1. Atsakinga institucija nustato visus jos veiklos srityje veikiančius infrastruktūros objektus, turinčius reikšmės teikiant ypatingos svarbos paslaugas. 6.2. Atsakinga institucija kreipiasi į instituciją, įstaigą, įmonę ar jos struktūrinį padalinį, kurie yra infrastruktūros objektai, ar į infrastruktūros objekto valdytoją, kai infrastruktūros objektas yra įrenginys ar įrenginio dalis (toliau – Atsakingas valdytojas), prašydama Atsakingo valdytojo atlikti visų jo valdomų 6.1 papunkčio nustatyta tvarka nustatytų infrastruktūros objektų svarbos vertinimą ir užpildyti Metodikos 2 priede pateiktą klausimyną (toliau – Klausimynas). Jeigu Atsakinga institucija ir Atsakingas valdytojas yra tas pats subjektas, Klausimyną pildo Atsakinga institucija. 6.3. Atsakingas valdytojas ne vėliau kaip per 20 darbo dienų nuo 6.2 papunktyje nurodyto prašymo gavimo užpildo Klausimyną ir teikia jį raštu Atsakingai institucijai. 6.4. Atsakinga institucija įvertina Atsakingo valdytojo pateiktą Klausimyną ir prireikus teikia Atsakingam valdytojui pastabas ir pasiūlymus, kartu nurodydama terminą, kurio reikia Klausimynui patikslinti. Atsakinga institucija turi teisę prašyti Atsakingo valdytojo papildomos informacijos, kuri reikalinga Klausimynui patikslinti, taip pat turi teisę Klausimyne papildomai nustatyti ir įvertinti jos veiklos srities sektoriaus specifinius kriterijus, galinčius turėti įtakos jos veiklos srityje veikiančių Atsakingų valdytojų veiklai. 6.5. Infrastruktūros objektų, kurie, atsižvelgiant į Atsakingos institucijos vertinimą ir Klausimyno kriterijus, įvertinami 16 ar daugiau balų, teikiamų paslaugų sutrikdymo neigiamas poveikis yra didelis, todėl šie infrastruktūros objektai nustatomi kaip ypatingos svarbos infrastruktūros objektai. <...> **III skyrius. Ypatingos svarbos informacinės infrastruktūros**	

	nustatymas <...> 8. Ypatingos svarbos informacinė infrastruktūra nustatoma šia tvarka: 8.1. Atsakinga institucija, Metodikos II skyriuje nustatyta tvarka nustačiusi ypatingos svarbos infrastruktūros objektus, kreipiasi į Atsakingą valdytoją prašydama jo nustatyti ypatingos svarbos informacinę infrastruktūrą užpildant Metodikos 3 priede pateiktą ypatingos svarbos informacinės infrastruktūros nustatymo lentelę (toliau – Lentelė) ir įtraukti nustatytą ypatingos svarbos informacinę infrastruktūrą į ypatingos svarbos informacinės infrastruktūros sąrašą (toliau – Sąrašas) užpildant Metodikos 4 priede pateiktą lentelę. 8.2. Atsakingas valdytojas ne vėliau kaip per 20 darbo dienų nuo 8.1 papunktyje nurodyto prašymo gavimo užpildo Lentelę ir Sąrašą ir pateikia raštu Atsakingai institucijai. 8.3. Atsakinga institucija įvertina Atsakingo valdytojo pateiktą Lentelę ir Sąrašą ir prireikus teikia Atsakingam valdytojui pastabas ir pasiūlymus, kartu nurodydama terminą, kurio reikia Lentelei ir Sąrašui patikslinti. Atsakinga institucija turi teisę prašyti Atsakingo valdytojo papildomos informacijos, kuri reikalinga Lentelei ir Sąrašui patikslinti. 8.4. Jeigu Atsakinga institucija ir Atsakingas Valdytojas yra tas pats subjektas, Lentelę ir Sąrašą pildo Atsakinga institucija. 8.5. Jeigu užpildytame Klausimyne, Lentelėje, Sąraše nurodyta, kad ypatingos svarbos paslauga teikiama dviejose ar daugiau Europos Sąjungos valstybėse narėse, Atsakinga institucija prieš priimdama sprendimą dėl ypatingos svarbos informacinės infrastruktūros nustatymo konsultuojasi su Europos Sąjungos valstybių narių institucijomis, kurių veiklos sritys apima užpildytame Klausimyne, Lentelėje, Sąraše nurodytus ypatingos svarbos sektorius, subsektorius ir juose teikiamas ypatingos	

