***Nutarimas netenka galios 2019-01-01:***
*Lietuvos Respublikos Vyriausybė, Nutarimas*
*Nr. 1209, 2018-12-05, paskelbta TAR 2018-12-10, i. k. 2018-20153*
*Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo*

***Suvestinė redakcija nuo 2018-03-06 iki 2018-12-31***

*Nutarimas paskelbtas: TAR 2016-01-28, i. k. 2016-01717*

***Nauja redakcija nuo 2018-03-06:***
*Nr. 198, 2018-02-28, paskelbta TAR 2018-03-05, i. k. 2018-03533*

**LIETUVOS RESPUBLIKOS VYRIAUSYBĖ**

# NUTARIMAS DĖL NACIONALINIO KIBERNETINIŲ INCIDENTŲ VALDYMO PLANO PATVIRTINIMO

2016 m. sausio 25 d. Nr. 87
Vilnius

Vadovaudamasi Lietuvos Respublikos kibernetinio saugumo įstatymo 5 straipsnio 4 punktu, Lietuvos Respublikos Vyriausybė n u t a r i a:

Patvirtinti Nacionalinį kibernetinių incidentų valdymo planą (pridedama).

Finansų ministras, pavaduojantis
Ministrą Pirmininką Rimantas Šadžius

Krašto apsaugos ministras Juozas Olekas

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2016 m. sausio 25 d. nutarimu Nr. 87
(Lietuvos Respublikos Vyriausybės
2018 m. vasario 28 d. nutarimo Nr. 198
redakcija)

# NACIONALINIS KIBERNETINIŲ INCIDENTŲ VALDYMO PLANAS

## I SKYRIUS
## BENDROSIOS NUOSTATOS

1. Nacionalinis kibernetinių incidentų valdymo planas (toliau – Planas) nustato kibernetinio saugumo politiką įgyvendinančių institucijų, kitų viešojo administravimo subjektų, valdančių valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų, elektroninės informacijos prieglobos paslaugų teikėjų (toliau – valdytojai) ir viešojo administravimo subjektų, tvarkančių valstybės informacinius išteklius (toliau – tvarkytojai), veiksmus, atliekamus siekiant suvaldyti kibernetinius incidentus, galinčius sutrikdyti ar sutrikdančius valstybės informacinių išteklių, ypatingos svarbos informacinės infrastruktūros ir (ar) kitų elektroninių ryšių tinklų ir paslaugų ir (ar) informacinių sistemų darbą ir taip sukelti grėsmę nacionaliniam saugumui, žmonių sveikatai ar gyvybei, visuomenės gerovei ar valstybės funkcijų atlikimui, taip pat tarpinstitucinę kibernetinių incidentų valdymo sąveiką, kibernetinių incidentų klasifikavimo tvarką ir tarpinstitucinį bendradarbiavimą tiriant kibernetinius incidentus.

2. Plane vartojamos sąvokos apibrėžtos Lietuvos Respublikos elektroninių ryšių įstatyme, Lietuvos Respublikos informacinės visuomenės paslaugų įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme ir Lietuvos Respublikos civilinės saugos įstatyme.

3. Už kibernetinių incidentų valdymą atsakingas Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – Nacionalinis kibernetinio saugumo centras).

## II SKYRIUS
## KIBERNETINIŲ INCIDENTŲ KLASIFIKAVIMO TVARKA

4. Kibernetiniai incidentai klasifikuojami pagal poveikį valstybės informaciniams ištekliams, ypatingos svarbos informacinei infrastruktūrai, viešiesiems ryšių tinklams ar informacinėms sistemoms, naudojamoms elektroninės informacijos prieglobos ar viešosioms elektroninių ryšių paslaugoms teikti (toliau – ryšių ir informacinės sistemos), ir (ar) įtaką ryšių ir informacinėmis sistemomis teikiamų paslaugų gavėjams.

5. Kibernetiniai incidentai skirstomi į keturias kategorijas:

5.1. pavojingi kibernetiniai incidentai;

5.2. didelės reikšmės kibernetiniai incidentai;

5.3. vidutinės reikšmės kibernetiniai incidentai;

5.4. nereikšmingi kibernetiniai incidentai.

