PATVIRTINTA
Lietuvos Respublikos Vyriausybės
nutarimu Nr.

NACIONALINIS KIBERNETINIŲ INCIDENTŲ VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nacionalinis kibernetinių incidentų valdymo planas (toliau – Planas) nustato kibernetinių incidentų klasifikavimo, informavimo apie kibernetinius incidentus, kibernetinių incidentų tyrimo ir kibernetinių incidentų analizės baigus kibernetinių incidentų tyrimą tvarką, valdant 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 valdymo organizavimą, stebėseną ir analizę nacionaliniu lygiu atsakingas Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – Nacionalinis kibernetinio saugumo centras). Valstybinė duomenų apsaugos inspekcija, Lietuvos policija ir kitos institucijos, kurių funkcijos susijusios su kibernetiniu saugumu pagal Kibernetinio saugumo įstatymu priskirtą kompetenciją, tiria ar dalyvauja valdant kibernetinius incidentus.

4. Nacionalinis kibernetinio saugumo centras, Valstybinė duomenų apsaugos inspekcija ir Lietuvos policija (toliau bendrai – kibernetinius incidentus valdančios ir (ar) tiriančios (toliau – KIVT) institucijos, o atskirai – KIVT institucija) paskiria kontaktinius asmenis, atsakingus už keitimąsi informacija kibernetinio incidento valdymo metu, numato šių asmenų pakeičiamumą ir pateikia jų kontaktinę informaciją Nacionaliniam kibernetinio saugumo centrui.

5. Lietuvos Respublikos Vyriausybės kanceliarija, Lietuvos Respublikos Seimo kanceliarija, Lietuvos Respublikos Prezidento kanceliarija, Lietuvos Respublikos valstybės saugumo departamentas, Lietuvos Respublikos krašto apsaugos ministerija paskiria asmenis, atsakingus už informacijos perdavimą pagal Plane nustatytą tvarką, ir pateikia šių asmenų kontaktinę informaciją Nacionaliniam kibernetinio saugumo centrui.

6. Kibernetinio saugumo subjektai pateikia Nacionaliniam kibernetinio saugumo centrui atsakingo asmens, su kuriuo galima susisiekti visą parą, telefono numerį, elektroninio pašto adresą, kitą kontaktinę informaciją Nacionalinio kibernetinio saugumo centro interneto svetainėje nurodytais kontaktais.

7. Nacionalinis kibernetinio saugumo centras ne vėliau kaip per 1 darbo dieną nuo informacijos apie paskirtus kontaktinius asmenis gavimo suveda gautą neįslaptintą

informaciją į kibernetinio saugumo informacinį tinklą ir informuoja apie tai pranešusį subjektą.

8. Pasikeitus atsakingiems asmenims ar kontaktinei informacijai, atnaujinta informacija ne vėliau kaip kitą darbo dieną nuo duomenų pasikeitimo teikiama Plano 4–6 punktuose nustatyta tvarka.

II SKYRIUS
KIBERNETINIŲ INCIDENTŲ KLASIFIKAVIMAS

9. Kibernetiniai incidentai klasifikuojami pagal poveikį kibernetinio saugumo subjektų ryšių ir informacinėms sistemoms ir (ar) paslaugų teikimui ir (ar) įtaką ryšių ir informacinių sistemų teikiamų paslaugų gavėjams.

10. Kibernetiniai incidentai skirstomi į keturias kategorijas:

10.1. pavojingi kibernetiniai incidentai;

10.2. didelio poveikio kibernetiniai incidentai;

10.3. vidutinio poveikio kibernetiniai incidentai;

10.4. nereikšmingo poveikio kibernetiniai incidentai.

11. Kriterijai, kuriais vadovaujantis kibernetiniai incidentai priskiriami Plano 10 punkte nustatytoms kategorijoms, nustatyti Plano priede.

12. Kibernetinius incidentus Plano 10.2–10.4 papunkčiuose nustatytoms kategorijoms, atsižvelgdami į Plano priede nustatytus kriterijus, priskiria kibernetinio saugumo subjektai, kurių ryšių ir informacinėse sistemose nustatyti kibernetiniai incidentai.

13. Kibernetinius incidentus Plano 10.1 papunktyje nustatytai pavojingo kibernetinio incidento kategorijai turi teisę priskirti tik Nacionalinis kibernetinio saugumo centras, jeigu nustatytas kibernetinis incidentas ir (ar) jo poveikis atitinka bent vieną iš kriterijų, nurodytų Plano priede, būdingų pavojingo incidento kategorijai.

III SKYRIUS
INFORMAVIMAS APIE KIBERNETINIUS INCIDENTUS

14. Kibernetinio saugumo subjektai Nacionalinį kibernetinio saugumo centrą informuoja apie:

14.1. didelio poveikio kibernetinius incidentus – nedelsiant, bet ne vėliau kaip per 1 valandą nuo jų nustatymo;

14.2. vidutinio poveikio kibernetinius incidentus – ne vėliau kaip per 4 valandas nuo jų nustatymo;

14.3. nereikšmingo poveikio kibernetinius incidentus – periodiškai kiekvieno kalendorinio mėnesio 1 dieną teikiant apibendrintą informaciją apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo teikimo dienos, skaičių.

