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:

1. Patvirtinti Nacionalinį kibernetinių incidentų valdymo planą (pridedama).

2. Įpareigoti:

2.1. Lietuvos Respublikos krašto apsaugos ministeriją ir Lietuvos Respublikos Vyriausybės kanceliariją paskirti asmenis, atsakingus už informacijos apie pavojingus kibernetinius incidentus įvertinimą ir perdavimą Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka, ir ne vėliau kaip per 10 darbo dienų nuo šio nutarimo įsigaliojimo pateikti šių asmenų kontaktinę informaciją Kibernetinio saugumo ir telekomunikacijų tarnybai prie Krašto apsaugos ministerijos;

2.2. Valstybinę duomenų apsaugos inspekciją, Policijos departamentą prie Lietuvos Respublikos vidaus reikalų ministerijos, Kibernetinio saugumo ir telekomunikacijų tarnybą prie Krašto apsaugos ministerijos paskirti kontaktinius asmenis, atsakingus už keitimąsi informacija, susijusia su kibernetinių incidentų tyrimu ir analize, tarp Lietuvos Respublikos ryšių reguliavimo tarnybos, Valstybinės duomenų apsaugos inspekcijos, Policijos departamento prie Lietuvos Respublikos vidaus reikalų ministerijos, Kibernetinio saugumo ir telekomunikacijų tarnybos prie Krašto apsaugos ministerijos, ir ne vėliau kaip per 10 darbo dienų nuo šio nutarimo įsigaliojimo minėtoms institucijoms pateikti šių asmenų kontaktinę informaciją.

3. Pasiūlyti:

3.1. Lietuvos Respublikos ryšių reguliavimo tarnybai paskirti kontaktinius asmenis, atsakingus už keitimąsi informacija, susijusia su kibernetinių incidentų tyrimu ir analize, tarp Lietuvos Respublikos ryšių reguliavimo tarnybos, Valstybinės duomenų apsaugos inspekcijos, Policijos departamento prie Lietuvos Respublikos vidaus reikalų ministerijos, Kibernetinio saugumo ir telekomunikacijų tarnybos prie Krašto apsaugos ministerijos, ir ne vėliau kaip per 10 darbo dienų nuo šio nutarimo įsigaliojimo pateikti minėtoms institucijoms šių asmenų kontaktinę informaciją;

3.2. Valstybės saugumo departamentui paskirti asmenį, kuriam Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka būtų pateikiama informacija apie kibernetinius incidentus, ir ne vėliau kaip per 10 darbo dienų nuo šio nutarimo įsigaliojimo pateikti Kibernetinio saugumo ir telekomunikacijų tarnybai prie Krašto apsaugos ministerijos šio asmens kontaktinę informaciją;

3.3. Lietuvos Respublikos Seimo kanceliarijai ir Lietuvos Respublikos Prezidento kanceliarijai paskirti asmenis, atsakingus už informacijos apie pavojingus kibernetinius incidentus įvertinimą ir perdavimą Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka, ir ne vėliau kaip per 10 darbo dienų nuo šio nutarimo įsigaliojimo pateikti Kibernetinio saugumo ir telekomunikacijų tarnybai prie Krašto apsaugos ministerijos šių asmenų kontaktinę informaciją.

Finansų ministras, pavaduojantis
Ministrą Pirmininką Rimantas Šadžius

Krašto apsaugos ministras Juozas Olekas

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2016 m. sausio 25 d. nutarimu Nr. 87

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 ir 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 ir Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.

3. Už kibernetinių incidentų valdymą atsakingos institucijos:

3.1. Kibernetinio saugumo ir telekomunikacijų tarnyba prie Krašto apsaugos ministerijos, vykdanti Nacionalinio kibernetinio saugumo centro funkcijas (toliau – Nacionalinis kibernetinio saugumo centras), kai kibernetinis incidentas nustatomas valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje arba gali paveikti valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros ir jų valdytojų ar tvarkytojų veiklą;

3.2. Lietuvos Respublikos ryšių reguliavimo tarnyba (toliau – Ryšių reguliavimo tarnyba) – visais kitais kibernetinių incidentų atvejais.