6. Tvarkytojas, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjas ar elektroninės informacijos prieglobos paslaugų teikėjas nustatytus kibernetinius incidentus Plano 5.2–5.4 papunkčiuose nurodytoms kibernetinių incidentų kategorijoms priskiria vadovaudamiesi:

6.1. Lietuvos Respublikos Vyriausybės patvirtintuose organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose valstybės informaciniams ištekliams ir ypatingos svarbos informacinei infrastruktūrai nustatytais kriterijais, kai kibernetinis incidentas nustatomas valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje;

6.2. Lietuvos Respublikos krašto apsaugos ministro patvirtintose Viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų kibernetinio saugumo užtikrinimo taisyklėse nustatytais kriterijais, kai kibernetinis incidentas nustatomas viešuosiuose ryšių tinkluose ar informacinėse sistemose, naudojamose elektroninės informacijos prieglobos ar viešosioms elektroninių ryšių paslaugoms teikti.

7. Nacionalinis kibernetinio saugumo centras kibernetinį incidentą priskiria Plano 5.1 papunktyje nurodytai pavojingo kibernetinio incidento kategorijai, jeigu nustatytas didelės reikšmės kibernetinis incidentas ir (ar) jo poveikis gali sukelti (sukelia) bent vieną iš šių padarinių:

7.1. gali sutrikdyti (arba sutrikdo) valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymą ilgiau nei 24 valandas;

7.2. gali nutraukti (arba nutraukia) ryšių ir informacinių sistemų veiklą ir taip gali sutrikdyti (sutrikdo) jomis teikiamų paslaugų teikimą ilgesniam laikui nei valdytojo patvirtintuose ryšių ir informacinių sistemų kibernetinio saugumo politiką ir jos įgyvendinimą reglamentuojančiuose teisės aktuose (toliau – valdytojo kibernetinio saugumo teisės aktai) nurodytas didžiausias leistinas neveikimo terminas (toliau – leistinas neveikimo terminas);

7.3. gali nutraukti (arba nutraukia) kelių valdytojų ar tvarkytojų ir (ar) jų valdomų ryšių ir informacinių sistemų veiklą ir taip sutrikdyti jomis teikiamų paslaugų teikimą;

7.4. gali sukelti ekstremalųjį įvykį.

## III SKYRIUS
## KIBERNETINIŲ INCIDENTŲ VALDYMAS

### PIRMASIS SKIRSNIS
### KIBERNETINIŲ INCIDENTŲ PREVENCIJA, NUSTATYMAS IR VERTINIMAS

8. Kibernetinių incidentų prevenciją ryšių ir informacinėse sistemose vykdo jų tvarkytojai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai ir elektroninės informacijos prieglobos paslaugų teikėjai, atsižvelgdami į Lietuvos Respublikos teisės aktus, reglamentuojančius kibernetinį saugumą ir elektroninės informacijos saugą, Nacionalinio kibernetinio saugumo centro, Policijos departamento prie Lietuvos Respublikos vidaus reikalų ministerijos ir jam pavaldžių įstaigų (toliau – policija), Valstybinės duomenų apsaugos inspekcijos (toliau – kibernetinius incidentus valdančios ir (ar) tiriančios institucijos) ir Kibernetinio saugumo tarybos rekomendacijas, Lietuvos ir tarptautinius standartus ir valdytojo kibernetinio saugumo teisės aktus.

9. Tvarkytojai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai ar elektroninės informacijos prieglobos paslaugų teikėjai iš kibernetinius incidentus valdančių ir (ar) tiriančių institucijų, kitų juridinių asmenų ar kitų valstybių arba tarptautinių organizacijų ar institucijų, atliekančių kibernetinio saugumo užtikrinimo funkcijas, gavę informacijos apie galimą kibernetinį incidentą jų tvarkomose ar valdomose ryšių ir informacinėse sistemose, nedelsdami, bet ne vėliau kaip per 1 darbo dieną nuo šios informacijos gavimo imasi veiksmų, reikalingų kibernetiniam incidentui nustatyti ir patvirtinti.