	svarbos paslaugas. 8.6. Informacinė infrastruktūra, kuri atlikus Atsakingos institucijos vertinimą atitinka visus Lentelėje nustatytus kriterijus, nustatoma kaip ypatingos svarbos informacinė infrastruktūra. **YSII nustatymo metodikos projekto 2 ir 3 priedai.**	
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.	**1. Kibernetinio saugumo įstatymas** <...> **14 straipsnis. Tarpinstitucinis bendradarbiavimas valdant ir tiriant kibernetinius incidentus** 1. Nacionalinis kibernetinio saugumo centras ir policija konsultuojasi ir bendradarbiauja tiriant kibernetinius incidentus, keičiasi su kibernetinių incidentų tyrimu susijusia informacija, reikalinga pagal kompetenciją šių institucijų funkcijoms atlikti. Prireikus apie kibernetinių incidentų tyrimą gali būti pranešama kitiems kriminalinės žvalgybos subjektams ir (arba) žvalgybos institucijoms. 2. Nacionalinis kibernetinio saugumo centras ir Valstybinė duomenų apsaugos inspekcija bendradarbiauja tiriant kibernetinius incidentus, susijusius su asmens duomenų ir (ar) privatumo apsaugos pažeidimais, keičiasi informacija, reikalinga teisės aktų nustatytoms funkcijoms, susijusioms su asmens duomenų ir (ar) privatumo apsaugą pažeidžiančių kibernetinių incidentų tyrimu, atlikti. 3. Tarpinstitucinio bendradarbiavimo valdant ir tiriant kibernetinius incidentus tvarka nustatoma Nacionaliniame kibernetinių incidentų valdymo plane. **2. Kibernetinių incidentų valdymo plano projektas** **IV skyrius. Kibernetinių incidentų tyrimas** **Trečiasis skirsnis. Tarpinstitucinis bendradarbiavimas ir**	Visiškas

	keitimasis informacija tiriant kibernetinius incidentus <...> 46. KIVT institucija, gavusi informaciją apie kibernetinį incidentą, nedelsdama, bet ne vėliau kaip per 24 val. nuo informacijos apie kibernetinį incidentą gavimo informuoja kitas KIVT institucijas: 46.1. Nacionalinį kibernetinio saugumo centrą – nustačiusi, kad kibernetinis incidentas taip pat gali paveikti kibernetinio saugumo subjektų ryšių ir informacines sistemas; 46.2. Lietuvos policiją – nustačiusi, kad kibernetinis incidentas gali turėti nusikalstamos veikos požymių; 46.3. Valstybinę duomenų apsaugos inspekciją – nustačiusi, kad kibernetinis incidentas gali būti susijęs su asmens duomenų saugumo pažeidimais. 47. KIVT institucija, pagal kompetenciją tirianti kibernetinį incidentą, nustačiusi papildomos informacijos apie kibernetinį incidentą poreikį, kreipiasi į kitas KIVT institucijas, kurios papildomą informaciją turi pateikti per KIVT institucijos, pagal kompetenciją tiriančios kibernetinį incidentą, prašyme nurodytą terminą. 48. Kibernetinio saugumo subjektai ir KIVT institucijos šiame Plane nurodytą informaciją, susijusią su kibernetiniais incidentais ir jų valdymu, perduoda per kibernetinio saugumo informacinį tinklą, o jeigu tokios galimybės nėra, kitomis saugiomis informacijos perdavimo priemonėmis.	
4. Valstybės narės informuoja Komisiją apie jų CSIRT incidentų valdymo proceso mastą ir pagrindinius elementus.	**1. Kibernetinio saugumo įstatymas** **8 straipsnis. Nacionalinis kibernetinio saugumo centras** 2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką: <...> 14) bendradarbiauja su tarptautinių organizacijų kompetentingomis institucijomis, jų įsteigtomis	Visiškas

