LIETUVOS RESPUBLIKOS VYRIAUSYBĖS KANCELIARIJA
VIEŠOJO VALDYMO IR SOCIALINĖS APLINKOS DEPARTAMENTO
INFORMACINĖS VISUOMENĖS SKYRIUS

PAŽYMA

DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL NACIONALINIO KIBERNETINIŲ INCIDENTŲ VALDYMO PLANO PATVIRTINIMO“ PROJEKTO (NR. 15-0635-02-N) (TAIS NR. 15-6282(6))

2016 01 18 Nr. NV-168

Vilnius

1. **Projekto rengėja:** Krašto apsaugos ministerija.
2. **Projekto tikslas, esmė.** Nutarimo projekto tikslas – įgyvendinant Kibernetinio saugumo įstatymą, reglamentuoti nacionalinę kibernetinio saugumo incidentų valdymo sistemą, t. y. nustatyti kibernetinio saugumo politiką įgyvendinančių institucijų, kitų viešojo administravimo subjektų, valdančių ir (arba) tvarkančių valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų veikas, atliekamas siekiant suvaldyti kibernetinius incidentus, galinčius sutrikdyti ar sutrikdančius valstybės informacinių išteklių, ypatingos svarbos informacinės infrastruktūros ir (ar) kitų elektroninių ryšių tinklų ir (ar) informacinių sistemų darbą ir taip sukeliančius grėsmę nacionaliniam saugumui, žmonių sveikatai ar gyvybei, visuomenės gerovei ar valstybės funkcijų atlikimui, taip pat nustatyti tarpinstitucinę kibernetinių incidentų valdymo sąveiką, kibernetinių incidentų klasifikavimo tvarką ir tarpinstitucinį bendradarbiavimą tiriant kibernetinius incidentus.

Nustatoma, kad už kibernetinių incidentų valdymą bus atsakingi Nacionalinis kibernetinio saugumo centras ir Ryšių reguliavimo tarnyba. Siūloma įteisinti informavimo apie kibernetinius incidentus tvarką ir patvirtinti, kad įvykus kibernetiniam incidentui informacija apie jį keičiamasi kibernetinio saugumo informaciniame tinkle ir šį incidentą iš pradžių bando valdyti tvarkytojas. Jeigu nepakanka išteklių incidentui suvaldyti, jo valdymą pagal kompetenciją perima Nacionalinis kibernetinio saugumo centras arba Ryšių reguliavimo tarnyba. Jeigu išteklių incidentui suvaldyti vis dar trūktų, informuojamas krašto apsaugos ministras, o, pavojingo kibernetinio incidento nesuvaldžius per maksimalų leistiną terminą, sprendimą dėl tolesnio jo valdymo priima Vyriausybė. Prireikus informuojami Seimas ir Respublikos Prezidento kanceliarija.

3. **Derinimas.** Nutarimo projektas derintas su Energetikos ministerija, Finansų ministerija, Lietuvos banku, Policijos departamentu prie Vidaus reikalų ministerijos, Ryšių reguliavimo tarnyba, Susisiekimo ministerija, Valstybine duomenų apsaugos inspekcija, Vidaus reikalų ministerija, Ūkio ministerija, Teisingumo ministerija ir visuomene.

Nutarimo projektas svarstytas 2015 m. rugsėjo 1 d. ir 2015 m. gruodžio 1 d. ministerijų atstovų pasitarimuose ir patikslintas pagal pasitarimuose pateiktas pastabas. Papildomai patikslintas nutarimo projektas derintas su Valstybės saugumo departamentu, Respublikos Prezidento kanceliarija ir Seimo kanceliarija.

Dėl pastabų ir pasiūlymų, į kuriuos neatsižvelgta arba atsižvelgta iš dalies, pridedama nutarimo projekto derinimo pažyma.

4. **Dalykinio vertinimo išvada.**

Teikiamas projektas iš esmės atitinka Vyriausybės darbo reglamento reikalavimus.

