

**DIREKTYVOS (ES) 2018/1972 IR LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMO ĮGYVENDINIMO“  
2018 M. RUGPJŪČIO 13 D. NUTARIMO NR. 818 „DĖL LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMO ĮGYVENDINIMO“  
PAKEITIMO“ PROJEKTO ATITIKTIES LENTELE**

<p><b>2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas (nauja redakcija)</b></p>	<p>1. Lietuvos Respublikos Vyriausybės nutarimo „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimo“ projektas (toliau – Nutarimo Nr. 818 pakeitimo projektas)</p> <p>2. Lietuvos Respublikos elektroninių ryšių įstatymo Nr. IX-2135 pakeitimo įstatymo projektas (toliau – ERĮ pakeitimo projektas)</p> <p>3. Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas Nr. XIII-1299 (toliau – Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas Nr. XIII-1299)</p> <p>4. Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimas Nr. 1209 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo“ (toliau – Nutarimas Nr. 1209)</p> <p>5. Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. balandžio 25 d. įsakymas Nr. 1V-394 „Dėl Viešųjų ryšių tinklų vientisumo užtikrinimo taisyklių patvirtinimo“ (toliau – Įsakymas Nr. 1V-394)</p>	<p><b>Direktyvos perkėlimo ir įgyvendinimo lygis</b></p>
<p style="text-align: center;"><b>I DALIS SISTEMA (SEKTORIAUS ORGANIZAVIMO BENDROSIOS TAISYKLĖS)</b></p>		
<p style="text-align: center;"><b>V ANTRAŠTINĖ DALIS SAUGUMAS</b></p>		
<p style="text-align: center;"><i>40 straipsnis</i> <b>Tinklų ir paslaugų saugumas</b></p>		
<p>1. Valstybės narės užtikrina, kad viešųjų elektroninių ryšių tinklų ar</p>	<p><b>Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas</b></p>	<p>Visiškas</p>

<p>viešai prieinamų elektroninių ryšių paslaugų teikėjai imtųsi tinkamų ir proporcingų techninių ir organizacinių priemonių teikiamų tinklų ir paslaugų saugumui kylančios rizikos tinkamam valdymui užtikrinti. Atsižvelgiant į naujausius technikos laimėjimus, tomis priemonėmis užtikrinamas kilusią riziką atitinkantis saugumo lygis. Visų pirma turi būti imamasi priemonių, įskaitant, kai tikslinga, šifravimą, siekiant užkirsti kelią su saugumu susijusiems incidentams arba sumažinti jų poveikį naudotojams ir kitiems tinklams ir paslaugoms.</p>	<p><b>Nr. XIII-1299</b>  <b>Kibernetinio saugumo įstatymas</b>  <b>2 straipsnis. Pagrindinės šio įstatymo sąvokos</b>  <b>8. Kibernetinio saugumo subjektas</b> – subjektas, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas.</p> <p><b>11 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos</b>  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, taikomies 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.</p> <p><b>Nutarimas Nr. 1209</b>  <b>Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas</b>  18. Viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai:  18.1. ne rečiau kaip kartą per dvejus metus arba po esminių organizacinių ar sisteminių pokyčių Aprašo II skyriuje nustatyta tvarka organizuoja ir atlieka rizikos vertinimą. Rizikos vertinimą viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai turi teisę atlikti kartu su veiklos rizikos ir (arba) informacinių technologijų saugos atitikties vertinimu;  18.2. įgyvendina organizacines ir technines priemones, užtikrinančias, kad suklastotų interneto protokolo (IP) adresų srautas būtų blokuojamas</p>	
--	---	--