10. Kibernetinius incidentus valdančios ir (ar) tiriančios institucijos, aptikusios kibernetinį incidentą, informaciją apie jį nedelsdamos pateikia tvarkytojui, ypatingos svarbos

informacinės infrastruktūros valdytojui, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjui ir elektroninės informacijos prieglobos paslaugų teikėjui.

11. Tvarkytojai, ypatingos svarbos informacinės infrastruktūros valdytojai apie nustatytą kibernetinį incidentą pagal Plano 15 punkte nurodytą kompetenciją informuoja:

11.1. Nacionalinį kibernetinio saugumo centrą, vadovaudamiesi Vyriausybės patvirtintuose organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose valstybės informaciniams ištekliams ir ypatingos svarbos informacinei infrastruktūrai nustatyta tvarka;

11.2. policiją, vadovaudamiesi policijos generalinio komisaro nustatyta tvarka ir sąlygomis;

11.3. Valstybinę duomenų apsaugos inspekciją, vadovaudamiesi šios institucijos nustatyta tvarka ir sąlygomis.

12. Viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai ir elektroninės informacijos prieglobos paslaugų teikėjai (elektroninės informacijos prieglobos paslaugų teikėjams Plano 12.3 papunktis netaikomas) apie nustatytą kibernetinį incidentą pagal Plano 15 punkte nurodytą kompetenciją informuoja:

12.1. Nacionalinį kibernetinio saugumo centrą, vadovaudamiesi krašto apsaugos ministro patvirtintose Viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų kibernetinio saugumo užtikrinimo taisyklėse nustatyta tvarka ir sąlygomis;

12.2. policiją, vadovaudamiesi policijos generalinio komisaro nustatyta tvarka ir sąlygomis;

12.3. Valstybinę duomenų apsaugos inspekciją, vadovaudamiesi šios institucijos nustatyta tvarka ir sąlygomis.

13. Tvarkytojai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai ir elektroninės informacijos prieglobos paslaugų teikėjai, nustatę kibernetinį incidentą, turi įvertinti kibernetinį incidentą, surinkti ir kibernetinius incidentus valdančioms ir (ar) tiriančioms institucijoms pateikti informaciją, reikalingą kibernetiniam incidentui apibūdinti, taip pat informaciją apie priemones kibernetiniam incidentui suvaldyti.

14. Nacionalinis kibernetinio saugumo centras, gavęs informaciją apie kibernetinį incidentą, atsižvelgdamas į kibernetinio incidento paplitimo mastą, nustatytus kriterijus, kuriais vadovaujantis kibernetinis incidentas priskiriamas Plano 5 punkte nurodytoms kategorijoms, nedelsdamas patvirtina arba patikslina kibernetinio incidento kategoriją (priskiria didesnės ar mažesnės reikšmės kibernetinių incidentų kategorijai) ir apie tai informuoja tvarkytoją, ypatingos svarbos informacinės infrastruktūros valdytoją, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėją ar elektroninės informacijos prieglobos paslaugų teikėją, kurių tvarkomose ar valdomose ryšių ir informacinėse sistemose nustatytas kibernetinis incidentas.

15. Kibernetinius incidentus valdanti ir (ar) tirianti institucija, gavusi informaciją apie kibernetinį incidentą, nedelsdama apie tai informuoja šias kibernetinius incidentus valdančias ir (ar) tiriančias institucijas:

15.1. Nacionalinį kibernetinio saugumo centrą – nustačiusi, kad kibernetinis incidentas gali paveikti ryšių ir informacines sistemas ir (ar) jomis teikiamų paslaugų teikimą;

15.2. policiją – nustačiusi, kad kibernetinis incidentas gali turėti nusikalstamos veikos požymių;

15.3. Valstybinę duomenų apsaugos inspekciją – nustačiusi, kad kibernetinis incidentas gali būti susijęs su asmens duomenų saugumo pažeidimais.

## ANTRASIS SKIRSNIS
## REAGAVIMAS Į KIBERNETINIUS INCIDENTUS

16. Tvarkytojai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai ir elektroninės informacijos prieglobos paslaugų teikėjai į kibernetinius incidentus reaguoja vadovaudamiesi valdytojo kibernetinio saugumo teisės aktais.

