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 identifikavimo metodika (toliau – YSII identifikavimo 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 identifikavimo 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** – tinklo įrenginys, per kurį siekiant palengvinti interneto duomenų srautų mainus sujungiamos daugiau nei dvi nepriklausomos autonominės sistemos. Interneto duomenų srautų mainų taškas sujungia tik autonomines sistemas; jį naudojant nebūtina, kad interneto duomenų srautai, kuriais mainosi autonominių sistemų pora, būtų perduodami per trečią autonominę sistemą; be to, jis nekeičia ir netrikdo tokių srautų.	
14) **domenų vardų sistema (DNS)** – pagal hierarchiją suskirstyta vardų suteikimo sistema tinkle, kuris persiunčia domenų vardų užklausas;	**YSII identifikavimo metodikos projektas** **I skyrius. Bendrosios nuostatos** <...> 2. Metodikoje vartojamos sąvokos: 2.2. **Domenų vardų sistema** – hierarchiškai suskirstyta vardų suteikimo sistema tinkle, kuris persiunčia domenų vardų užklausas.	Visiškas
15) **DNS paslaugų teikėjas** – subjektas, kuris teikia DNS paslaugas internetu;	**YSII identifikavimo metodikos projektas** **I skyrius. Bendrosios nuostatos** <...> 2. Metodikoje vartojamos sąvokos: 2.3. **Domenų vardų sistemos paslaugų teikėjas** – subjektas, teikiantis domenų vardų sistemos 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 identifikavimo metodikos projektas** **I skyrius. Bendrosios nuostatos** <...> 2. Metodikoje vartojamos sąvokos: 2.1. **Aukščiausio lygio domenų vardų registro tvarkytojas** – subjektas, registruojantis ir administruojantis interneto domenų vardus su konkrečiu aukščiausio lygio domenu.	Visiškas
5 straipsnis. Esminių paslaugų operatorių identifikavimas	**1. Lietuvos Respublikos Vyriausybės nutarimo „Dėl Lietuvos**	Visiškas

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.	**Respublikos kibernetinio saugumo įstatymo įgyvendinimo" projektas** <...> 4. Pavesti: 4.1. institucijoms, nurodytoms Metodikos 1 priede, iki 2019 m. vasario 1 d. Metodikos nustatyta tvarka inicijuoti ypatingos svarbos infrastruktūros objektų peržiūrą ir kreiptis į institucijas, įstaigas, įmones ar jos struktūrinius padalinius, kurie yra infrastruktūros objektai, ar į infrastruktūros objekto valdytojus, kai infrastruktūros objektas yra įrenginys ar įrenginio dalis (toliau – Atsakingas valdytojas), prašant Atsakingų valdytojų atlikti visų jų valdomų infrastruktūros objektų svarbos vertinimą ir užpildyti Metodikos 2 priede pateiktą klausimyną; **2. YSII identifikavimo metodikos projektas** Ypatingos svarbos informacinės infrastruktūros identifikavimo 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. Finansų sektorius 3.1. Kredito įstaigų subsektorius	

	3.2. Finansinių rinkų infrastruktūros subsektorius 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 identifikavimo metodikos projektas** **III skyrius. Ypatingos svarbos informacinės infrastruktūros nustatymas** <...> 6.1. Atsakinga institucija nustato visus jos veiklos srityje veikiančius infrastruktūros objektus, turinčius reikšmės teikiant ypatingos svarbos paslaugas, ir 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 infrastruktūros objektų svarbos vertinimą ir užpildyti Metodikos 2 priede pateiktą klausimyną (toliau – Klausimynas). **YSII identifikavimo metodikos projekto 2 ir 3 priedai.**	Visiškas
3. 1 dalies tikslais kiekviena valstybė narė sudaro 2 dalies a punkte nurodytų paslaugų sąrašą.	**YSII identifikavimo 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 veikiančius infrastruktūros objektus, turinčius reikšmės teikiant	Visiškas