	<p>jų teikiamuose viešuosiuose ryšių tinkluose;</p> <p>18.3. įgyvendina organizacines ir technines priemones, užtikrinančias, kad elektroninių paslaugų trikdymo atakos srautas būtų blokuojamas jų teikiamuose viešuosiuose ryšių tinkluose;</p> <p>18.4. įgyvendina organizacines ir technines priemones, užtikrinančias jų viešųjų ryšių tinklą ir (arba) viešųjų elektroninių ryšių paslaugoms teikti naudojamų sistemų ir įrangos kibernetinį saugumą;</p> <p>18.5. tvirtina ir po esminių organizacinių ar sisteminių pokyčių atnauja savo viešųjų ryšių tinklą ir (arba) viešųjų elektroninių paslaugų kibernetinio saugumo valdymo taisykles, o Nacionalinio kibernetinio saugumo centro reikalavimu, jas pateikia Nacionaliniam kibernetinio saugumo centrui. Viešųjų ryšių tinklą ir (arba) viešųjų elektroninių paslaugų kibernetinio saugumo valdymo taisyklėse nurodoma:</p> <p>18.5.1. kibernetiniams incidentams valdyti reikalingų priemonių aprašymai;</p> <p>18.5.2. viešųjų ryšių tinklą ir (arba) viešųjų elektroninių ryšių paslaugų nepertraukiamo teikimo užtikrinimo planas ir jo taikymo sąlygos bei maksimalus leistinas paslaugos neveikimo laikas;</p> <p>18.5.3. už kibernetinių incidentų valdymą atsakingų asmenų funkcijos ir atsakomybė;</p> <p>18.5.4. viešųjų ryšių tinklą ir (arba) viešųjų elektroninių ryšių paslaugoms teikti naudojamų sistemų ir įrangos stebėsenos, patikrinimo, testavimo bei auditavimo tvarka ir sąlygos;</p> <p>18.5.5. atitiktis Lietuvos ir tarptautiniams standartams, apibūdinantiems kibernetinį saugumą ar saugų elektroninės informacijos tvarkymą;</p> <p>18.6. neatlygintinai informuoja viešųjų elektroninių ryšių paslaugų gavėjus apie priemones, kuriomis viešųjų elektroninių ryšių paslaugų gavėjai gali pasinaudoti kibernetinių incidentų grėsmei, susijusiai su viešųjų elektroninių ryšių paslaugų gavėjų galiniais įrenginiais, pašalinti, ir nurodo tikėtinas tokių priemonių panaudojimo išlaidas;</p> <p>18.7. ne vėliau kaip prieš penkias darbo dienas informuoja viešųjų elektroninių ryšių paslaugų gavėjus ir Nacionalinį kibernetinio saugumo centrą apie numatomus planinius darbus, kuriuos atliekant yra tikimybė sutrikdyti viešųjų ryšių tinklą ir (arba) viešųjų elektroninių ryšių</p>	
--	--	--

	<p>paslaugų kibernetinį saugumą;  18.8. viešai skelbia rekomendacijas viešųjų elektroninių ryšių paslaugų gavėjams apie priemones kibernetiniam saugumui užtikrinti naudojantis viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų paslaugomis.</p> <p><b>ERĮ pakeitimo projektas</b>  <b>Lietuvos Respublikos elektroninių ryšių įstatymas</b></p> <p><b>51 straipsnis. Viešųjų elektroninių ryšių tinklų vientisumas</b>  <b>1. Viešųjų elektroninių ryšių tinklų teikėjai privalo įgyvendinti tinkamas technines ir organizacines priemones savo teikiamų viešųjų elektroninių ryšių tinklų vientisumui užtikrinti, taip užtikrindami šiais tinklais teikiamų viešųjų elektroninių ryšių paslaugų nepertraukiamą teikimą.</b>  <b>2. Ryšių reguliavimo tarnyba gali nustatyti techninius ir organizacinius reikalavimus viešųjų elektroninių ryšių tinklų vientisumui užtikrinti.</b>  <b>3. Ryšių reguliavimo tarnyba, siekdama užtikrinti viešųjų elektroninių ryšių tinklų vientisumą, turi teisę duoti privalomus nurodymus ir nustatyti nurodymų įvykdymo terminą viešųjų elektroninių ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjams. Ryšių reguliavimo tarnybos nurodymai turi būti motyvuoti, pagrįsti ir proporcingi tikslui pasiekti.</b></p> <p><b>Įsakymas Nr. 1V-394</b>  <b>Viešųjų ryšių tinklų vientisumo užtikrinimo taisyklės</b>  3. Viešųjų ryšių tinklų teikėjai privalo:  3.1. įgyvendinti tinkamas technines ir organizacines priemones savo teikiamų viešųjų ryšių tinklų vientisumui užtikrinti, kad šiais tinklais būtų nepertraukiamai teikiamos viešosios elektroninių ryšių paslaugos;</p>	
<p>Europos Sąjungos tinklų ir informacijos apsaugos agentūra (toliau – ENISA) pagal Europos Parlamento ir Tarybos reglamentą (ES)</p>	<p><i>Šios pastraipos perkelti ir įgyvendinti nereikia, nes ji skirta Europos Sąjungos tinklų ir informacijos apsaugos agentūrai.</i></p>	