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 informacinė sistema arba RIS), ir (ar) įtaką Ryšių ir informacinės sistemos 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. Kriterijus, kuriais vadovaujantis kibernetinis incidentas priskiriamas Plano 5.2–5.4 papunkčiuose nustatytoms kategorijoms, nustato:

6.1. Lietuvos Respublikos Vyriausybė (toliau – Vyriausybė) – tvirtinamuose organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose valstybės informaciniams ištekliams ir ypatingos svarbos informacinei infrastruktūrai, kai kibernetinis incidentas nustatomas valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje;

6.2. Ryšių reguliavimo tarnyba – tvirtinamame Informacijos apie kibernetinius incidentus ir taikytas šių incidentų valdymo priemones teikimo Ryšių reguliavimo tarnybai tvarkos ir sąlygų apraše.

7. Atsižvelgdami į nustatytus kriterijus, Plano 5.2–5.4 papunkčiuose nustatytoms kibernetinių incidentų kategorijoms kibernetinius incidentus priskiria tvarkytojas, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjas ar elektroninės informacijos prieglobos paslaugų teikėjas, kurio RIS nustatytas kibernetinis incidentas.

8. Nacionalinis kibernetinio saugumo centras ar Ryšių reguliavimo tarnyba pagal kompetenciją kibernetinį incidentą gali priskirti Plano 5.1 papunktyje nustatytai pavojingo kibernetinio incidento kategorijai, jeigu nustatytas didelės reikšmės kibernetinis incidentas ir (ar) jo poveikis gali sukelti (sukelia) bent vieną iš šių padarinių:

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

8.2. gali visiškai sutrikdyti (arba visiškai sutrikdo) RIS veiklą ir taip gali sutrikdyti (sutrikdo) RIS teikiamų paslaugų teikimą didžiausią leistiną neveikimo terminą, nustatytą valdytojo teisės aktuose, reglamentuojančiuose kibernetinį saugumą, ar kituose valdytojo vadovo patvirtintuose dokumentuose, kuriuose nustatyti valdytojų ar tvarkytojų veiksmai, funkcijos ir atsakomybė įvykus kibernetiniam incidentui, taip pat kibernetinių incidentų prevencijos priemonės (toliau – valdytojo kibernetinio saugumo teisės aktai) (toliau – maksimalus leistinas neveikimo terminas). Maksimalus leistinas neveikimo terminas pagal

kompetenciją turi būti suderintas su Nacionaliniu kibernetinio saugumo centru arba Ryšių reguliavimo tarnyba;

8.3. gali visiškai sutrikdyti (arba visiškai sutrikdo) kelių valdytojų ar tvarkytojų ir (ar) jų valdomų RIS veiklą ir taip sutrikdyti RIS teikiamų paslaugų teikimą;

8.4. gali sukelti ekstremalųjį įvykį, nurodytą Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų sąraše.

9. Atsižvelgdami į kibernetinio incidento paplitimo mastą, nustatytus kriterijus, kuriais vadovaujantis kibernetinis incidentas priskiriamas Plano 5.2–5.4 papunkčiuose nustatytoms kategorijoms, ar kibernetinio incidento poveikį RIS, Nacionalinis kibernetinio saugumo centras arba Ryšių reguliavimo tarnyba, gavę iš tvarkytojo, ypatingos svarbos informacinės infrastruktūros valdytojo, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjo ar elektroninės informacijos prieglobos paslaugų teikėjo informaciją apie nustatytą kibernetinį incidentą, turi teisę patikslinti tvarkytojo, ypatingos svarbos informacinės infrastruktūros valdytojo, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjo ar elektroninės informacijos prieglobos paslaugų teikėjo priskirtą kibernetinio incidento kategoriją (priskirti didesnės ar mažesnės reikšmės kibernetinių incidentų kategorijai).

III SKYRIUS
KIBERNETINIŲ INCIDENTŲ VALDYMAS

PIRMASIS SKIRSNIS
KIBERNETINIŲ INCIDENTŲ PREVENCIJA, NUSTATYMAS IR VERTINIMAS

10. 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, Ryšių reguliavimo tarnybos, Policijos departamento prie Lietuvos Respublikos vidaus reikalų ministerijos ir jam pavaldžių įstaigų (toliau – policija), Valstybinės duomenų apsaugos inspekcijos (toliau bendrai – kibernetinius incidentus valdančios ir (ar) tiriančios (toliau – KIVT) institucijos, o atskirai – KIVT institucija) ir Kibernetinio saugumo tarybos rekomendacijas, Lietuvos ir tarptautinius standartus ir valdytojo kibernetinio saugumo teisės aktus.