	ypatingos svarbos paslaugas, ir 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 infrastruktūros objektų svarbos vertinimą ir užpildyti Metodikos 2 priede pateiktą klausimyną (toliau – Klausimynas). 6.2. Atsakingas valdytojas ne vėliau kaip per dvidešimt darbo dienų nuo 6.1 papunktyje nurodyto prašymo gavimo dienos užpildo Klausimyną ir teikia jį raštu Atsakingai institucijai. Jeigu Atsakinga institucija ir Atsakingas valdytojas yra tas pats subjektas, Klausimyną pildo Atsakinga institucija. 6.3. Atsakinga institucija įvertina Atsakingo valdytojo pateiktą Klausimyną ir prireikus teikia Atsakingam valdytojui pastabas ir pasiūlymus, kartu nurodydama terminą 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. 6.4. Infrastruktūros objektų, kurių suminis svarbos balas, atsižvelgiant į Atsakingos institucijos vertinimą, atliktą vadovaujantis Metodikos 15 punkte nurodyta metodine medžiaga, ir Klausimyno kriterijus, sudaro šešiolika ar daugiau balų, teikiamų paslaugų sutrikdymo neigiamas poveikis yra didelis, todėl šie infrastruktūros objektai Atsakingos institucijos 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 vyksta prieš priimant sprendimą dėl identifikavimo.	**YSII identifikavimo metodikos projektas** **III skyrius. Ypatingos svarbos informacinės infrastruktūros nustatymas** <...> 8.4. Jeigu užpildytame Klausimyne, Lentelėje, Sąraše nurodyta,	Visiškas

	kad ypatingos svarbos paslauga teikiama dviejose ar daugiau Europos Sąjungos valstybių narių, Atsakinga institucija, prieš priimdama sprendimą dėl ypatingos svarbos informacinės infrastruktūros nustatymo, siekiant nustatyti, kurioje Europos Sąjungos valstybėje turėtų būti taikomas ypatingos svarbos paslaugos reguliavimas, 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. Krašto apsaugos ministerija kartu su Nacionaliniu kibernetinio saugumo centru koordinuoja pasikeitimą duomenimis ir informacija, perduodama Europos Sąjungos valstybių narių institucijų, 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 identifikavimo 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 steigiamas naujas infrastruktūros objektas, skirtas ypatingos svarbos paslaugoms teikti, kurio funkcionavimas pagrįstas informacine infrastruktūra, nedelsdamas, bet ne vėliau kaip per dešimt darbo dienų nuo pokyčių arba sprendimo steigti naują infrastruktūros objektą priėmimo dienos apie tai informuoja Atsakingą instituciją. 13. Atsakinga institucija, gavusi 12 punkte nurodytą informaciją, inicijuoja ypatingos svarbos infrastruktūros objektų peržiūrą ir ne vėliau kaip per dvidešimt darbo dienų nuo 12 punkte nurodytos informacijos gavimo kreipiasi į Atsakingą valdytoją, prašydama	Visiškas

	atlikti visų jo valdomų infrastruktūros objektų svarbos vertinimą ir užpildyti Klausimyną. Atsakinga institucija nustato ypatingos svarbos infrastruktūros objektus, ypatingos svarbos informacinę infrastruktūrą, ją įvertina ir teikia tvirtinti Metodikos II, III ir IV skyriuose nurodyta tvarka. 14. Jeigu per dvejus metus neįvyksta ypatingos svarbos infrastruktūros objekto, ypatingos svarbos informacinės infrastruktūros ir (arba) jos valdymo pokyčių, Atsakinga institucija inicijuoja ypatingos svarbos infrastruktūros objektų peržiūrą ir ne vėliau kaip per dvidešimt darbo dienų nuo šiame punkte nurodyto dvejų metų termino pabaigos kreipiasi į Atsakingą valdytoją, prašydama jo atlikti visų jo valdomų infrastruktūros objektų svarbos vertinimą ir užpildyti Klausimyną. Atsakinga institucija nustato ypatingos svarbos infrastruktūros objektus, ypatingos svarbos informacinę infrastruktūrą, ją įvertina ir teikia tvirtinti Metodikos II, III ir IV skyriuose nurodyta tvarka.	
7. 23 straipsnyje nurodytos peržiūros tikslais ir ne vėliau kaip 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	**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 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; <...>	Visiškas

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.	**2. YSII identifikavimo 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, Metodikos 1 priede nurodytuose sektoriuose nustatytos informacinės infrastruktūros valdytojų skaičių ir vartotojų skaičiaus nustatymo kriterijus, pasirinktus ypatingos svarbos informacinei infrastruktūrai nustatyti.	
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; 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.	**YSII identifikavimo 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 veikiančius infrastruktūros objektus, turinčius reikšmės teikiant ypatingos svarbos paslaugas, ir 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 infrastruktūros objektų svarbos vertinimą ir užpildyti Metodikos 2 priede pateiktą klausimyną (toliau – Klausimynas). 6.2. Atsakingas valdytojas ne vėliau kaip per dvidešimt darbo dienų nuo 6.1 papunktyje nurodyto prašymo gavimo dienos užpildo Klausimyną ir teikia jį raštu Atsakingai institucijai. Jeigu Atsakinga institucija ir Atsakingas valdytojas yra tas pats subjektas, Klausimyną pildo Atsakinga institucija. 6.3. Atsakinga institucija įvertina Atsakingo valdytojo pateiktą	Visiškas