<p>Nr. 526/2013 (1) palengvina valstybių narių veiksmų koordinavimą siekiant išvengti skirtingų nacionalinių reikalavimų, kurie gali sukelti saugumo riziką ir kliūčių vidaus rinkai, taikymo.</p>		
<p>2. Valstybės narės užtikrina, kad viešųjų elektroninių ryšių tinklų ar viešai prieinamų elektroninių ryšių paslaugų teikėjai nedelsiant praneštų kompetentingai institucijai apie saugumo incidentą, kuris turėjo didelės įtakos tinklų veikimui arba paslaugų teikimui.</p>	<p><b>Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas Nr. XIII-1299</b>  <b>Kibernetinio saugumo įstatymas</b>  <b>2 straipsnis. Pagrindinės šio įstatymo sąvokos</b>  <b>8. Kibernetinio saugumo subjektas</b> – subjektas, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas.</p> <p><b>11 straipsnis. Bendrosios kibernetinio saugumo subjektų pareigos</b>  1. Kibernetinio saugumo subjektai:  3) Nacionaliniame kibernetinių incidentų valdymo plane nustatytais 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.</p> <p><b>Nutarimas Nr. 1209</b>  <b>Nacionalinis kibernetinių incidentų valdymo planas</b>  13. Kibernetinio saugumo subjektai Nacionalinį kibernetinio saugumo centrą informuoja apie:  13.1. didelio poveikio kibernetinius incidentus – nedelsiant, bet ne vėliau kaip per vieną valandą nuo jų nustatymo.</p> <p><b>ERI pakeitimo projektas</b>  <b>Lietuvos Respublikos elektroninių ryšių įstatymas</b></p> <p><b>51 straipsnis. Viešųjų elektroninių ryšių tinklų vientisumas</b>  <b>4. Įvykus vientisumo pažeidimui, kuris gali turėti, turi ar turėjo didelę įtaką viešojo elektroninių ryšių tinklo veikimui arba viešųjų</b></p>	<p>Visiškas</p>

	<p>elektroninių ryšių paslaugų teikimui, viešųjų elektroninių ryšių tinklų teikėjas privalo nedelsdamas apie šį vientisumo pažeidimą informuoti Ryšių reguliavimo tarnybą jos nustatyta tvarka ir sąlygomis. Nustatant vientisumo pažeidimo mastą, atsižvelgiama į paslaugų gavėjų, kuriuos paveikė vientisumo pažeidimas, skaičių, vientisumo pažeidimo trukmę, teritoriją, kurioje vientisumo pažeidimas daro poveikį, poveikio viešojo elektroninių ryšių tinklo veikimui ar viešųjų elektroninių ryšių paslaugų teikimui mastą, poveikio ekonominei ir visuomeninei veiklai mastą. Ryšių reguliavimo tarnyba nustato konkrečius vientisumo pažeidimo masto vertinimo kriterijus. Prireikus apie įvykusį vientisumo pažeidimą Ryšių reguliavimo tarnyba praneša kitų Europos Sąjungos valstybių narių nacionalinėms reguliavimo institucijoms, Europos tinklų ir informacijos apsaugos agentūrai ir visuomenei.</p> <p><b>Įsakymas Nr. 1V-394</b>  <b>Viešųjų ryšių tinklų vientisumo užtikrinimo taisyklės</b>  3. Viešųjų ryšių tinklų teikėjai privalo:  3.4. nedelsdami, bet ne vėliau kaip per dvi valandas po vientisumo pažeidimo nustatymo, informuoti Tarnybą apie vientisumo pažeidimus, kurie pagal Taisyklių 1 priedo 1 lentelėje nurodytus kriterijus gali turėti, turi ar turėjo didelę įtaką jų teikiamų viešųjų ryšių tinklų veikimui ir (arba) šiais tinklais teikiamų viešųjų elektroninių ryšių paslaugų teikimui; apie šiame papunktyje nurodytus vientisumo pažeidimus Tarnyba turi būti informuota vienu iš šių telefono ryšio numerių – +370 618 13 476, +370 673 99 568 arba +370 686 58 193, taip pat elektroninio pašto adresu vientisumas@rrt.lt pateikiant užpildytą Taisyklių 2 priede pateiktos formos pranešimą.</p>	
<p>Siekiant nustatyti su saugumu susijusio incidento poveikio mastą, atsižvelgiama, kai žinoma, visų pirma į šiuos parametrus:</p> <ul style="list-style-type: none"> <li>a) naudotojų, kuriuos paveikė saugumo incidentas, skaičių;</li> <li>b) saugumo incidento trukmę;</li> <li>c) geografinę teritoriją, kurioje saugumo incidentas daro poveikį;</li> <li>d) poveikio tinklo veikimui arba paslaugos teikimo mastą;</li> </ul>	<p><b>Nutarimas Nr. 1209</b>  <b>Nacionalinis kibernetinių incidentų valdymo planas</b>  9. Kibernetiniai incidentai skirstomi į keturias kategorijas:  9.1. pavojingi kibernetiniai incidentai;  9.2. didelio poveikio kibernetiniai incidentai;  9.3. vidutinio poveikio kibernetiniai incidentai;</p>	Visiškas