15. Nacionalinis kibernetinio saugumo centras informuojamas apie didelio ar vidutinio poveikio kibernetinius incidentus kibernetinio saugumo subjekto pranešimu, kuriame nurodoma:

15.1. kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Plano priede pateiktus kriterijus;

15.2. trumpas kibernetinio incidento apibūdinimas;

15.3. tikslus laikas, kada kibernetinis incidentas įvyko ir buvo nustatytas;

15.4. kibernetinio incidento šalinimo tvarka (nurodant, ar tai prioritetas, ar ne);

15.5. tikslus laikas, kada bus teikiama kibernetinio incidento tyrimo ataskaita.

16. Skaitmeninių paslaugų teikėjai Nacionalinį kibernetinio saugumo centrą informuoja tik apie kibernetinius incidentus, turinčius didelį poveikį teikiamų skaitmeninių paslaugų teikimui, ir tik tuo atveju, kai skaitmeninių paslaugų teikėjas gali naudotis informacija, kuri yra reikalinga incidento poveikiui įvertinti.

17. Ypatingos svarbos informacinės infrastruktūros valdytojai, kurių paslaugų teikimas priklauso nuo trečiųjų šalių skaitmeninių paslaugų teikėjų teikiamų paslaugų, nedelsdami, bet ne vėliau kaip per 1 valandą nuo jų nustatymo informuoja Nacionalinį kibernetinio saugumo centrą ir skaitmeninių paslaugų teikėjus apie neigiamą poveikį ypatingos svarbos infrastruktūros veiklai, kurį lėmė skaitmeninių paslaugų teikėjų ryšių ir informacinėse sistemose įvykę sutrikimai.

18. Asmenys, kuriems teisės aktuose nėra nustatytos pareigos pranešti apie kibernetinius incidentus jų valdomose ryšių ir informacinėse sistemose, turi teisę savanoriškai pranešti Nacionaliniam kibernetinio saugumo centrui apie kibernetinius incidentus ir taikytas kibernetinių incidentų tyrimo ar valdymo priemones Nacionalinio kibernetinio saugumo centro interneto svetainėje nurodytais kontaktais.

19. Nacionalinis kibernetinio saugumo centras, apie kibernetinį incidentą gavęs informacijos iš asmenų, kuriems nėra nustatytos pareigos pranešti apie kibernetinius incidentus jų valdomose ryšių ir informacinėse sistemose, šį kibernetinį incidentą savarankiškai priskiria kibernetinio incidento kategorijai ir tiria ta pačia tvarka, kaip ir kibernetinius incidentus, apie kuriuos sužinoma gavus kibernetinio saugumo subjektų pranešimus.

20. Atsižvelgdamas į kibernetinio incidento paplitimo mastą, nustatytus kriterijus, kuriais vadovaujantis kibernetinis incidentas priskiriamas Plano 10.2–10.4 papunkčiuose nustatytoms kategorijoms, ar kibernetinio incidento poveikį ryšių ir informacinei sistemai, Nacionalinis kibernetinio saugumo centras, gavęs informaciją apie kibernetinį incidentą, turi teisę:

20.1. patikslinti kibernetinio incidento kategoriją (priskirti didesnės ar mažesnės reikšmės kibernetinių incidentų kategorijai);

20.2. prašyti papildomos informacijos, reikalingos kibernetinio saugumo subjekto ryšių ir informacinės sistemos kibernetinio saugumo būsenai vertinti, nurodant informacijos pateikimo terminą.

21. Nacionalinis kibernetinio saugumo centras, įvertinęs gautą informaciją, patvirtina, patikslina arba savarankiškai priskiria kibernetinio incidento kategoriją, nustatytą Plano 10 punkte, ir ne vėliau kaip per 1 valandą nuo informacijos gavimo arba, jeigu kibernetinio saugumo subjekto prašoma papildomos informacijos, nuo papildomos informacijos gavimo informuoja apie tai pranešėją.

22. Kai būtina informuoti visuomenę siekiant išvengti kibernetinio incidento arba valdyti vykstantį kibernetinį incidentą, Nacionalinis kibernetinio saugumo centras, pasikonsultavęs su kibernetinio saugumo subjektu, pranešusiu apie kibernetinį incidentą, turi teisę informuoti visuomenę apie pavienius kibernetinius incidentus arba reikalauti, kad tai padarytų kibernetinio saugumo subjektas.