	Klausimyną ir prireikus teikia Atsakingam valdytojui pastabas ir pasiūlymus, kartu nurodydama terminą 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. 6.4. Infrastruktūros objektų, kurių suminis svarbos balas, atsižvelgiant į Atsakingos institucijos vertinimą, atliktą vadovaujantis Metodikos 15 punkte nurodyta metodine medžiaga, ir Klausimyno kriterijus, sudaro šešiolika ar daugiau balų, teikiamų paslaugų sutrikdymo neigiamas poveikis yra didelis, todėl šie infrastruktūros objektai Atsakingos institucijos 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 išdėstyta tvarka nustačiusi ypatingos svarbos infrastruktūros objektus, ne vėliau kaip per dvidešimt darbo dienų nuo užpildyto Klausimyno gavimo dienos 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 dvidešimt darbo dienų nuo 8.1 papunktyje nurodyto prašymo gavimo dienos užpildo Lentelę ir Sąrašą ir pateikia juos raštu Atsakingai	

	institucijai. Jeigu Atsakinga institucija ir Atsakingas valdytojas yra tas pats subjektas, Lentelę ir Sąrašą pildo Atsakinga institucija. 8.3. Atsakinga institucija įvertina Atsakingo valdytojo pateiktą Lentelę ir Sąrašą ir prireikus teikia Atsakingam valdytojui pastabas ir pasiūlymus, kartu nurodydama terminą Lentelei ir Sąrašui patikslinti. Atsakinga institucija turi teisę prašyti Atsakingo valdytojo papildomos informacijos, kuri reikalinga Lentelei ir Sąrašui patikslinti. 8.4. Jeigu užpildytame Klausimyne, Lentelėje, Sąraše nurodyta, kad ypatingos svarbos paslauga teikiama dviejose ar daugiau Europos Sąjungos valstybių narių, Atsakinga institucija, prieš priimdama sprendimą dėl ypatingos svarbos informacinės infrastruktūros nustatymo, siekiant nustatyti, kurioje Europos Sąjungos valstybėje turėtų būti taikomas ypatingos svarbos paslaugos reguliavimas, 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. Krašto apsaugos ministerija kartu su Nacionaliniu kibernetinio saugumo centru koordinuoja pasikeitimą duomenimis ir informacija, perduodama Europos Sąjungos valstybių narių institucijų, kurių veiklos sritys apima užpildytame Klausimyne, Lentelėje, Sąraše nurodytus ypatingos svarbos sektorius, subsektorius ir juose teikiamas ypatingos svarbos paslaugas. 8.5. Informacinė infrastruktūra, kuri atlikus Atsakingos institucijos vertinimą atitinka visus Lentelėje nurodytus kriterijus, Atsakingos institucijos nustatoma kaip ypatingos svarbos informacinė infrastruktūra. **YSII identifikavimo metodikos projekto 2 ir 3 priedai.**	
6. Kompetentingos institucijos ir bendrasis informacinis centras	**1. Kibernetinio saugumo įstatymas**	Visiškas

prireikus ir pagal nacionalinę teisę konsultuojasi ir bendradarbiauja su atitinkamomis nacionalinėmis teisėsaugos institucijomis ir nacionalinėmis duomenų apsaugos institucijomis.	<...> **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 keitimasis informacija tiriant kibernetinius incidentus** <...> 44. KIVT institucija, gavusi informaciją apie kibernetinį incidentą, nedelsdama, bet ne vėliau kaip per dvidešimt keturias valandas nuo informacijos apie kibernetinį incidentą gavimo informuoja kitas KIVT institucijas: 44.1. Nacionalinį kibernetinio saugumo centrą – nustačiusi, kad kibernetinis incidentas taip pat gali paveikti kibernetinio	