e) poveikio ekonominei ir visuomeninei veiklai mastą.

9.4. nereikšmingo poveikio kibernetiniai incidentai.  
10. Kriterijai, kuriais vadovaujantis kibernetiniai incidentai priskiriami Plano 9 punkte nustatytoms kategorijoms, nustatyti Plano priede.

#### Priedas

### KRITERIJŲ, KURIAIS VADOVAUJANTIS KIBERNETINIAI INCIDENTAI PRISKIRIAMSI KIBERNETINIŲ INCIDENTŲ KATEGORIJOMS, SĄRAŠAS

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis	Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)	Vidutinis (V) (du ar daugiau kriterijų)	Didelis (D) (du ar daugiau kriterijų)	Pavojingas (P) (bent vienas iš kriterijų)
				RS trūkumai < 1 val. Poveikio paslaugos gavėjų ar kompiuterizacijų Pavojingumas tiksliai, bet trūkumai Nustatomi < 250 000 Eur	RS trūkumai ≥ 1 val., bet < 2 val. Poveikio paslaugos gavėjų ar kompiuterizacijų Pavojingumas tiksliai, bet trūkumai Paveiktas informacijos ar RIS konfidencialumas Nustatomi ≥ 250 000, bet < 500 000 Eur	RS trūkumai ≥ 2 val. Poveikio paslaugos gavėjų ar kompiuterizacijų Pavojingumas tiksliai visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje Paveiktas informacijos ar RIS konfidencialumas Nustatomi ≥ 500 000 Eur	RS trūkumai ≥ 24 val., ir (ar) viešumas Poveikio paslaugos gavėjų ar kompiuterizacijų Sunkūs ir (ar) pavojingi paslaugų veikimas visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) pramonės, energetikos, sveikatos, mokymosi (gali būti)
			1.1. Nepažeidžiamais laikyti ir (ar)				

#### ERĮ pakeitimo projektas Lietuvos Respublikos elektroninių ryšių įstatymas

#### 51 straipsnis. Viešųjų elektroninių ryšių tinklų vientisumas

4. Įvykus vientisumo pažeidimui, kuris gali turėti, turi ar turėjo didelę įtaką viešojo elektroninių ryšių tinklo veikimui arba viešųjų elektroninių ryšių paslaugų teikimui, viešųjų elektroninių ryšių tinklų teikėjas privalo nedelsdamas apie šį vientisumo pažeidimą informuoti Ryšių reguliavimo tarnybą jos nustatyta tvarka ir sąlygomis. Nustatant vientisumo pažeidimo mastą, atsižvelgiama į paslaugų gavėjų, kuriuos paveikė vientisumo pažeidimas, skaičių, vientisumo pažeidimo trukmę, teritoriją, kurioje vientisumo pažeidimas daro poveikį, poveikio viešojo elektroninių ryšių tinklo veikimui ar viešųjų elektroninių ryšių paslaugų teikimui mastą, poveikio ekonominei ir visuomeninei veiklai mastą. Ryšių reguliavimo tarnyba nustato konkrečius vientisumo pažeidimo masto vertinimo kriterijus. Prireikus apie įvykusį vientisumo pažeidimą Ryšių reguliavimo tarnyba praneša kitų Europos

**Sąjungos valstybių narių nacionalinėms reguliavimo institucijoms, Europos tinklų ir informacijos apsaugos agentūrai ir visuomenei.**