IV SKYRIUS
KIBERNETINIŲ INCIDENTŲ TYRIMAS

PIRMASIS SKIRSNIS
DIDELIO, VIDUTINIO IR NEREIKŠMINGO POVEIKIO KIBERNETINIŲ INCIDENTŲ TYRIMAS

23. Kibernetinio saugumo subjektai kibernetinių incidentų tyrimą atlieka vadovaudamiesi savo patvirtintais kibernetinio saugumo teisės aktais tiek, kiek to nereglamentuoja Planas, ir imasi visų įmanomų priemonių, būtinų kibernetiniam incidentui suvaldyti ir įprastai ryšių ir informacinių sistemų veiklai atkurti.

24. Kibernetinio saugumo subjektai Nacionaliniam kibernetinio saugumo centrui pateikia kibernetinio incidento tyrimo ataskaitą apie:

24.1. didelio poveikio kibernetinių incidentų valdymo būklę – ne vėliau kaip per 4 valandas nuo jų nustatymo ir ne rečiau kaip kas 4 valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;

24.2. vidutinio poveikio kibernetinių incidentų valdymo būklę – ne vėliau kaip per 24 valandas nuo jų nustatymo ir ne rečiau kaip kas 24 valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;

24.3. didelio ar vidutinio poveikio kibernetinių incidentų suvaldymą ar pasibaigimą – ne vėliau kaip per 4 valandas nuo jų suvaldymo ar pasibaigimo.

25. Nacionaliniam kibernetinio saugumo centrui teikiant didelio ar vidutinio poveikio kibernetinio incidento tyrimo ataskaitą nurodoma žinoma informacija:

25.1. kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Plano priede pateiktus kriterijus;

25.2. ryšių ir informacinės sistemos, kurioje nustatytas kibernetinis incidentas, tipas (elektroninių ryšių tinklas, informacinė sistema, registras, pramoninių procesų valdymo sistema, tarnybinė stotis ir panašiai);

25.3. kibernetinio incidento veikimo trukmė;

25.4. kibernetinio incidento šaltinis;

25.5. kibernetinio incidento požymiai;

25.6. kibernetinio incidento veikimo metodas;

25.7. galimos ir (ar) nustatytos kibernetinio incidento pasekmės;

25.8. kibernetinio incidento poveikio pasireiškimo (galimo išplitimo) mastas;

25.9. kibernetinio incidento būsena (aktyvus, pasyvus);

25.10. priemonės, kuriomis kibernetinis incidentas nustatytas;

25.11. galimos ir (ar) taikomos kibernetinio incidento valdymo priemonės;

25.12. tikslus laikas, kada bus teikiama informacija apie kibernetinio incidento valdymo būklę pagal Plano 24 punkte nustatytus reikalavimus.

26. Kibernetinio saugumo subjektai, įvertinę, kad negalės savarankiškai ištirti ar suvaldyti kibernetinio incidento per maksimaliai leistiną paslaugos neveikimo laiką, nustatytą savo patvirtintuose kibernetinio saugumo teisės aktuose, ne vėliau kaip per 24 val. nuo šių aplinkybių nustatymo kreipiasi pagalbos į Nacionalinį kibernetinio saugumo centrą.

27. Nacionalinis kibernetinio saugumo centras imasi būtinų veiksmų kibernetiniam incidentui ištirti ir visoms kibernetinio saugumo subjektų pranešime nurodytoms aplinkybėms išsiaiškinti:

27.1. didelio poveikio kibernetinių incidentų tyrimai pradedami nedelsiant tą pačią darbo dieną, kai gaunamas kibernetinio saugumo subjektų pranešimas;

27.2. vidutinio poveikio kibernetinių incidentų tyrimai pradedami tik atlikus didelio poveikio kibernetinių incidentų tyrimus arba ne vėliau kaip per 3 darbo dienas nuo kibernetinio saugumo subjektų pranešimo apie kibernetinį incidentą gavimo;

27.3. nereikšmingo poveikio kibernetiniai incidentai stebimi. Jei nereikšmingo poveikio kibernetiniai incidentai Plane nustatyta tvarka priskiriami didesnės reikšmės kibernetinių incidentų kategorijai, jie tiriami vadovaujantis Plane nustatytais reikalavimais.

28. Didelio ar vidutinio poveikio kibernetinių incidentų tyrimas baigiamas ir kibernetinis incidentas laikomas suvaldytu ar pasibaigusiu, kai išnyksta kibernetinio incidento poveikis ryšių ir informacinei sistemai ir (ar) atkuriama įprasta ryšių ir informacinių sistemų veikla, atitinkanti kriterijus, kuriuos kibernetinio saugumo subjektai nustato savo kibernetinio saugumo teisės aktuose.

29. Kibernetinio saugumo subjektai ne vėliau kaip per 8 valandas nuo kibernetinio incidento suvaldymo ar pasibaigimo informuoja ryšių ir informacinės sistemos teikiamų paslaugų gavėjus (jeigu tokių yra), jeigu kibernetinio incidento poveikis padarė arba gali ateityje padaryti žalos ryšių ir informacinės sistemos teikiamų paslaugų gavėjui.