Edmundas Kazakevičius, tel. 8 706 63 889, el. p. edmundas.kazakevicius@lrv.lt

LIETUVOS RESPUBLIKOS KRAŠTO APSAUGOS MINISTERIJA

Biudžetinė įstaiga, Totorių g. 25, LT-01121 Vilnius, tel.: (8 5) 273 5501 / 262 4821, faks. (8 5) 264 8517, el. p. kam@kam.lt.
Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 188602751, PVM mokėtojo kodas LT100001016116

Lietuvos Respublikos Vyriausybei 2016-01-13 Nr. 12-01-80

DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO PROJEKTO

Lietuvos Respublikos krašto apsaugos ministerija, atsižvelgdama į 2015 m. gruodžio 1 d. ministerijų atstovų pasitarime Vyriausybės kanceliarijos Teisės departamento ir Viešojo valdymo ir socialinės aplinkos departamento Informacinės visuomenės skyriaus pateiktas pastabas, patikslino ir pakartotinai teikia Lietuvos Respublikos Vyriausybės nutarimo „Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“ projektą (toliau – Nutarimo projektas).

Nutarimo projekto tikslas – įgyvendinant Įstatymą, nustatyti nacionalinę kibernetinio saugumo incidentų valdymo sistemą, t. y. nustatyti kibernetinio saugumo politiką įgyvendinančių institucijų, kitų viešojo administravimo subjektų, valdančių ir (arba) tvarkančių valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų veikas, atliekamas siekiant suvaldyti kibernetinius incidentus, galinčius sutrikdyti ar sutrikdančius valstybės informacinių išteklių, ypatingos svarbos informacinės infrastruktūros ir (ar) kitų elektroninių ryšių tinklų ir (ar) informacinių sistemų darbą ir taip sukeliančius grėsmę nacionaliniam saugumui, žmonių sveikatai ar gyvybei, visuomenės gerovei ar valstybės funkcijų vykdymui, taip pat nustatyti tarpinstitucinę kibernetinių incidentų valdymo sąveiką, kibernetinių incidentų klasifikavimo tvarką ir tarpinstitucinį bendradarbiavimą tiriant kibernetinius incidentus.

Nutarimo projekto numatomo teisinio reguliavimo poveikis pateikiamas vertinimo pažymoje.

Nutarimo projektas neperkelia Europos Sąjungos teisės aktų ir atitinka Lietuvos Respublikos Vyriausybės programą.

Nutarimo projektas paskelbtas Lietuvos Respublikos Seimo teisės aktų informacinėje sistemoje.

Dėl pastabų, į kurias neatsižvelgta, teikiama derinimo pažyma. Dėl Viešojo valdymo ir socialinės aplinkos departamento Informacinės visuomenės skyriaus 2015 m. lapkričio 24 d. išvadoje Nr. NV-3771 pateiktos pastabos (4.5 p.) patikslintas Nutarimo projekto 33 p. darbo tvarka suderintas su Valstybės saugumo departamentu.

Nutarimo projektą parengė Krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų departamento (direktorius Arvydas Plėštys, tel. 8 706 80 800) Kibernetinio saugumo ir elektroninės informacijos saugos skyriaus (vedėjas plk. ltn. Artūras Litvaitis, tel. 8 706 80 806) vyriausiasis specialistas Miroslavas Tribockis (tel. 8 706 80 807, el. paštas miroslavas.tribockis@kam.lt).

PRIDEDAMA:

1. Lietuvos Respublikos Vyriausybės nutarimo „Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“ projektas, 11 lapų.
2. Nutarimo projekto numatomo teisinio reguliavimo poveikio vertinimo pažyma, 2 lapai.
3. Nutarimo projekto derinimo pažyma, 5 lapai.

2

4. Lietuvos Respublikos Vyriausybės kanceliarijos Teisės departamento 2015 m. lapkričio 26 d. išvados Nr. NV-3781 kopija, 2 lapai.

5. Lietuvos Respublikos Vyriausybės kanceliarijos Viešojo valdymo ir socialinės aplinkos departamento Informacinės visuomenės skyriaus 2015 m. lapkričio 24 d. išvados Nr. NV-3771 kopija, 2 lapai.

Krašto apsaugos ministras Juozas Olekas

Miroslavas Tribockis tel. 8 706 80 807, el. paštas miroslavas.tribockis@kam.lt

Projektas

LIETUVOS RESPUBLIKOS VYRIAUSYBĖ

NUTARIMAS DĖL NACIONALINIO KIBERNETINIŲ INCIDENTŲ VALDYMO PLANO PATVIRTINIMO

2016 m. d. Nr.
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 šių asmenų kontaktinę informaciją ne vėliau kaip per 10 darbo dienų nuo šio nutarimo įsigaliojimo dienos pateikti Kibernetinio saugumo ir telekomunikacijų tarnybai prie Krašto apsaugos ministerijos;

2.2. Valstybinę duomenų apsaugos inspekciją, Policijos departamentą prie 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 Vidaus reikalų ministerijos, Kibernetinio saugumo ir telekomunikacijų tarnybos prie Krašto apsaugos ministerijos ir šių asmenų kontaktinę informaciją ne vėliau kaip per 10 darbo dienų nuo šio nutarimo įsigaliojimo dienos pateikti minėtoms institucijoms.