**Įsakymas Nr. 1V-394**

**Viešųjų ryšių tinklų vientisumo užtikrinimo taisyklės**

3. Viešųjų ryšių tinklų teikėjai privalo:

3.4. nedelsdami, bet ne vėliau kaip per dvi valandas po vientisumo pažeidimo nustatymo, informuoti Tarnybą apie vientisumo pažeidimus, kurie pagal Taisyklių 1 priedo 1 lentelėje nurodytus kriterijus gali turėti, turi ar turėjo didelę įtaką jų teikiamų viešųjų ryšių tinklų veikimui ir (arba) šiais tinklais teikiamų viešųjų elektroninių ryšių paslaugų teikimui; apie šiame papunktyje nurodytus vientisumo pažeidimus Tarnyba turi būti informuota vienu iš šių telefono ryšio numerių – +370 618 13 476, +370 673 99 568 arba +370 686 58 193, taip pat elektroninio pašto adresu vientisumas@rrt.lt pateikiant užpildytą Taisyklių 2 priede pateiktos formos pranešimą.

Viešųjų ryšių tinklų vientisumo užtikrinimo taisyklių

1 priedas

**VIENTISUMO PAŽEIDIMŲ, APIE KURIUOS TURI BŪTI PRANEŠTA LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBAI, NUSTATYMO KRITERIJAI**

1 lentelė. Vientisumo pažeidimai, apie kuriuos turi būti pranešama nedelsiant, bet ne vėliau kaip per dvi valandas po vientisumo pažeidimo nustatymo

Kriterijus	Kriterijaus reikšmė	Paslaugų teikimo sutrikimo trukmė
Interneto prieigos paslaugų teikimo nutraukimas	Daugiau kaip 1/3 savivaldybės paslaugų gavėjų arba daugiau kaip 25 000 paslaugų gavėjų	1 valanda ir ilgiau



	<b>Viešųjų fiksuotojo telefono ryšio paslaugų teikimo nutraukimas</b>	Daugiau kaip 1/3 savivaldybės paslaugų gavėjų arba daugiau kaip 25 000 paslaugų gavėjų	1 valanda ir ilgiau	
	<b>Viešųjų judriojo telefono ryšio paslaugų teikimo nutraukimas</b>	Daugiau kaip 1/3 savivaldybės paslaugų gavėjų arba daugiau kaip 25 000 paslaugų gavėjų	1 valanda ir ilgiau	
	<b>Lietuvos nacionalinio radijo ir televizijos transliavimo nutraukimas</b>	Daugiau kaip 1/3 savivaldybės paslaugų gavėjų arba daugiau kaip 25 000 paslaugų gavėjų	1 valanda ir ilgiau	
<p>Prireikus atitinkama kompetentinga institucija informuoja kitų valstybių narių kompetentingas institucijas ir ENISA. Atitinkama kompetentinga institucija gali informuoti visuomenę arba reikalauti, kad tai padarytų paslaugų teikėjai, jei ji nustato, kad saugumo incidento atskleidimas atitinka visuomenės interesus.</p> <p>Kartą per metus atitinkama kompetentinga institucija pateikia Komisijai ir ENISA apibendrintą pagal šią dalį gautų pranešimų ir įvykdytų veiksmų ataskaitą.</p>	<p><b>Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas Nr. XIII-1299</b></p> <p><b>Kibernetinio saugumo įstatymas</b></p> <p><b>8 straipsnis. Nacionalinis kibernetinio saugumo centras</b></p> <p>2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:</p> <p>13) kai būtina informuoti visuomenę siekiant išvengti kibernetinio incidento arba valdyti vykstantį kibernetinį incidentą, pasikonsultavęs su kibernetinio saugumo subjektu, pranešusiu apie kibernetinį incidentą, informuoja visuomenę apie pavienius kibernetinius incidentus arba reikalauja, kad tai padarytų kibernetinio saugumo subjektas.</p> <p><b>Nutarimo Nr. 818 pakeitimo projektas</b></p> <p><b>1.2. Pakeisti nurodytu nutarimu patvirtintą Nacionalinio kibernetinių incidentų valdymo planą ir 50.2 papunktį išdėstyti taip:</b></p> <p><b>„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</b></p>			Visiškas