11. Tvarkytojai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai ar elektroninės informacijos prieglobos paslaugų teikėjai iš KIVT institucijų, kitų juridinių asmenų ar kitų valstybių ar tarptautinių organizacijų ar institucijų, atliekančių kibernetinio saugumo užtikrinimo funkcijas, gavę informacijos apie galimą kibernetinį incidentą jų tvarkomose ar valdomose RIS, nedelsdami imasi veiksmų, reikalingų kibernetiniam incidentui nustatyti ir patvirtinti.

12. KIVT institucijos nedelsdamos, ne vėliau kaip per 30 minučių nuo kibernetinio incidento aplinkybių aptikimo, pateikia informaciją apie galimą kibernetinį incidentą tvarkytojui, ypatingos svarbos informacinės infrastruktūros valdytojui, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjui ir elektroninės informacijos prieglobos paslaugų teikėjui.

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, per kibernetinio saugumo informacinį tinklą ar kitas informacijos perdavimo priemones (paštu, el. paštu, telefonu, per pasiuntinius ir panašiai) informuoja apie šį faktą KIVT institucijoms pagal jų kompetenciją.

14. 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, per kaip įmanoma trumpesnį laiką turi įvertinti kibernetinį incidentą, surinkti ir KIVT institucijoms pagal jų kompetenciją pateikti informaciją, reikalingą kibernetiniam incidentui apibūdinti, taip pat informaciją apie priemones kibernetiniam incidentui suvaldyti.

15. Nacionalinis kibernetinio saugumo centras arba Ryšių reguliavimo tarnyba, pagal kompetenciją įvertinę gautą informaciją apie kibernetinį incidentą, patvirtina arba, atsižvelgdami į Plano 9 punktą, patikslina kibernetinio incidento kategoriją ir apie tai nedelsdami informuoja pranešusį tvarkytoją, ypatingos svarbos informacinės infrastruktūros valdytoją, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėją ar elektroninės informacijos prieglobos paslaugų teikėją.

16. KIVT institucija, pagal kompetenciją įvertinusi gautą informaciją apie kibernetinį incidentą, nedelsdama informuoja apie kibernetinio incidento nustatymo faktą kitas KIVT institucijas:

16.1. Nacionalinį kibernetinio saugumo centrą – nustačiusi, kad kibernetinis incidentas taip pat gali paveikti valstybės informacinius išteklius ir ypatingos svarbos informacinę infrastruktūrą;

16.2. Ryšių reguliavimo tarnybą – nustačiusi, kad kibernetinis incidentas taip pat gali paveikti viešuosius ryšių tinklus, viešąsias elektroninių ryšių ir elektroninės informacijos prieglobos paslaugas;

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

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

ANTRASIS SKIRSNIS
REAGAVIMAS Į KIBERNETINIUS INCIDENTUS

17. 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.

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

19. Tvarkytojai ir ypatingos svarbos informacinės infrastruktūros valdytojai, įvertinę, kad negalės savarankiškai suvaldyti kibernetinio incidento per didžiausią leistiną neveikimo terminą, pirmiausia kreipiasi pagalbos į Nacionalinį kibernetinio saugumo centrą, o viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų ir (arba) elektroninės informacijos prieglobos paslaugų teikėjai ir gavėjai, jeigu jie nėra tvarkytojai ar ypatingos svarbos informacinės infrastruktūros valdytojai, – į Ryšių reguliavimo tarnybą.

20. Pavojingo kibernetinio incidento atveju Nacionalinis kibernetinio saugumo centras arba Ryšių reguliavimo tarnyba, atsižvelgdami į kibernetinio saugumo situaciją, pagal kompetenciją 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 pagal kompetenciją perima pavojingo kibernetinio incidento valdymą.

21. Nacionaliniam kibernetinio saugumo centrui arba Ryšių reguliavimo tarnybai pagal kompetenciją 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:

21.1. nuolat renka, apdoroja informaciją, susijusią su kibernetiniu incidentu, ir ją teikia KIVT institucijoms pagal kompetenciją;

21.2. nuolat teikia Nacionalinio kibernetinio saugumo centrui arba Ryšių reguliavimo tarnybai pagal kompetenciją informaciją apie atliktus kibernetinio incidento valdymo veiksmus ir jų rezultatus;

21.3. vykdo Nacionalinio kibernetinio saugumo centro arba Ryšių reguliavimo tarnybos nurodymus, susijusius su kibernetinio incidento valdymu, ir dalyvauja kibernetinio incidento valdymo procese, taikydami kibernetinio saugumo užtikrinimo priemones.