30. Nacionalinis kibernetinio saugumo centras, gavęs iš kibernetinio saugumo subjekto tyrimo ataskaitą apie didelio ar vidutinio poveikio kibernetinių incidentų suvaldymą ar pasibaigimą, ne vėliau kaip per 1 darbo dieną nuo informacijos gavimo suveda gautą neįslaptintą informaciją į kibernetinio saugumo informacinį tinklą ir informuoja apie tai pranešėją.

ANTRASIS SKIRSNIS
PAVOJINGŲ KIBERNETINIŲ INCIDENTŲ TYRIMAS

31. Nacionalinis kibernetinio saugumo centras, priskyręs kibernetinį incidentą pavojingo kibernetinio incidento kategorijai, atsižvelgdamas į kibernetinio saugumo situaciją nedelsdamas, bet ne vėliau kaip per 24 val. nuo informacijos apie pavojingą kibernetinį incidentą gavimo informuoja kitas KIVT institucijas Plano 46.2–46.3 papunkčiuose nustatyta tvarka ir nurodo kibernetinio saugumo subjektams, kad pavojingas kibernetinis incidentas toliau turi būti tiriamas ir valdomas vadovaujantis kibernetinio saugumo subjekto patvirtintais teisės aktais, arba perima pavojingo kibernetinio incidento tyrimą ir (ar) valdymo organizavimą.

32. Kibernetinio saugumo subjektai, Nacionalinio kibernetinio saugumo centro nurodymu toliau tiriantys ir valdantys pavojingą kibernetinį incidentą, ne rečiau kaip kas 4 valandas teikia Nacionaliniam kibernetinio saugumo centrui atnaujintą informaciją apie pavojingo kibernetinio incidento valdymo būklę, kurią sudaro Plano 25 punkte nurodyta informacija. Nacionalinis kibernetinio saugumo centras, atsižvelgdamas į kibernetinio saugumo subjektų teikiamą informaciją, turi teisę perimti pavojingo kibernetinio incidento tyrimą ir (ar) valdymo organizavimą.

33. Nacionaliniam kibernetinio saugumo centrui perėmus tirti ir (ar) organizuoti pavojingo kibernetinio incidento valdymą, kibernetinio saugumo subjektai:

33.1. nuolat renka, apdoroja informaciją, susijusią su kibernetiniu incidentu, ir ne rečiau kaip kas 4 valandas ją teikia KIVT institucijoms pagal kompetenciją;

33.2. ne rečiau kaip kas 4 valandas teikia Nacionaliniam kibernetinio saugumo centrui informaciją apie atliktus kibernetinio incidento tyrimo ir (ar) valdymo veiksmus ir jų rezultatus, kurią sudaro Plano 25 punkte nurodyta informacija;

33.3. vykdo Nacionalinio kibernetinio saugumo centro nurodymus, susijusius su kibernetinio incidento tyrimu ir (ar) valdymo organizavimu, ir dalyvauja kibernetinio incidento valdymo procese, taikydami kibernetinio saugumo užtikrinimo priemones.

34. Nacionalinis kibernetinio saugumo centras, perėmęs kibernetinio incidento tyrimą ir (ar) valdymo organizavimą, imasi būtinų veiksmų kibernetiniam incidentui ištirti ir visoms kibernetinio saugumo subjektų nurodytoms aplinkybėms išsiaiškinti:

34.1. vertina kibernetinio saugumo subjektų pateiktą informaciją apie kibernetinį incidentą;

34.2. priima sprendimus dėl kibernetinio incidento tyrimo ir (ar) valdymo;

34.3. duoda kibernetinio saugumo subjektams nurodymus, susijusius su kibernetinio incidento tyrimu ir (ar) valdymu;

34.4. turi teisę surengti koordinacinį pasitarimą dėl kibernetinio incidento tyrimo ir (ar) valdymo, kuriame privalo dalyvauti suinteresuotų KIVT institucijų atstovai, kibernetinio saugumo subjektų paskirti kompetentingi asmenys, atsakingi už kibernetinio saugumo organizavimą ir užtikrinimą, ir kiti kibernetinio saugumo subjektų atstovai, kuriems būtina

dalyvauti, siekiant suvaldyti kibernetinį incidentą. Nacionalinis kibernetinio saugumo centras turi teisę į koordinacinį pasitarimą pakviesti kitų kompetentingų ekspertų.

35. Tuo pačiu metu vykstant keliems pavojingiems kibernetinio saugumo incidentams, Nacionalinis kibernetinio saugumo centras pirmiausia tiria ir valdo tuos pavojingus kibernetinius incidentus, kurių sukeliama žala gali būti ar yra didžiausia.

36. 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.

37. Nacionalinis kibernetinio saugumo centras apie pavojingo kibernetinio incidento nustatymą, pavojingo kibernetinio incidento tyrimo ir (ar) valdymo veiksmų eigą nedelsdamas, bet ne vėliau kaip per 1 valandą nuo pavojingo kibernetinio incidento nustatymo informuoja Lietuvos Respublikos krašto apsaugos ministerijos, Vyriausybės kanceliarijos, Lietuvos Respublikos Seimo (toliau – Seimas) kanceliarijos ir Lietuvos Respublikos Prezidento (toliau – Prezidentas) kanceliarijos paskirtus atsakingus asmenis ir ne vėliau kaip per 4 valandas nuo pavojingo kibernetinio incidento nustatymo pateikia jiems apibendrintą pavojingų kibernetinių incidentų tyrimo ataskaitą, kurią sudaro Plano 25 punkte nurodyta informacija.