	bendradarbiavimo grupėmis ir užsienio valstybių kompetentingomis institucijomis ir tarnybomis, turi teisę jas pasitelkti kartu atliekant šio įstatymo ir kitų teisės aktų nustatytas funkcijas kibernetinio saugumo srityje; <...> **2. Kibernetinių incidentų valdymo plano projektas** **IV skyrius. Kibernetinių incidentų tyrimas** **Ketvirtasis skirsnis. Tarptautinis bendradarbiavimas ir keitimasis informacija tiriant kibernetinius incidentus** <...> 52. Nacionalinis kibernetinio saugumo centras, koordinuodamas tarptautinio ir tarpinstitucinio bendradarbiavimo veiksmus: <...> 52.2. informuoja Europos Komisiją apie kibernetinių incidentų valdymo proceso mastą ir pagrindinius elementus ir kiekvienais metais 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;	
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.	**1. Kibernetinio saugumo įstatymas** **11 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos** 1. Kibernetinio saugumo subjektai: <...> 3) Nacionaliniame kibernetinių incidentų valdymo plane nustatytomis sąlygomis ir tvarka praneša Nacionaliniam kibernetinio saugumo centrui apie jų valdomose ir (arba) tvarkomose ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones; <...> **2. Kibernetinių incidentų valdymo plano projektas**	Visiškas

	III skyrius. Informavimas apie kibernetinius incidentus <...> 14. Kibernetinio saugumo subjektai Nacionalinį kibernetinio saugumo centrą informuoja apie: 14.1. didelio poveikio kibernetinius incidentus – nedelsiant, bet ne vėliau kaip per 1 valandą nuo jų nustatymo; 14.2. vidutinio poveikio kibernetinius incidentus – ne vėliau kaip per 4 valandas nuo jų nustatymo; 14.3. nereikšmingo poveikio kibernetinius incidentus – periodiškai kiekvieno kalendorinio mėnesio 1 dieną teikiant informaciją apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo teikimo dienos, skaičių.	
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 perkelta į Kibernetinių incidentų valdymo plano projektą.** **IV skyrius. Kibernetinių incidentų tyrimas** **Ketvirtasis skirsnis. Tarptautinis bendradarbiavimas ir keitimasis informacija tiriant kibernetinius incidentus** <...> 52. Nacionalinis kibernetinio saugumo centras, koordinuodamas tarptautinio ir tarpinstitucinio bendradarbiavimo veiksmus: <...> 52.2. informuoja Europos Komisiją apie kibernetinių incidentų valdymo proceso mastą ir pagrindinius elementus ir kiekvienais metais bendradarbiavimo grupei pateikia suvestinę ataskaitą apie gautus pranešimus, kurioje, be kita ko, nurodomas pranešimų skaičius ir incidentų, apie kuriuos pranešta, pobūdis, taip pat	Visiškas