	<p><b>bendradarbiavimo grupei, Europos Komisijai ir Europos tinklų ir informacijos apsaugos agentūrai (ENISA) 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;“.</b></p> <p><b>Nutarimas Nr. 1209</b>  <b>Nacionalinis kibernetinių incidentų valdymo planas</b>  50. Nacionalinis kibernetinio saugumo centras, koordinuodamas tarptautinio ir tarpinstitucinio bendradarbiavimo veiksmus:  50.1. užtikrina tarpvalstybinį Lietuvos Respublikos ir kitų Europos Sąjungos valstybių narių institucijų bendradarbiavimą ir bendradarbiavimą su šių valstybių bendradarbiavimo grupėmis, reagavimo į kompiuterinius saugumo incidentus tarnybomis (toliau – CSIRT) ir kitomis institucijomis, kad būtų galima vykdyti efektyvią kibernetinio saugumo priežiūrą ir operatyviai keistis informacija tarp suinteresuotų asmenų;  &lt;...&gt;  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;</p> <p><b>ERI pakeitimo projektas</b>  <b>Lietuvos Respublikos elektroninių ryšių įstatymas</b></p> <p><b>51 straipsnis. Viešųjų elektroninių ryšių tinklų vientisumas</b>  4. Įvykus vientisumo pažeidimui, kuris gali turėti, turi ar turėjo didelę įtaką viešojo elektroninių ryšių tinklo veikimui arba viešųjų elektroninių ryšių paslaugų teikimui, viešųjų elektroninių ryšių tinklų teikėjas privalo nedelsdamas apie šį vientisumo pažeidimą informuoti Ryšių reguliavimo tarnybą jos nustatyta tvarka ir sąlygomis. Nustatant vientisumo pažeidimo mastą, atsižvelgiama į paslaugų gavėjų, kuriuos paveikė vientisumo pažeidimas, skaičių,</p>	
--	---	--

	<p>vientisumo pažeidimo trukmę, teritoriją, kurioje vientisumo pažeidimas daro poveikį, poveikio viešojo elektroninių ryšių tinklo veikimui ar viešųjų elektroninių ryšių paslaugų teikimui mastą, poveikio ekonominei ir visuomeninei veiklai mastą. Ryšių reguliavimo tarnyba nustato konkrečius vientisumo pažeidimo masto vertinimo kriterijus. Prireikus apie įvykusį vientisumo pažeidimą Ryšių reguliavimo tarnyba praneša kitų Europos Sąjungos valstybių narių nacionalinėms reguliavimo institucijoms, Europos tinklų ir informacijos apsaugos agentūrai ir visuomenei.</p> <p>5. Ryšių reguliavimo tarnyba kaupia informaciją apie pagal šio straipsnio 4 dalį pateiktus viešųjų elektroninių ryšių tinklų teikėjų pranešimus ir įvykdytus veiksmus ir kiekvienais metais pateikia apibendrintą informaciją Europos Komisijai ir Europos tinklų ir informacijos apsaugos agentūrai.</p>	
<p>3. Valstybės narės užtikrina, kad esant konkrečiai ir didelei viešųjų elektroninių ryšių tinklų ar viešai prieinamų elektroninių ryšių paslaugų saugumo incidento rizikai tokių tinklų ar paslaugų teikėjai informuotų savo naudotojus, kuriems tokia grėsmė gali turėti įtakos, apie visas galimas apsaugos ar taisomąsias priemones, kurių gali imtis naudotojai. Kai tikslinga, paslaugų teikėjai apie pačią grėsmę taip pat informuoja savo naudotojus.</p>	<p><b>Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas Nr. XIII-1299</b></p> <p><b>Kibernetinio saugumo įstatymas</b></p> <p><b>2 straipsnis. Pagrindinės šio įstatymo sąvokos</b></p> <p>8. <b>Kibernetinio saugumo subjektas</b> – subjektas, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas.</p> <p><b>8 straipsnis. Nacionalinis kibernetinio saugumo centras</b></p> <p>2. Nacionalinis kibernetinio saugumo centras, įgyvendindamas kibernetinio saugumo politiką:</p> <p>13) kai būtina informuoti visuomenę siekiant išvengti kibernetinio incidento arba valdyti vykstantį kibernetinį incidentą, pasikonsultavęs su kibernetinio saugumo subjektu, pranešusiu apie kibernetinį incidentą, informuoja visuomenę apie pavienius kibernetinius incidentus arba reikalauja, kad tai padarytų kibernetinio saugumo subjektas.</p>	Visiškas