	saugumo subjektų ryšių ir informacines sistemas; 44.2. Lietuvos policiją – nustačiusi, kad kibernetinis incidentas gali turėti nusikalstamos veikos požymių; 44.3. Valstybinę duomenų apsaugos inspekciją – nustačiusi, kad kibernetinis incidentas gali būti susijęs su asmens duomenų saugumo pažeidimais. 45. KIVT institucija, pagal kompetenciją tirianti kibernetinį incidentą, nustačiusi papildomos informacijos apie kibernetinį incidentą poreikį, turi teisę kreiptis į kitas KIVT institucijas ar kibernetinius subjektus, kurie papildomą informaciją turi pateikti per KIVT institucijos, pagal kompetenciją tiriančios kibernetinį incidentą, prašyme nurodytą terminą. 46. 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 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**	Visiškas

	keitimasis informacija tiriant kibernetinius incidentus <...> 50. Nacionalinis kibernetinio saugumo centras, koordinuodamas tarptautinio ir tarpinstitucinio bendradarbiavimo veiksmus: <...> 50.2. informuoja Europos Komisiją apie kibernetinių incidentų valdymo proceso mastą (nurodydamas įvykusių kibernetinių incidentų grupes, poveikį, skaičių, kibernetinius incidentus, galimai turėjusius poveikį kitoms Europos Sąjungos valstybėms, ir kitą aktualią informaciją) 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** **III skyrius. Informavimas apie kibernetinius incidentus** <...> 13. Kibernetinio saugumo subjektai Nacionalinį kibernetinio saugumo centrą informuoja apie:	Visiškas

	13.1. didelio poveikio kibernetinius incidentus – nedelsiant, bet ne vėliau kaip per vieną valandą nuo jų nustatymo; 13.2. vidutinio poveikio kibernetinius incidentus – ne vėliau kaip per keturias valandas nuo jų nustatymo; 13.3. nereikšmingo poveikio kibernetinius incidentus – periodiškai kiekvieno kalendorinio mėnesio pirmą darbo dieną teikiant apibendrintą 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** <...> 50. Nacionalinis kibernetinio saugumo centras, koordinuodamas tarptautinio ir tarpinstitucinio bendradarbiavimo veiksmus: <...> 50.2. informuoja Europos Komisiją apie kibernetinių incidentų valdymo proceso mastą (nurodydamas įvykusių kibernetinių incidentų grupes, poveikį, skaičių, kibernetinius incidentus, galimai turėjusius poveikį kitoms Europos Sąjungos valstybėms, ir kitą aktualią informaciją) 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,	Visiškas

	taip pat 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** <...> 5. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai: 5.1. ne rečiau kaip kartą per metus arba po esminių organizacinių ar sisteminių pokyčių Aprašo II skyriuje nustatyta tvarka organizuoja ir atlieka rizikos vertinimą. Šį rizikos vertinimą subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ir ypatingos svarbos informacinės infrastruktūros valdytojai turi teisę atlikti kartu su valstybės informacinių išteklių rizikos ar ypatingos svarbos informacinės infrastruktūros	Visiškas

	rizikos 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 ar padalinio kontaktinę informaciją; <...>	Visiškas

	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** <...> 5. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės	

	infrastruktūros valdytojai: <...> 5.2. atsižvelgdami į atlikto rizikos vertinimo rezultatus, taip pat jeigu nustatoma kibernetinių incidentų valdymo ir šalinimo, organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, tobulina valstybės informacinių išteklių 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 veiksmingumo išbandymo rezultatai išdėstomi šių planų veiksmingumo išbandymo ir pastebėtų trūkumų ataskaitose, kurių kopijos ne vėliau kaip per penkias darbo dienas nuo šių 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** <...> 13. Kibernetinio saugumo subjektai Nacionalinį kibernetinio saugumo centrą informuoja apie:	Visiškas

	13.1. 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.	<...> 50. Nacionalinis kibernetinio saugumo centras, koordinuodamas tarptautinio ir tarpinstitucinio bendradarbiavimo veiksmus: <...> 50.3. 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; <...> 51. Koordinuodamas tarptautinio ir tarpinstitucinio bendradarbiavimo veiksmus, Nacionalinis kibernetinio saugumo centras kibernetinio saugumo subjektų pateikta informacija, įskaitant konfidencialią informaciją ir komercines paslaptis, turi teisę keistis tik tiek, kiek tai yra būtina tarptautiniam ir tarpinstituciniam bendradarbiavimui koordinuoti, 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. Reikalavimai elektroninės informacijos prieglobos paslaugų teikėjams ir skaitmeninių paslaugų**	Visiškas