	veiksmai, kurių buvo imtasi;	
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.	**1. Kibernetinio saugumo įstatymas** **11 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos** 1. Kibernetinio saugumo subjektai: 1) atsako už jų valdomų ryšių ir informacinių sistemų ar teikiamų paslaugų kibernetinį saugumą, užtikrina jų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams; 2) organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše nustatyta tvarka atlieka rizikos vertinimą ir įdiegia kitas, naujausiais technikos laimėjimais paremtas ir nustatytai rizikai proporcingas, technines ir organizacines kibernetinio saugumo priemones; <...> **2. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo projektas** **III skyrius. Organizaciniai kibernetinio saugumo reikalavimai subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams** <...> 6. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai: 6.1. ne rečiau kaip kartą per metus arba po esminių organizacinių ar sisteminių pokyčių šio Aprašo II skyriuje nustatyta tvarka organizuoja ir atlieka grėsmių ir pažeidžiamumų, galinčių turėti įtakos valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros kibernetiniam saugumui, rizikos vertinimą. Šį rizikos vertinimą subjektai, valdantys ir (arba)	Visiškas

	tvarkantys valstybės informacinius išteklius, ir ypatingos svarbos informacinės infrastruktūros valdytojai turi teisę atlikti kartu su valstybės informacinių išteklių rizikos ar ypatingos svarbos informacinės infrastruktūros rizikos vertinimu ir (arba) informacinių technologijų saugos atitikties vertinimu; <...> **IV skyrius. Techniniai kibernetinio saugumo reikalavimai subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams** <...> 17. Kibernetinio saugumo priemonės, nurodytos Aprašo priede, turi būti diegiamos atsižvelgiant į naujausius technikos laimėjimus, vadovaujantis gamintojo pateikiama bent viena gerąja saugumo praktikos rekomendacija.	
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.	**1. Kibernetinio saugumo įstatymas** **11 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos** 1. Kibernetinio saugumo subjektai: 1) atsako už jų valdomų ryšių ir informacinių sistemų ar teikiamų paslaugų kibernetinį saugumą, užtikrina jų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams; 2) organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše nustatyta tvarka atlieka rizikos vertinimą ir įdiegia kitas, naujausiais technikos laimėjimais paremtas ir nustatytai rizikai proporcingas, technines ir organizacines kibernetinio saugumo priemones; <...> 5) paskiria kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, ir Nacionaliniam kibernetinio saugumo centrui pateikia šio asmens	Visiškas

	ar padalinio kontaktinę informaciją; <...> **12 straipsnis. Specialiosios kibernetinio saugumo subjektų pareigos** 1. Ypatingos svarbos informacinės infrastruktūros valdytojai: 1) vadovaudamiesi krašto apsaugos ministro patvirtintu tipiniu kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planu, patvirtina ir Nacionaliniam kibernetinio saugumo centrui pateikia kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus; <...> 3) ne rečiau kaip kartą per kalendorinius metus išbando kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planuose numatytų priemonių veikimą ir bandymų rezultatus organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše nustatyta tvarka pateikia Nacionaliniam kibernetinio saugumo centrui; 4) sudaro sąlygas Nacionaliniam kibernetinio saugumo centrui diegti ir valdyti technines kibernetinio saugumo priemones ypatingos svarbos informacinėje infrastruktūroje ir taikyti technines priemones, siekiant įvertinti ypatingos svarbos informacinių infrastruktūrų atsparumą kibernetiniams incidentams. <...> **2. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo projektas** **III skyrius. Organizaciniai kibernetinio saugumo reikalavimai subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams**	

	<...> 6. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai: 6.2. atsižvelgdami į atlikto rizikos vertinimo rezultatus ir jeigu nustatoma incidentų valdymo ir šalinimo, taip pat organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, tobulina veiklos tęstinumo valdymo planus ar kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus. Veiklos tęstinumo valdymo planų ar kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planų veikimo bandymų rezultatai išdėstomi šių planų bandymo ataskaitose, kurių kopijos ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikiamos Nacionaliniam kibernetinio saugumo centrui;	
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.	**1. Kibernetinio saugumo įstatymas** **11 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos** 1. Kibernetinio saugumo subjektai: <...> 3) Nacionaliniame kibernetinių incidentų valdymo plane nustatytomis sąlygomis ir tvarka praneša Nacionaliniam kibernetinio saugumo centrui apie jų valdomose ir (arba) tvarkomose ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones; **2. Kibernetinių incidentų valdymo plano projektas** **III skyrius. Informavimas apie kibernetinius incidentus** <...> 14. Kibernetinio saugumo subjektai Nacionalinį kibernetinio saugumo centrą informuoja apie:	Visiškas