17. Tvarkytojai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai ir elektroninės informacijos prieglobos paslaugų teikėjai privalo imtis organizacinių, techninių ir teisinių priemonių, būtinų kibernetiniam incidentui suvaldyti ir įprastai ryšių ir informacinių sistemų veiklai atkurti.

18. Tvarkytojai ir ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų teikėjai, įvertinę, kad negalės savarankiškai suvaldyti kibernetinio incidento per leistiną neveikimo terminą, kreipiasi pagalbos į Nacionalinį kibernetinio saugumo centrą.

19. Įvykus pavojingam kibernetiniam incidentui Nacionalinis kibernetinio saugumo centras, atsižvelgdamas į kibernetinio saugumo situaciją, nurodo tvarkytojui, ypatingos svarbos informacinės infrastruktūros valdytojui, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjui ar elektroninės informacijos prieglobos paslaugų teikėjui, kad pavojingas kibernetinis incidentas toliau turi būti valdomas vadovaujantis valdytojo kibernetinio saugumo teisės aktais, arba perima pavojingo kibernetinio incidento valdymą.

20. Nacionaliniam kibernetinio saugumo centrui perėmus valdyti kibernetinį incidentą, tvarkytojas, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjas ir elektroninės informacijos prieglobos paslaugų teikėjas:

20.1. renka, apdoroja informaciją, susijusią su kibernetiniu incidentu, ir ją pagal Plano 15.1–15.3 papunkčiuose nurodytą kompetenciją teikia kibernetinius incidentus valdančioms ir (ar) tiriančioms institucijoms;

20.2. teikia Nacionaliniam kibernetinio saugumo centrui informaciją apie atliktus kibernetinio incidento valdymo veiksmus ir jų rezultatus;

20.3. vykdo Nacionalinio kibernetinio saugumo centro nurodymus, susijusius su kibernetinio incidento valdymu, ir dalyvauja kibernetinio incidento valdymo procese, taikydami kibernetinio saugumo užtikrinimo priemones.

21. Nacionalinis kibernetinio saugumo centras, perėmęs valdyti kibernetinį incidentą:

21.1. vertina tvarkytojo, ypatingos svarbos informacinės infrastruktūros valdytojo, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjo ir elektroninės informacijos prieglobos paslaugų teikėjo pateiktą informaciją apie kibernetinį incidentą;

21.2. priima sprendimus dėl kibernetinio incidento valdymo;

21.3. duoda tvarkytojui, ypatingos svarbos informacinės infrastruktūros valdytojui, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjui ir elektroninės informacijos prieglobos paslaugų teikėjui nurodymus, susijusius su kibernetinio incidento valdymu;

21.4. turi teisę surengti koordinacinį pasitarimą dėl kibernetinio incidento valdymo, kuriame privalo dalyvauti suinteresuotų kibernetinius incidentus valdančių ir (ar) tiriančių institucijų atstovai, tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų paskirti kompetentingi asmenys, atsakingi už kibernetinio saugumo organizavimą ir užtikrinimą, ir kiti tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų atstovai, kurių dalyvavimas reikalingas, siekiant suvaldyti kibernetinį incidentą;

21.5. turi teisę į Plano 21.4 papunktyje nurodytą pasitarimą pakviesti kitų kompetentingų ekspertų.

22. Tuo pačiu metu vykstant keliems pavojingiems kibernetinio saugumo incidentams, Nacionalinis kibernetinio saugumo centras pirmiausia valdo tuos pavojingus kibernetinius incidentus, kurių galimas poveikis ir žala gali būti didesni.

23. Nacionalinis kibernetinio saugumo centras apie pavojingo kibernetinio incidento nustatymą ir pavojingo kibernetinio incidento valdymo veiksmų eigą nedelsdamas, bet ne vėliau kaip per 1 valandą nuo pavojingo kibernetinio incidento nustatymo informuoja Lietuvos Respublikos krašto apsaugos ministeriją, Lietuvos Respublikos Vyriausybės kanceliariją, Lietuvos Respublikos Seimo kanceliariją ir Lietuvos Respublikos Prezidento kanceliariją ir kartu pateikia apibendrintą informaciją apie kibernetinį incidentą ir galimą jo poveikį. Krašto apsaugos ministerija, Vyriausybės kanceliarija, Seimo kanceliarija ir Prezidento kanceliarija apie pavojingą kibernetinį incidentą nedelsdamos informuoja atitinkamai krašto apsaugos ministrą, Ministrą Pirmininką, Seimo Pirmininką ir Prezidentą.