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

39. Nacionalinis kibernetinio saugumo centras apie pavojingo kibernetinio incidento tyrimą ir (ar) valdymą reguliariai, bet ne rečiau kaip kas 4 valandas informuoja Plano 37 punkte nurodytus informacijos gavėjus, pateikdamas atnaujintą pavojingų kibernetinių incidentų tyrimo ataskaitą, o informaciją apie pavojingo kibernetinio incidento suvaldymą ar pasibaigimą šiems gavėjams ir kibernetinio saugumo subjektui pateikia ne vėliau kaip per 1 valandą suvaldžius pavojingą kibernetinį incidentą ar jam pasibaigus. Pavojingo kibernetinio incidento tyrimas baigiamas ir kibernetinis incidentas laikomas suvaldytu ar pasibaigusiu, kai išnyksta kibernetinio incidento poveikis ryšių ir informacinei sistemai ir (ar) atkuriama įprasta ryšių ir informacinių sistemų veikla, atitinkanti kriterijus, kuriuos kibernetinio saugumo subjektai nustato savo kibernetinio saugumo teisės aktuose.

40. Nacionalinis kibernetinio saugumo centras ne vėliau kaip per 1 darbo dieną nuo pavojingo kibernetinio incidento suvaldymo ar pasibaigimo suveda pavojingų kibernetinių incidentų tyrimo ataskaitos neįslaptintą informaciją į kibernetinio saugumo informacinį tinklą.

41. Nacionalinis kibernetinio saugumo centras, nustatęs, kad nepakanka turimų KIVT institucijų ir kibernetinio saugumo subjektų išteklių pavojingam kibernetiniam incidentui ištirti ir (ar) suvaldyti, nedelsdamas, bet ne vėliau kaip per 1 valandą nuo šių aplinkybių nustatymo informuoja Krašto apsaugos ministerijos ir Vyriausybės kanceliarijos paskirtus

atsakingus asmenis, taip pat krašto apsaugos ministrą, o šis ne vėliau kaip per 24 val. priima sprendimą dėl pavojingo kibernetinio incidento tyrimo ir (ar) valdymo priemonių.

42. Pavojingo kibernetinio incidento nesuvaldžius krašto apsaugos ministro skirtomis papildomomis priemonėmis, Nacionalinis kibernetinio saugumo centras nedelsdamas, bet ne vėliau kaip per 1 valandą nuo šios aplinkybės nustatymo informuoja apie tai krašto apsaugos ministrą ir Vyriausybės kanceliarijos paskirtą atsakingą asmenį, pateikdamas pavojingų kibernetinių incidentų tyrimo ataskaitą.

43. Krašto apsaugos ministras ne vėliau kaip per 24 val. nuo Plano 41 punkte nurodytos informacijos gavimo teikia Vyriausybei pasitarimo protokolo projektą, kuriuo siūloma kibernetinį incidentą pripažinti kibernetinio saugumo krize.

TREČIASIS SKIRSNIS
TARPINSTITUCINIS BENDRADARBIAVIMAS IR KEITIMASIS INFORMACIJA TIRIANT KIBERNETINIUS INCIDENTUS

44. KIVT institucijos, nustačiusios, kad kibernetinio saugumo subjekto ryšių ir informacinėse sistemose galimai vyksta kibernetinis incidentas, nedelsdamos, bet ne vėliau kaip per 4 val. nuo šių aplinkybių nustatymo informuoja kibernetinio saugumo subjektą.

45. Kibernetinio saugumo subjektai, iš KIVT 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, imasi veiksmų, reikalingų kibernetiniam incidentui nustatyti ir patvirtinti. Nenustačius kibernetinio incidento požymių, kibernetinio saugumo subjektai KIVT institucijas apie tai informuoja ne vėliau kaip per 4 valandas nuo pranešimo apie kibernetinį incidentą gavimo.

46. KIVT institucija, gavusi informaciją apie kibernetinį incidentą, nedelsdama, bet ne vėliau kaip per 24 val. nuo informacijos apie kibernetinį incidentą gavimo informuoja kitas KIVT institucijas:

46.1. Nacionalinį kibernetinio saugumo centrą – nustačiusi, kad kibernetinis incidentas taip pat gali paveikti kibernetinio saugumo subjektų ryšių ir informacines sistemas;

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

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

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

48. Kibernetinio saugumo subjektai ir KIVT institucijos šiame Plane nurodytą informaciją, susijusią su kibernetiniais incidentais ir jų valdymu, perduoda per kibernetinio

saugumo informacinį tinklą, o jeigu tokios galimybės nėra, kitomis saugiomis informacijos perdavimo priemonėmis.