	14.1. didelio poveikio kibernetinius incidentus – nedelsiant, bet ne vėliau kaip per 1 valandą nuo jų nustatymo; <...> Nacionalinio kibernetinių incidentų valdymo plano projekto priedas **KIBERNETINIŲ INCIDENTŲ KATEGORIJŲ SĄRAŠAS** Didelis incidento poveikis Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	
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.	**Kibernetinių incidentų valdymo plano projektas** Nacionalinio kibernetinių incidentų valdymo plano projekto priedas **KIBERNETINIŲ INCIDENTŲ KATEGORIJŲ SĄRAŠAS** Nereikšmingas incidento poveikis: • RIS trikdoma < 1 val. • Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 % • Paslauga teikiama, bet trikdoma Vidutinis incidento poveikis: • RIS trikdoma ≥ 1 val., bet < 2 val. • Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 % • Paslauga trikdoma dalyje šalies teritorijos Didelis incidento poveikis: • RIS trikdoma ≥ 2 val. • Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25,% • Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Visiškas
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	**Kibernetinių incidentų valdymo plano projektas** **IV skyrius. Kibernetinių incidentų tyrimas** **Ketvirtasis skirsnis. Tarptautinis bendradarbiavimas ir keitimasis informacija tiriant kibernetinius incidentus**	Visiškas

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 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.	<...> 52. Nacionalinis kibernetinio saugumo centras, koordinuodamas tarptautinio ir tarpinstitucinio bendradarbiavimo veiksmus: 52.3. informuoja kitas Europos Sąjungos valstybes nares, jų CSIRT apie pavojingus ir didelio poveikio kibernetinius incidentus, kai gali būti paveiktas daugiau negu vienos valstybės narės ypatingos svarbos informacinės infrastruktūros paslaugų teikimas; <...> 53. Koordinuodamas tarptautinio ir tarpinstitucinio bendradarbiavimo veiksmus, Nacionalinis kibernetinio saugumo centras kibernetinio saugumo subjektų pateikta informacija, įskaitant ir konfidencialią informaciją, turi teisę keistis tik tiek, kiek tai yra būtina tarptautinio ir tarpinstitucinio bendradarbiavimo koordinavimui, ir užtikrina gautos informacijos apsaugą.	
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; b) incidentų valdymą; c) veiklos tęstinumo valdymą; d) stebėseną, auditą ir bandymus; e) atitiktį tarptautiniams standartams.	**1. Kibernetinio saugumo įstatymas** **11 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos** 1. Kibernetinio saugumo subjektai: <...> 2) organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše nustatyta tvarka atlieka rizikos vertinimą ir įdiegia kitas, naujausiais technikos laimėjimais paremtas ir nustatytai rizikai proporcingas, technines ir organizacines kibernetinio saugumo priemones; **2. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo projektas** **VI skyrius. Elektroninės informacijos prieglobos paslaugų teikėjų ir skaitmeninių paslaugų teikėjų organizaciniai ir techniniai kibernetinio saugumo reikalavimai**	Visiškas