24. Nacionalinis kibernetinio saugumo centras apie pavojingo kibernetinio incidento valdymą reguliariai, ne rečiau kaip kas 4 valandas, informuoja Plano 23 punkte nurodytus informacijos gavėjus, o informacija apie pavojingo kibernetinio incidento suvaldymą šiems gavėjams pateikiama ne vėliau kaip per 1 valandą nuo pavojingo kibernetinio incidento suvaldymo.

25. Kibernetinis incidentas laikomas suvaldytu ar pasibaigusiu, kai išnyksta kibernetinio incidento poveikis ryšių ir informacinėms sistemoms ir ryšių ir informacinės sistemos atitinka veiklos kriterijus, nustatytus valdytojo kibernetinio saugumo teisės aktuose.

26. Nacionalinis kibernetinio saugumo centras apie rengiamą pasitarimą dėl pavojingo kibernetinio incidento valdymo atsakingus asmenis, paskirtus tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų, ir suinteresuotų kibernetinius incidentus valdančių ir (ar) tiriančių institucijų atstovus informuoja naudodamasis kibernetinio saugumo informaciniu tinklu ar kitomis saugiomis informacijos perdavimo priemonėmis.

27. Nacionalinis kibernetinio saugumo centras, nustatęs, kad nepakanka turimų kibernetinius incidentus valdančių ir (ar) tiriančių institucijų, tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų išteklių pavojingam kibernetiniam incidentui suvaldyti, nedelsdamas, bet ne vėliau kaip per 1 valandą informuoja Krašto apsaugos ministeriją ir Vyriausybės kanceliariją. Krašto apsaugos ministras, gavęs anksčiau nurodytą informaciją, nedelsdamas priima sprendimą dėl pavojingo kibernetinio incidento valdymo veiksmų ir priemonių.

28. Nacionalinis kibernetinio saugumo centras, nustatęs, kad pavojingo kibernetinio incidento organizatorius (-iai), vykdytojas (-ai) ar šaltinis yra ne Lietuvos Respublikos teritorijoje, turi teisę kreiptis pagalbos į kitų valstybių institucijas ar tarptautines organizacijas, kurios atlieka kibernetinio saugumo užtikrinimo funkcijas ir su kuriomis bendradarbiaujama kibernetinio saugumo srityje, ir pateikti informaciją, susijusią su kibernetiniu incidentu.

29. Nacionalinis kibernetinio saugumo centras nedelsdamas, bet ne vėliau kaip per 1 valandą nuo pavojingo kibernetinio incidento nustatymo ar informacijos apie Plano 5.2–5.3 papunkčiuose nurodytus kibernetinius incidentus gavimo apie šiuos kibernetinius incidentus informuoja Lietuvos Respublikos valstybės saugumo departamentą.

30. Nesuvaldžius pavojingo kibernetinio incidento per leistiną neveikimo terminą, Nacionalinis kibernetinio saugumo centras nedelsdamas, bet ne vėliau kaip per 1 valandą nuo leistino neveikimo termino pabaigos informuoja apie tai Vyriausybės kanceliariją, taip pat informaciją apie kibernetinį incidentą ir siūlomus tolesnius kibernetinio incidento valdymo veiksmus ir priemones pateikia svarstyti Vyriausybei.

## TREČIASIS SKIRSNIS

## KIBERNETINIO INCIDENTO ANALIZĖ IR TARPINSTITUCINIS BENDRADARBIAVIMAS TIRIANT KIBERNETINIUS INCIDENTUS

31. Tvarkytojai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai, elektroninės informacijos prieglobos paslaugų teikėjai ir kibernetinius incidentus valdančios ir (ar) tiriančios institucijos ne vėliau kaip per 30 kalendorinių dienų nuo kibernetinio incidento suvaldymo ar pasibaigimo atlieka ir Nacionaliniam kibernetinio saugumo centrui per kibernetinio saugumo informacinį tinklą ar kitomis informacijos perdavimo priemonėmis pateikia kibernetinio incidento analizę. Nacionalinis kibernetinio saugumo centras apibendrintą kibernetinio incidento analizės informaciją, naudingą kibernetinių incidentų prevencijai, paskelbia kibernetinio saugumo informaciniame tinkle.