49. Valstybės saugumo departamento prašymu Nacionalinis kibernetinio saugumo centras ne vėliau kaip per 7 darbo dienas nuo tokio prašymo gavimo informuoja Valstybės saugumo departamento paskirtą atsakingą asmenį apie įvykusius didelės reikšmės ir pavojingus kibernetinius incidentus per kibernetinio saugumo informacinį tinklą, o jeigu tokios galimybės nėra, kitomis saugiomis informacijos perdavimo priemonėmis.

50. KIVT institucijos, gavusios iš kitų valstybių arba tarptautinių organizacijų ar institucijų, atliekančių kibernetinio saugumo užtikrinimo funkcijas, informaciją apie kitose valstybėse įvykusius kibernetinius incidentus, kurie galėtų būti klasifikuojami kaip didelio poveikio ar pavojingi, nedelsdamos, bet ne vėliau kaip per 1 valandą nuo kibernetinio incidento aplinkybių sužinojimo pateikia informaciją apie kibernetinį incidentą kibernetinio saugumo subjektams, kuriuos gali paveikti kitose valstybėse įvykęs kibernetinis incidentas.

KETVIRTASIS SKIRSNIS
TARPTAUTINIS BENDRADARBIAVIMAS IR KEITIMASIS INFORMACIJA TIRIANT KIBERNETINIUS INCIDENTUS

51. Nacionalinis kibernetinio saugumo centras koordinuoja pasikeitimą duomenimis ir informacija, perduodama tarp kitų valstybių arba tarptautinių organizacijų ar institucijų, atliekančių kibernetinio saugumo užtikrinimo funkcijas, KIVT institucijų ir kibernetinio saugumo subjektų.

52. Nacionalinis kibernetinio saugumo centras, koordinuodamas tarptautinio ir tarpinstitucinio bendradarbiavimo veiksmus:

52.1. užtikrina tarpvalstybinį valstybių narių institucijų bendradarbiavimą ir bendradarbiavimą su kitų valstybių narių 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 subjektų;

52.2. informuoja Europos Komisiją apie kibernetinių incidentų valdymo proceso mastą ir pagrindinius elementus ir kiekvienais metais bendradarbiavimo grupei pateikia suvestinę ataskaitą apie gautus pranešimus, kurioje, be kita ko, nurodomas pranešimų skaičius ir incidentų, apie kuriuos pranešta, pobūdis, taip pat veiksmai, kurių buvo imtasi;

52.3. informuoja kitas Europos Sąjungos valstybes nares, jų CSIRT apie pavojingus ir didelio poveikio kibernetinius incidentus, kai gali būti paveiktas daugiau negu vienos valstybės narės ypatingos svarbos informacinės infrastruktūros paslaugų teikimas;

52.4. teikia su kibernetiniu saugumu susijusius išankstinius įspėjimus, perspėjimus ir rekomendacijas suinteresuotiems subjektams.

53. Koordinuodamas tarptautinio ir tarpinstitucinio bendradarbiavimo veiksmus, Nacionalinis kibernetinio saugumo centras kibernetinio saugumo subjektų pateikta

informacija, įskaitant ir konfidencialią informaciją, turi teisę keistis tik tiek, kiek tai yra būtina tarptautinio ir tarpinstitucinio bendradarbiavimo koordinavimui, ir užtikrina gautos informacijos apsaugą.

54. Krašto apsaugos ministrui pritarus, Nacionalinis kibernetinio saugumo centras, atlikdamas Plane nustatytas funkcijas, turi teisę pasitelkti tarptautinių organizacijų kompetentingas institucijas, jų įsteigtas bendradarbiavimo grupes ir užsienio valstybių kompetentingas institucijas bei tarnybas. Už pasitelktų tarptautinių organizacijų kompetentingų institucijų, jų įsteigtų bendradarbiavimo grupių ir užsienio valstybių kompetentingų institucijų bei tarnybų veiklą atsako Nacionalinis kibernetinio saugumo centras.

V SKYRIUS
KIBERNETINIŲ INCIDENTŲ ANALIZĖ BAIGUS KIBERNETINIŲ INCIDENTŲ TYRIMĄ

55. Kibernetinio saugumo subjektai ir KIVT institucijos po kibernetinio incidento suvaldymo ar pasibaigimo pagal kompetenciją atlieka jo analizę.

56. Kibernetinio saugumo subjektas, kurio ryšių ir informacinėje sistemoje tirtas kibernetinis incidentas, išanalizavęs ir įvertinęs visą informaciją, susijusią su kibernetiniu incidentu, atliktus veiksmus ir panaudotas priemones:

56.1. ne vėliau kaip per 30 darbo dienų pateikia kibernetinio incidento analizės rezultatus Nacionaliniam kibernetinio saugumo centrui ir kibernetinio saugumo informaciniame tinkle paskelbia susistemintą ir aktualią neįslaptintą informaciją apie kibernetinio incidento nustatymą ir suvaldymą;

56.2. imasi priemonių, kad būtų pašalintas ryšių ir informacinės sistemos pažeidžiamumas;

56.3. įvertina ryšių ir informacinės sistemos riziką ir (ar) atitiktį Vyriausybės nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams;

56.4. nustačius teisinio reglamentavimo spragų, inicijuoja savo kibernetinio saugumo teisės aktų pakeitimus.