	<...> 19. Elektroninės informacijos prieglobos paslaugų teikėjai ir skaitmeninių paslaugų teikėjai: 19.1. ne rečiau kaip kartą per 2 metus arba po esminių organizacinių ar sisteminių pokyčių šio Aprašo II skyriuje nustatyta tvarka organizuoja ir atlieka grėsmių ir pažeidžiamumų, galinčių turėti įtakos savo teikiamų elektroninės informacijos prieglobos ar skaitmeninių paslaugų kibernetiniam saugumui, rizikos vertinimą. Šį rizikos vertinimą elektroninės informacijos prieglobos paslaugų teikėjai ir skaitmeninių paslaugų teikėjai turi teisę atlikti kartu su veiklos rizikos vertinimu ir (arba) informacinių technologijų saugos atitikties vertinimu; <...> 19.4. tvirtina ir, kai įvyksta esminių organizacinių ar sisteminių pokyčių, atnaujina savo paslaugų kibernetinio saugumo valdymo taisykles, o Nacionaliniam kibernetinio saugumo centrui pareikalavus, jas pateikia Nacionaliniam kibernetinio saugumo centrui. Elektroninės informacijos prieglobos paslaugų ar skaitmeninių paslaugų kibernetinio saugumo valdymo taisyklėse nurodoma: 19.4.1. kibernetiniams incidentams valdyti reikalingų priemonių aprašymai; 19.4.2. elektroninės informacijos prieglobos paslaugų ar skaitmeninių paslaugų nepertraukiamo teikimo užtikrinimo planas ir jo taikymo sąlygos bei maksimalus leistinas paslaugos neveikimo laikas; 19.4.3. už kibernetinių incidentų valdymą atsakingų asmenų funkcijos ir atsakomybė; 19.4.4. viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugoms teikti naudojamų sistemų ir įrangos stebėsenos, patikrinimo, testavimo bei auditavimo tvarka ir sąlygos; 19.4.5. atitiktis Lietuvos ir tarptautiniams standartams,	

	apibūdinantiems kibernetinį saugumą ar saugų elektroninės informacijos tvarkymą;	
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.	**1. Kibernetinio saugumo įstatymas** **11 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos** 1. Kibernetinio saugumo subjektai: 1) atsako už jų valdomų ryšių ir informacinių sistemų ar teikiamų paslaugų kibernetinį saugumą, užtikrina jų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams; <...> **2. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo projektas** **VI skyrius. Elektroninės informacijos prieglobos paslaugų teikėjų ir skaitmeninių paslaugų teikėjų organizaciniai ir techniniai kibernetinio saugumo reikalavimai** <...> 19. Elektroninės informacijos prieglobos paslaugų teikėjai ir skaitmeninių paslaugų teikėjai: 19.1. ne rečiau kaip kartą per 2 metus arba po to esminių organizacinių ar sisteminių pokyčių šio Aprašo II skyriuje nustatyta tvarka organizuoja ir atlieka grėsmių ir pažeidžiamumų, galinčių turėti įtakos savo teikiamų elektroninės informacijos prieglobos ar skaitmeninių paslaugų kibernetiniam saugumui, rizikos vertinimą. Šį rizikos vertinimą elektroninės informacijos prieglobos paslaugų teikėjai ir skaitmeninių paslaugų teikėjai turi teisę atlikti kartu su veiklos rizikos vertinimu ir (arba) informacinių technologijų saugos atitikties vertinimu; 19.2. kartu su viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjais imasi reikiamų priemonių kibernetiniam saugumui užtikrinti; 19.3. įgyvendina organizacines ir technines priemones, kurios	Visiškas