22. Nacionalinis kibernetinio saugumo centras arba Ryšių reguliavimo tarnyba, pagal kompetenciją perėmę valdyti kibernetinį incidentą:

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

22.2. priima sprendimus dėl kibernetinio incidento valdymo;

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

22.4. turi teisę surengti koordinacinį pasitarimą dėl kibernetinio incidento valdymo, kuriame privalo dalyvauti suinteresuotų KIVT 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 pagal poreikį kiti tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų atstovai, kuriems būtina dalyvauti, siekiant suvaldyti kibernetinį incidentą;

22.5. turi teisę į koordinacinį pasitarimą pakviesti kitų kompetentingų ekspertų.

23. Tuo pačiu metu vykstant keliems pavojingiems kibernetinio saugumo incidentams, Nacionalinis kibernetinio saugumo centras arba Ryšių reguliavimo tarnyba, pagal kompetenciją įvertinę informaciją apie pavojingus kibernetinius incidentus, pirmiausia valdo tuos pavojingus kibernetinius incidentus, kurių galimas poveikis ir žala gali būti didžiausi.

24. Ryšių reguliavimo tarnyba apie pavojingo kibernetinio incidento nustatymą ir pavojingo kibernetinio incidento valdymo veiksmų eigą nedelsdama, ne vėliau kaip per vieną valandą nuo pavojingo kibernetinio incidento nustatymo, informuoja Nacionalinį kibernetinio saugumo centrą bei Vyriausybės kanceliarijos, Lietuvos Respublikos Seimo (toliau – Seimas) kanceliarijos ir Lietuvos Respublikos Prezidento (toliau – Prezidentas) kanceliarijos paskirtus asmenis ir kartu pateikia apibendrintą informaciją apie kibernetinį incidentą ir galimą jo poveikį.

25. Nacionalinis kibernetinio saugumo centras apie pavojingo kibernetinio incidento nustatymą ir pavojingo kibernetinio incidento valdymo veiksmų eigą nedelsdamas, ne vėliau kaip per vieną valandą nuo pavojingo kibernetinio incidento nustatymo, informuoja Ryšių reguliavimo tarnybą, Lietuvos Respublikos krašto apsaugos ministerijos, Vyriausybės kanceliarijos, Seimo kanceliarijos ir Prezidento kanceliarijos paskirtus asmenis ir kartu pateikia apibendrintą informaciją apie kibernetinį incidentą ir galimą jo poveikį.

26. Nacionalinis kibernetinio saugumo centras arba Ryšių reguliavimo tarnyba apie pavojingo kibernetinio incidento valdymą reguliariai, ne rečiau kaip kas 4 valandas, informuoja Plano 24 ir 25 punktuose nurodytus informacijos gavėjus, o informacija apie pavojingo kibernetinio incidento suvaldymą šiems gavėjams pateikiama ne vėliau kaip per vieną valandą suvaldžius pavojingą kibernetinį incidentą.

27. Kibernetinis incidentas laikomas suvaldytu ar pasibaigusiu, kai išnyksta kibernetinio incidento poveikis RIS ir RIS atitinka veiklos kriterijus, kuriuos valdytojai nustato valdytojo kibernetinio saugumo teisės aktuose.

28. Vyriausybės kanceliarija, Seimo kanceliarija ir Prezidento kanceliarija, įvertinusios informaciją apie pavojingą kibernetinį incidentą, informuoja atitinkamai institucijos vadovus, Ministrą Pirmininką, Seimo Pirmininką ir Prezidentą.

29. Nacionalinis kibernetinio saugumo centras arba Ryšių reguliavimo tarnyba apie rengiamą koordinacinį 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 KIVT institucijų atstovus informuoja, naudodamiesi kibernetinio saugumo informaciniu tinklu ar kitomis saugiomis informacijos perdavimo priemonėmis.

30. Ryšių reguliavimo tarnyba, nustačiusi, kad jos turimų išteklių nepakanka pavojingam kibernetiniam incidentui suvaldyti, nedelsdama informuoja apie tai Nacionalinį kibernetinio saugumo centrą.