57. KIVT institucijos turi teisę reikalauti kibernetinio saugumo subjektų ne vėliau kaip per 30 darbo dienų pateikti papildomą informaciją, reikalingą kibernetinio incidento analizei atlikti.

58. KIVT institucijos, išanalizavusios ir įvertinusios visą informaciją, susijusią su įvykusiu kibernetiniu incidentu, atliktus veiksmus ir panaudotas priemones:

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

58.2. prireikus pakeičia (inicijuoja pakeitimus) ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planą;

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

59. Nacionalinis kibernetinio saugumo centras, atlikęs kibernetinio incidento analizę arba gavęs kibernetinio incidento analizės rezultatus iš kibernetinio saugumo subjekto ar KVIT institucijų, naudingą apibendrintą neįslaptintą informaciją apie atliktą kibernetinio incidento analizę ne vėliau kaip per 30 darbo dienų nuo šios informacijos gavimo paskelbia kibernetinio saugumo informaciniame tinkle arba savo interneto svetainėje.

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

Krašto apsaugos viceministras
Edvinas Kerza

KAM Administracijos departamento
Dokumentų administravimo skyriaus
vyr. specialistė
Vesta Adomaitienė

Krašto apsaugos ministerijos
Teisės departamento direktorė
Judita Nagienė

Nacionalinio kibernetinių incidentų valdymo plano priedas

KIBERNETINIŲ INCIDENTŲ KATEGORIJŲ SĄRAŠAS

Eil. Nr.	Incidento grupės	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)		
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	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	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	Sutrikdomas (gali sutrikti) paslaugų veikimas visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų sąraše
1.	Nepageidaujamų laiškų, klaidinančios ar žeidžiančios informacijos platinimas (angl. *abusive content*, *spam*)	Nepageidaujami laiškai ir (ar) klaidinančios, žeidžiančios informacijos platinimas trikdo ryšių ir informacinės sistemos (toliau – RIS) veiklą ir (ar) teikiamas paslaugas	N				V					D					P		
		Nepageidaujamų laiškų ir (ar) klaidinančios, žeidžiančios informacijos platinimas	N																
2.	Kenkimo programinė įranga	Aptikta moderni kenkimo					V					D					P		

Eil. Nr.	Incidento grupės	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)		
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	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	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	Sutrikdomas (gali sutrikti) paslaugų veikimas visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų sąraše
	(angl. *malicious software / code*) Programinė įranga ar jos dalis, kuri padeda neteisėtai prisijungti prie RIS, ją užvaldyti ir kontroliuoti, sutrikdyti ar pakeisti jų veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę ja naudotis ir neteisėtai pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims	programinė įranga (angl. *advanced persistent threat, APT*)																	
		RIS aktyviai kontroliuojama įsibrovėlių (pavyzdžiui, „galinės durys (angl. *back door*), kompiuterizuotos darbo vietos ar tarnybinės stotys tampa „Botinklo“ (angl. *Botnet*) infrastruktūros dalimi					V					D					P		
		Kenkimo programinė įranga, trikdanti saugumo priemonių darbą					V					D					P		
		Kenkimo programinė įranga, kurią aptinka saugumo priemonės per reguliarų patikrinimą ir (ar) kurią saugumo priemonės automatiškai blokuoja	N				V												
		Kenkimo programinė įranga,	N				V					D					P		

Eil. Nr.	Incidento grupės	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)		
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	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	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	Sutrikdomas (gali sutrikti) paslaugų veikimas visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų sąraše
		platinama naudojant socialinės inžinerijos metodus																	
3.	Informacijos rinkimas (angl. *information gathering*) Žvalgyba ar kita įtartina veikla (angl. *scanning, sniffing*), manipuliavimas naudotojų emocijomis, psichologija, pastabumo stoka, pasinaudojimas technologiniu neišmanymu (angl. *social engineering*), siekiant stebėti ir rinkti informaciją, atrasti silpnąsias vietas, atlikti grėsmę keliančius veiksmus, apgavystės, siekiant įtikinti	RIS paketų / informacijos perėmimas					V					D					P		
		RIS klastojimas, siekiant surinkti prisijungimo ar kitą svarbią informaciją, tiksliniai laiškai, kuriuose, pasinaudojant socialinės inžinerijos principais, siekiama išvilioti prisijungimo ir (ar) kitą svarbią informaciją, priversti atlikti norimus veiksmus (pvz., finansines operacijas)					V					D					P		
		Vykdoma perimetro priemonių žvalgyba (nebandant įsilaužti)	N				V												
		Naudojami socialinės inžinerijos metodai, siekiant išvilioti	N				V												