	užtikrintų jų elektroninės informacijos prieglobos ar skaitmeninėms paslaugoms teikti naudojamų sistemų ir įrangos kibernetinį saugumą; 19.4. tvirtina ir, kai įvyksta esminių organizacinių ar sisteminių pokyčių, atnaujina savo paslaugų kibernetinio saugumo valdymo taisykles, o Nacionaliniam kibernetinio saugumo centrui pareikalavus, jas pateikia Nacionaliniam kibernetinio saugumo centrui. Elektroninės informacijos prieglobos paslaugų ar skaitmeninių paslaugų kibernetinio saugumo valdymo taisyklėse nurodoma: 19.4.1. kibernetiniams incidentams valdyti reikalingų priemonių aprašymai; 19.4.2. elektroninės informacijos prieglobos paslaugų ar skaitmeninių paslaugų nepertraukiamo teikimo užtikrinimo planas ir jo taikymo sąlygos bei maksimalus leistinas paslaugos neveikimo laikas; 19.4.3. už kibernetinių incidentų valdymą atsakingų asmenų funkcijos ir atsakomybė; 19.4.4. viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugoms teikti naudojamų sistemų ir įrangos stebėsenos, patikrinimo, testavimo bei auditavimo tvarka ir sąlygos; 19.4.5. atitiktis Lietuvos ir tarptautiniams standartams, apibūdinantiems kibernetinį saugumą ar saugų elektroninės informacijos tvarkymą; 19.5. neatlygintinai informuoja elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjus apie nustatytus kibernetinius incidentus, susijusius su elektroninės informacijos prieglobos ar skaitmeninėmis paslaugomis, priskirtus prie turinčių didelį poveikį, nustatytą Nacionaliniame kibernetinių incidentų valdymo plane; 19.6. ne vėliau kaip prieš 5 darbo dienas informuoja elektroninės informacijos prieglobos paslaugų ar skaitmeninių paslaugų	

	gavėjus ir Nacionalinį kibernetinio saugumo centrą apie numatomus planinius darbus, kuriuos atliekant yra tikimybė sutrikdyti elektroninės informacijos prieglobos ar skaitmeninių paslaugų kibernetinį saugumą; 19.7. informuoja elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjus, kuriose šalyse gali būti saugoma jų elektroninė informacija, kuri yra kuriama, tvarkoma ar pateikta saugoti naudojantis elektroninės informacijos prieglobos ar skaitmeninėmis paslaugomis, ir kokiais atvejais tokia informacija perkeliama į kitas šalis; 19.8. nustato elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjų įspėjimo apie elektroninės informacijos prieglobos ar skaitmeninių paslaugų kibernetinio saugumo pažeidimus tvarką ir kokių veiksmų tokiu atveju privalo imtis elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjai ir (ar) teikėjai; 19.9. viešai skelbia rekomendacijas elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjams apie priemones kibernetiniam saugumui užtikrinti naudojantis elektroninės informacijos prieglobos ar skaitmeninėmis paslaugomis.	
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.	**1. Kibernetinio saugumo įstatymas** **11 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos** 1. Kibernetinio saugumo subjektai: <...> 3) Nacionaliniame kibernetinių incidentų valdymo plane nustatytomis sąlygomis ir tvarka praneša Nacionaliniam kibernetinio saugumo centrui apie jų valdomose ir (arba) tvarkomose ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones.	Visiškas

	2. Kibernetinių incidentų valdymo plano projektas **III skyrius. Informavimas apie kibernetinius incidentus** <...> 14. Kibernetinio saugumo subjektai Nacionalinį kibernetinio saugumo centrą informuoja apie: 14.1. didelio poveikio kibernetinius incidentus – nedelsiant, bet ne vėliau kaip per 1 valandą nuo jų nustatymo; <...> Nacionalinio kibernetinių incidentų valdymo plano projekto priedas **KIBERNETINIŲ INCIDENTŲ KATEGORIJŲ SĄRAŠAS** Didelis incidento poveikis Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	
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; 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 įstatymas** **11 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos** 1. Kibernetinio saugumo subjektai: <...> 3) Nacionaliniame kibernetinių incidentų valdymo plane nustatytomis sąlygomis ir tvarka praneša Nacionaliniam kibernetinio saugumo centrui apie jų valdomose ir (arba) tvarkomose ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones; <...> **2. Kibernetinių incidentų valdymo plano projektas** Nacionalinio kibernetinių incidentų valdymo plano projekto priedas **KIBERNETINIŲ INCIDENTŲ KATEGORIJŲ SĄRAŠAS** Didelis incidento poveikis: • RIS trikdoma ≥ 2 val. • Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo	Visiškas