32. Kibernetinius incidentus valdančios ir (ar) tiriančios institucijos, kartu su tvarkytoju, ypatingos svarbos informacinės infrastruktūros valdytoju, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėju ir (ar) elektroninės informacijos prieglobos paslaugų teikėju išanalizavusios ir įvertinusios visą informaciją, susijusią su įvykusiu kibernetiniu incidentu, atliktus veiksmus ir panaudotas priemones:

32.1. nustačiusios nepakankamą teisinį reglamentavimą, keičia teisės aktus, reglamentuojančius kibernetinį saugumą, ar inicijuoja jų pakeitimus;

32.2. atnaujina ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planus ar inicijuoja jų atnaujinimą;

32.3. įvertina organizacinių ir techninių kibernetinio saugumo užtikrinimo priemonių atnaujinimo poreikį, suplanuoja priemones šiam poreikiui patenkinti ir užtikrina jų įgyvendinimą.

33. Tvarkytojas, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjas ar elektroninės informacijos prieglobos paslaugų teikėjas, kurio ryšių ir informacinėse sistemose nustatytas kibernetinis incidentas, išanalizavęs ir įvertinęs visą informaciją, susijusią su kibernetiniu incidentu, atliktus veiksmus ir panaudotas priemones:

33.1. privalo imtis priemonių, kad būtų pašalintas ryšių ir informacinių sistemų pažeidžiamumas;

33.2. įvertina ryšių ir informacinių sistemų riziką ir atitiktį Vyriausybės nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams ar krašto apsaugos ministro nustatytoms Viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų kibernetinio saugumo užtikrinimo taisyklėms;

33.3. kibernetinius incidentus valdančių ir (ar) tiriančių institucijų reikalavimu pateikia papildomą informaciją, reikalingą kibernetiniam incidentui tirti;

33.4. nustačius spragų valdytojo kibernetinio saugumo teisės aktuose, inicijuoja jų atnaujinimą;

33.5. kibernetinio saugumo informaciniame tinkle paskelbia susistemintą ir aktualią informaciją apie kibernetinio incidento nustatymą ir suvaldymą;

33.6. nedelsdamas, bet ne vėliau kaip per 1 darbo dieną nuo kibernetinio incidento suvaldymo informuoja ryšių ir informacinėmis sistemomis teikiamų paslaugų gavėjus (jeigu tokių yra), jeigu kibernetinio incidento poveikis padarė arba gali ateityje padaryti žalos ryšių ir informacinėmis sistemomis teikiamų paslaugų gavėjui.

34. Kibernetinius incidentus valdančios ir (ar) tiriančios institucijos duomenis ir informaciją, susijusius su kibernetinių incidentų tyrimu, kitoms kibernetinius incidentus valdančioms ir (ar) tiriančioms institucijoms perduoda elektroniniu būdu per kibernetinio saugumo informacinį tinklą, o jeigu tokios galimybės nėra – kitomis saugiomis informacijos perdavimo priemonėmis.

35. Jeigu kibernetinius incidentus valdančiai ir (ar) tiriančiai institucijai reikia papildomos informacijos kibernetiniam incidentui tirti, ji kreipiasi į kitas kibernetinius

incidentus valdančias ir (ar) tiriančias institucijas, kurios šią informaciją turi pateikti per besikreipiančios institucijos nurodytą terminą.

---

*Priedo pakeitimai:*
*Nr. 198, 2018-02-28, paskelbta TAR 2018-03-05, i. k. 2018-03533*

**Pakeitimai:**

1.
Lietuvos Respublikos Vyriausybė, Nutarimas
Nr. 198, 2018-02-28, paskelbta TAR 2018-03-05, i. k. 2018-03533
Dėl Lietuvos Respublikos Vyriausybės 2016 m. sausio 25 d. nutarimo Nr. 87 „Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“ pakeitimo