	<p><b>12 straipsnis. Specialiosios kibernetinio saugumo subjektų pareigos</b></p> <p>3. Viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai viešai skelbia savo interneto svetainėse ar kitomis visuomenės informavimo priemonėmis paslaugų gavėjams rekomendacijas dėl priemonių kibernetiniam saugumui užtikrinti naudojantis viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų teikiamomis paslaugomis.</p> <p><b>Nutarimas Nr. 1209</b></p> <p><b>Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas</b></p> <p>18. Viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai:</p> <p>18.6. neatlygintinai informuoja viešųjų elektroninių ryšių paslaugų gavėjus apie priemones, kuriomis viešųjų elektroninių ryšių paslaugų gavėjai gali pasinaudoti kibernetinių incidentų grėsmei, susijusiai su viešųjų elektroninių ryšių paslaugų gavėjų galiniais įrenginiais, pašalinti, ir nurodo tikėtinas tokių priemonių panaudojimo išlaidas;</p> <p>18.7. ne vėliau kaip prieš penkias darbo dienas informuoja viešųjų elektroninių ryšių paslaugų gavėjus ir Nacionalinį kibernetinio saugumo centrą apie numatomus planinius darbus, kuriuos atliekant yra tikimybė sutrikdyti viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų kibernetinį saugumą;</p> <p>18.8. viešai skelbia rekomendacijas viešųjų elektroninių ryšių paslaugų gavėjams apie priemones kibernetiniam saugumui užtikrinti naudojantis viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų paslaugomis.</p> <p><b>Įsakymas Nr. 1V-394</b></p> <p><b>Viešųjų ryšių tinklų vientisumo užtikrinimo taisyklės</b></p> <p>3. Viešųjų ryšių tinklų teikėjai privalo:</p> <p>3.2. nedelsdami nemokamai informuoti viešųjų elektroninių ryšių paslaugų teikėjus, kurie teikia viešąsias elektroninių ryšių paslaugas naudodamiesi viešojo ryšių tinklo teikėjo viešuoju ryšių tinklu, ir viešųjų</p>	
--	--	--

	<p>elektroninių ryšių paslaugų gavėjus, kuriems viešojo ryšių tinklo teikėjas teikia viešąsias elektroninių ryšių paslaugas, apie dėl vientisumo pažeidimo kilusius viešųjų ryšių tinklų ir (arba) šiais tinklais teikiamų viešųjų elektroninių ryšių paslaugų teikimo sutrikimus;</p> <p>3.3. ne vėliau kaip prieš 5 darbo dienas informuoti viešųjų elektroninių ryšių paslaugų teikėjus, kurie teikia viešąsias elektroninių ryšių paslaugas naudodamiesi viešojo ryšių tinklo teikėjo viešuoju ryšių tinklu, viešųjų elektroninių ryšių paslaugų gavėjus, kuriems viešojo ryšių tinklo teikėjas teikia viešąsias elektroninių ryšių paslaugas, ir Tarnybą apie numatomus planinius darbus, kuriuos atliekant yra tikimybė sutrikdyti viešųjų ryšių tinklų vientisumą ir (arba) šiais tinklais teikiamų viešųjų elektroninių ryšių paslaugų nepertraukiamą teikimą.</p>	
4. Šis straipsnis nedaro poveikio Reglamentui (ES) 2016/679 ir Direktyvai 2002/58/EB.	<i>Šios dalies papildomai perkelti ir įgyvendinti nereikia, nes Direktyvos nacionalinės įgyvendinimo priemonės taikomos nedarant įtakos Reglamentui (ES) 2016/679 ir Direktyvą 2002/58/EB perkeliančioms nuostatoms.</i>	
<p>5. Komisija, kuo labiau atsižvelgdama į ENISA nuomonę, gali priimti įgyvendinimo aktus, kuriuose būtų išsamiai išdėstytos 1 dalyje nurodytos techninės ir organizacinės priemonės, taip pat aplinkybės, forma ir procedūros, taikomos pranešimo reikalavimams pagal 2 dalį. Jie kuo labiau grindžiami Europos ir tarptautiniais standartais ir netrukdo valstybėms narėms patvirtinti papildomus reikalavimus siekiant šio straipsnio 1 dalyje nustatytų tikslų.</p> <p>Įgyvendinimo aktai priimami laikantis 118 straipsnio 4 dalyje nurodytos nagrinėjimo procedūros.</p>	<i>Šios dalies perkelti ir įgyvendinti nereikia, nes ji skirta Europos Komisijai.</i>	