	vietų skaičius ≥ 1000, arba 25,% • Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje • Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas • Nuostoliai ≥ 500 000 Eur	
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.	**1. Kibernetinio saugumo įstatymas** **12 straipsnis. Specialiosios kibernetinio saugumo subjektų pareigos** 1. Ypatingos svarbos informacinės infrastruktūros valdytojai: <...> 2) Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka praneša skaitmeninių paslaugų teikėjams apie neigiamą poveikį ypatingos svarbos informacinės infrastruktūros veiklai, kurį lėmė skaitmeninių paslaugų teikėjų ryšių ir informacinėse sistemose įvykę sutrikimai. **2. Kibernetinių incidentų valdymo plano projektas** **III skyrius. Informavimas apie kibernetinius incidentus** <...> 17. Ypatingos svarbos informacinės infrastruktūros valdytojai, kurių paslaugų teikimas priklauso nuo trečiųjų šalių skaitmeninių paslaugų teikėjų teikiamų paslaugų, nedelsdami, bet ne vėliau kaip per 1 valandą nuo jų nustatymo informuoja Nacionalinį kibernetinio saugumo centrą ir skaitmeninių paslaugų teikėjus apie neigiamą poveikį ypatingos svarbos infrastruktūros veiklai, kurį lėmė skaitmeninių paslaugų teikėjų ryšių ir informacinėse sistemose įvykę sutrikimai.	Visiškas
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	**1. Kibernetinio saugumo įstatymas** **16 straipsnis. Savanoriškas pranešimas apie kibernetinius incidentus** 1. Asmenys, kuriems šiame įstatyme nėra nustatytos pareigos	Visiškas

<table>
<tr>
<td>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.</td>
<td>pranešti apie kibernetinius incidentus jų valdomose ryšių ir informacinėse sistemose, turi teisę savanoriškai pranešti Nacionaliniam kibernetinio saugumo centrui apie kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones. Nacionalinis kibernetinio saugumo centras tokius pranešimus tvarko Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka.
2. Asmeniui, savanoriškai pranešusiam apie kibernetinį incidentą, nenustatoma pareigų, susijusių su pranešimo pateikimu.

2. Kibernetinių incidentų valdymo plano projektas
III skyrius. Informavimas apie kibernetinius incidentus
<...>
18. Asmenys, kuriems teisės aktuose nėra nustatytos pareigos pranešti apie kibernetinius incidentus jų valdomose ryšių ir informacinėse sistemose, turi teisę savanoriškai pranešti Nacionaliniam kibernetinio saugumo centrui apie kibernetinius incidentus ir taikytas kibernetinių incidentų tyrimo ar valdymo priemones Nacionalinio kibernetinio saugumo centro interneto svetainėje nurodytais kontaktais.</td>
<td></td>
</tr>
<tr>
<td>2 priedas. Subjektų rūšys 4 straipsnio 4 punkto taikymo tikslais
<table><tr><td>7. Skaitmeninė infrastruktūra</td><td></td><td>— IXP</td></tr><tr><td></td><td></td><td>— DNS paslaugų teikėjai</td></tr><tr><td></td><td></td><td>— ALD vardų registrai</td></tr></table></td>
<td>YSII nustatymo metodikos projektas
Ypatingos svarbos informacinės infrastruktūros nustatymo metodikos projekto 1 priedas
YPATINGOS SVARBOS SEKTORIAI, SUBSEKTORIAI, PASLAUGOS IR ATSAKINGOS INSTITUCIJOS
<...>
6. Informacinių technologijų ir elektroninių ryšių sektorius
6.1. Skaitmeninės infrastruktūros subsektorius
6.1.1. Interneto duomenų srautų mainų taško (IXP) paslauga
6.1.2. Domenų vardų sistemos (DNS) paslauga
6.1.3. Aukščiausio lygio domenų vardų registro (lt. domeno)</td>
<td></td>
</tr>
</table>

	paslauga	

Lietuvos Respublikos
vidaus reikalų ministras
Eimutis Misiūnas
2018-11-06

Krašto apsaugos viceministras
Edvinas Kerza