	teikėjams <...> 19. Elektroninės informacijos prieglobos paslaugų teikėjai ir skaitmeninių paslaugų teikėjai: 19.1. ne rečiau kaip kartą per dvejus metus arba po esminių organizacinių ar sisteminių pokyčių Aprašo II skyriuje nustatyta tvarka organizuoja ir atlieka rizikos vertinimą. Šį rizikos vertinimą elektroninės informacijos prieglobos paslaugų teikėjai ir skaitmeninių paslaugų teikėjai turi teisę atlikti kartu su veiklos rizikos ir (arba) informacinių technologijų saugos atitikties vertinimu; <...> 19.4. tvirtina ir po esminių organizacinių ar sisteminių pokyčių atnaujina savo paslaugų kibernetinio saugumo valdymo taisykles, o Nacionalinio kibernetinio saugumo centro reikalavimu 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. Reikalavimai elektroninės informacijos prieglobos paslaugų teikėjams ir skaitmeninių paslaugų teikėjams** <...> 19. Elektroninės informacijos prieglobos paslaugų teikėjai ir skaitmeninių paslaugų teikėjai: 19.1. ne rečiau kaip kartą per dvejus metus arba po esminių organizacinių ar sisteminių pokyčių Aprašo II skyriuje nustatyta tvarka organizuoja ir atlieka rizikos vertinimą. Šį rizikos vertinimą elektroninės informacijos prieglobos paslaugų teikėjai ir skaitmeninių paslaugų teikėjai turi teisę atlikti kartu su veiklos rizikos 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, užtikrinančias jų elektroninės informacijos prieglobos ar skaitmeninėms paslaugoms teikti naudojamų sistemų ir įrangos kibernetinį saugumą; 19.4. tvirtina ir po esminių organizacinių ar sisteminių pokyčių	Visiškas

	atnaujina savo paslaugų kibernetinio saugumo valdymo taisykles, o Nacionalinio kibernetinio saugumo centro reikalavimu 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 penkias 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 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. **2. Kibernetinių incidentų valdymo plano projektas** **III skyrius. Informavimas apie kibernetinius incidentus** <...> 13. Kibernetinio saugumo subjektai Nacionalinį kibernetinio saugumo centrą informuoja apie:	Visiškas

	13.1. didelio poveikio kibernetinius incidentus – nedelsiant, bet ne vėliau kaip per vieną 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 vietų skaičius ≥ 1000, arba 25 % • Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje • Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Visiškas

	• 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** <...> 16. Ypatingos svarbos informacinės infrastruktūros valdytojai, kurių paslaugų teikimas priklauso nuo skaitmeninių paslaugų teikėjų teikiamų paslaugų, nustatę neigiamą poveikį jų valdomos ypatingos svarbos informacinės infrastruktūros veiklai, kurį lėmė skaitmeninių paslaugų teikėjų ryšių ir informacinėse sistemose įvykę sutrikimai, apie šį neigiamą poveikį nedelsdami, bet ne vėliau kaip per vieną valandą nuo neigiamo poveikio nustatymo informuoja Nacionalinį kibernetinio saugumo centrą ir skaitmeninių paslaugų teikėjus, kurių ryšių ir informacinėse sistemose įvyko nurodyti 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 incidentus, kurie daro didelį poveikį jų teikiamų paslaugų tęstinumui. 2. Tvarkydamos tokius pranešimus valstybės narės veikia pagal	**1. Kibernetinio saugumo įstatymas** **16 straipsnis. Savanoriškas pranešimas apie kibernetinius incidentus** 1. Asmenys, kuriems šiame įstatyme nėra nustatytos pareigos pranešti apie kibernetinius incidentus jų valdomose ryšių ir informacinėse sistemose, turi teisę savanoriškai pranešti Nacionaliniam kibernetinio saugumo centrui apie kibernetinius	Visiškas

<table>
<tr>
<td>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>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
<...>
17. 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 rowspan="3">7. Skaitmeninė infrastruktūra</td><td rowspan="3"></td><td>— IXP</td></tr>
<tr><td>— DNS paslaugų teikėjai</td></tr>
<tr><td>— ALD vardų registrai</td></tr>
</table></td>
<td>YSII identifikavimo metodikos projektas
Ypatingos svarbos informacinės infrastruktūros identifikavimo 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) paslauga</td>
<td></td>
</tr>
</table>

Krašto apsaugos viceministras
Edvinas Kerza

Lietuvos Respublikos
vidaus reikalų ministras
Eimutis Misiūnas