Eil. Nr.	Incidento grupės	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)			
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	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	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	Sutrikdomas (gali sutrikti) paslaugų veikimas visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų sąraše
	naudotoją atskleisti informaciją (angl. *phishing*) arba atlikti norimus veiksmus	prisijungimo prie RIS ir (ar) kitą svarbią informaciją																
4.	Mėginimas įsilaužti (angl. *intrusion attempts*) Mėginimas įsilaužti arba sutrikdyti RIS veikimą išnaudojant žinomus pažeidžiamumus (angl. *exploiting of known vulnerabilities*), bandant parinkti slaptažodžius (angl. *login attempts*), kitą įsilaužimo būdą (angl. *new attack signature*)	Išnaudojamas vienas ar keli nežinomi (angl. *zero day*) pažeidžiamumai, siekiant tikslingai sutrikdyti konkrečią RIS					V					D					P			
		Išnaudojamas vienas ar keli nežinomi (angl. *zero day*) pažeidžiamumai	N				V					D					P			
		Vidinė RIS žvalgyba ar kita kenkimo veika (prievadų skenavimas, slaptažodžių parinkimas, kenkimo programinės įrangos platinimas ir kita)					V					D					P			
		Išnaudojami žinomi ir viešai publikuoti pažeidžiamumai arba	N				V													

Eil. Nr.	Incidento grupės	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)		
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	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	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	Sutrikdomas (gali sutrikti) paslaugų veikimas visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų sąraše
		atliekami bandymai prisijungti prie RIS parenkant slaptažodžius																	
5.	Įsilaužimas (angl. *intrusions*) Sėkmingas įsilaužimas ir (ar) neteisėtas RIS, taikomosios programinės įrangos ar paslaugos naudojimas (angl. *privileged account compromise, unprivileged account compromise, application compromise*)	Veiksmai prieš RIS ar jos saugumo priemones, informacijos pasisavinimas, naikinimas, RIS ar jos dalies pažeidimas, sutrikdantis RIS teikiamų paslaugų nepertraukiamą teikimą, galintis turėti įtakos tvarkomos informacijos ir teikiamų paslaugų patikimumui, iškreipti turinį ir mažinti RIS naudotojų pasitikėjimą jais					V					D					P		
		Gaunama neteisėta prieiga prie RIS, taikomosios programinės įrangos ar paslaugos					V					D					P		
6.	Paslaugų trikdymas,	Teikiamų paslaugų nutraukimas arba					V					D					P		

Eil. Nr.	Incidento grupės	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)		
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	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	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	Sutrikdomas (gali sutrikti) paslaugų veikimas visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų sąraše
	prieinamumo pažeidimai (angl. *availability*) Veiksmai, kuriais trikdoma RIS veikla, teikiamos paslaugos (angl. *DoS, DDoS*), RIS ar jos dalies pažeidimas, sutrikdantis RIS ir (ar) jos teikiamas paslaugas (angl. *sabotage, outage*)	maksimalaus leistino paslaugos neveikimo laiko viršijimas																	
		Teikiamų paslaugų nepertraukiamo teikimo trikdymas, galintis turėti įtakos tvarkomos informacijos ir (ar) teikiamų paslaugų prieinamumui	N				V												
		Aptinkamas paslaugos trikdymas, kuris neturi įtakos paslaugų teikimui	N				V												
7.	Informacijos turinio saugumo pažeidimai (angl. *information content security*) Neteisėta prieiga prie informacijos, neteisėtas informacijos keitimas (angl. *unauthorised access to*	Neteisėta prieiga prie informacijos, galinčios turėti įtakos RIS veiklai ir (ar) teikiamoms paslaugoms					V					D					P		
		Neteisėta prieiga prie informacijos, neteisėtas informacijos keitimas	N				V					D					P		

Eil. Nr.	Incidento grupės	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)		
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	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	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	Sutrikdomas (gali sutrikti) paslaugų veikimas visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų sąraše
	information, unauthorised modification of information)																		
8.	Neteisėta veikla, sukčiavimas (angl. *fraud*) Vagystė, apgavystė, neteisėtas išteklių (angl. *unauthorized use of resources*), nelegalios programinės įrangos ar autorių teisių (angl. *copyright*) naudojimas, tapatybės klastojimo, apgavystės ir kiti panašaus pobūdžio incidentai	Neteisėta įtaka RIS veiklai ir (ar) teikiamoms paslaugoms	N				V					D					P		
9.	Kita Incidentai, kurie neatitinka nei vienos iš nurodytų grupių aprašymų		N				V					D					P		

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

KAM Administracinio departamento
Dokumentų administravimo skyriaus
vyr. specialistė
Vesta Adomaitienė

Krašto apsaugos ministerijos
Teisės departamento direktorė
Judita Nagienė

Krašto apsaugos viceministras
Edvinas Kerza