31. Nacionalinis kibernetinio saugumo centras, nustatęs, kad nepakanka turimų KIVT institucijų ir 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 informuoja Lietuvos Respublikos krašto apsaugos ministerijos ir Vyriausybės kanceliarijos paskirtus asmenis, taip pat krašto apsaugos ministrą, o šis priima sprendimą dėl pavojingo kibernetinio incidento valdymo priemonių.

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

33. Nacionalinis kibernetinio saugumo centras nedelsdamas, ne vėliau kaip per vieną valandą nuo pavojingo kibernetinio incidento nustatymo ir informacijos apie Plano 5.2–5.3 papunkčiuose nustatytus kibernetinius incidentus gavimo, informuoja apie Plano 5.1–5.3 papunkčiuose nustatytus kibernetinius incidentus Lietuvos Respublikos valstybės saugumo departamento paskirtą asmenį.

34. Pavojingo kibernetinio incidento nesuvaldžius per didžiausią leistiną neveikimo terminą, Nacionalinis kibernetinio saugumo centras arba Ryšių reguliavimo tarnyba nedelsdami informuoja apie tai Vyriausybės kanceliarijos paskirtą atsakingą asmenį, taip pat informaciją apie kibernetinį incidentą ir tolesnius kibernetinio incidento valdymo veiksmus ir priemones (kartu su Vyriausybės pasitarimo protokolo projektu) pateikia Vyriausybei, o ši šią informaciją apsvarsto Vyriausybės pasitarime.

TREČIASIS SKIRSNIS
KIBERNETINIO INCIDENTO ANALIZĖ IR TARPINSTITUCINIS BENDRADARBIAVIMAS TIRIANT KIBERNETINIUS INCIDENTUS

35. Tvarkytojai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai, elektroninės informacijos prieglobos paslaugų teikėjai ir KIVT institucijos pagal kompetenciją atlieka kibernetinio incidento analizę. Nacionalinis kibernetinio saugumo centras ir Ryšių reguliavimo tarnyba naudingą apibendrintą informaciją, gautą kibernetinių incidentų analizės metu, paskelbia kibernetinio saugumo informaciniame tinkle.

36. KIVT 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:

36.1. nustačiusios nepakankamą teisinį reglamentavimą, keičia teisės aktus (inicijuoja teisės aktų pakeitimus), reglamentuojančius kibernetinį saugumą;

36.2. prireikus atnaujina (inicijuoja atnaujinimą) ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planus;

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

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

37.1. privalo imtis priemonių, kad būtų pašalintas RIS pažeidžiamumas;

37.2. įvertina RIS riziką ir (ar) atitiktį Vyriausybės nustatytiems ar Ryšių reguliavimo tarnybos patvirtintiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams;

37.3. KIVT institucijų reikalavimu pateikia papildomą informaciją, reikalingą kibernetiniam incidentui tirti;

37.4. nustačius teisinio reglamentavimo spragų, inicijuoja valdytojo kibernetinio saugumo teisės aktų atnaujinimą;

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

37.6. ne vėliau kaip per 8 valandas nuo kibernetinio incidento suvaldymo informuoja RIS teikiamų paslaugų gavėjus (jeigu tokių yra), jeigu kibernetinio incidento poveikis padarė arba gali ateityje padaryti žalos RIS teikiamų paslaugų gavėjui.

38. KIVT institucijos, tirdamos kibernetinius incidentus, bendradarbiauja operatyviai, duomenis ir informaciją perduoda KIVT institucijų paskirtiems kontaktiniams asmenims, atsakingiems už keitimąsi informacija, susijusia su kibernetinių incidentų tyrimu ir analize,

elektroniniu būdu per kibernetinio saugumo informacinį tinklą, o jeigu tokios galimybės nėra, – kitomis saugiomis informacijos perdavimo priemonėmis.

39. KIVT institucija, pagal kompetenciją tirianti kibernetinį incidentą, nustačiusi papildomos informacijos apie kibernetinį incidentą poreikį, kreipiasi į kitas KIVT institucijas, kurios papildomą informaciją turi pateikti per KIVT institucijos, pagal kompetenciją tiriančios kibernetinį incidentą, prašyme nurodytą terminą.

_____