3. Rekomenduoti:

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 Vidaus reikalų ministerijos, Kibernetinio saugumo ir telekomunikacijų tarnybos prie Krašto apsaugos ministerijos ir šių asmenų kontaktinę informaciją ne vėliau kaip per 10 darbo dienų nuo šio nutarimo įsigaliojimo dienos pateikti minėtoms institucijoms.

3.2. Valstybės saugumo departamentui paskirti asmenį, kuriam Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka būtų pateikiama informacija apie kibernetinius incidentus,

ir šio asmens kontaktinę informaciją ne vėliau kaip per 10 darbo dienų nuo šio nutarimo įsigaliojimo dienos pateikti Kibernetinio saugumo ir telekomunikacijų tarnybai prie Krašto apsaugos ministerijos;

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 šių asmenų kontaktinę informaciją ne vėliau kaip per 10 darbo dienų nuo šio nutarimo įsigaliojimo dienos pateikti Kibernetinio saugumo ir telekomunikacijų tarnybai prie Krašto apsaugos ministerijos.

Ministras Pirmininkas

Krašto apsaugos ministras

Juozas Olekas
Krašto apsaugos ministras

5

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2016 m. d. nutarimu Nr.

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 vykdymui, taip pat tarpinstitucinę kibernetinių incidentų valdymo sąveiką, kibernetinių incidentų klasifikavimo tvarką ir tarpinstitucinį bendradarbiavimą tiriant kibernetinius incidentus.

2. Plane vartojamos sąvokos atitinka 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 vartojamas sąvokas.

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 identifikuotas 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 identifikuotas 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, jei identifikuotas 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 val.;

8.2. gali visiškai sutrikdyti (arba visiškai sutrikdo) RIS veiklą ir taip gali sutrikdyti (sutrikdo) RIS teikiamų paslaugų teikimą maksimalų 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, iš tvarkytojo, ypatingos svarbos informacinės infrastruktūros valdytojo, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjo ar elektroninės informacijos prieglobos paslaugų teikėjo gavę informaciją apie identifikuotą 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, IDENTIFIKAVIMAS 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, vykdančių kibernetinio saugumo užtikrinimo funkcijas, gavę

informacijos apie galimą kibernetinį incidentą jų tvarkomose ar valdomose RIS, nedelsdami imasi veiksmų, reikalingų kibernetiniam incidentui patvirtinti ir identifikuoti.

12. KIVT institucijos 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 pateikia nedelsdamos, bet ne vėliau kaip per 30 minučių nuo kibernetinio incidento aplinkybių aptikimo.

13. Tvarkytojai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai ir elektroninės informacijos prieglobos paslaugų teikėjai, identifikavę kibernetinį incidentą, apie šį faktą informuoja KIVT institucijas pagal jų kompetenciją, naudodami kibernetinio saugumo informacinį tinklą ar kitas informacijos perdavimo priemones (paštu, el. paštu, telefonu, per pasiuntinius ir pan.).

14. Tvarkytojai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai ir elektroninės informacijos prieglobos paslaugų teikėjai, identifikavę 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, reikalingas 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, apie kibernetinio incidento identifikavimo faktą nedelsdama informuoja 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 maksimalų leistiną neveikimo terminą, pirmiausia pagalbos kreipiasi į Nacionalinį kibernetinio saugumo centrą, o viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų ir (arba) elektroninės informacijos prieglobos paslaugų teikėjai ir gavėjai, jei 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 jų 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 kitus kompetentingus ekspertus.

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 didžiausia.

24. Ryšių reguliavimo tarnyba apie pavojingo kibernetinio incidento identifikavimą ir pavojingo kibernetinio incidento valdymo veiksmų eigą nedelsdama, bet ne vėliau kaip per 1 valandą nuo pavojingo kibernetinio incidento identifikavimo, 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 identifikavimą ir pavojingo kibernetinio incidento valdymo veiksmų eigą nedelsdamas, bet ne vėliau kaip per 1 valandą nuo pavojingo kibernetinio incidento identifikavimo, informuoja Ryšių reguliavimo tarnybą, Lietuvos Respublikos krašto apsaugos ministerijos (toliau – Krašto apsaugos

ministerija), 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 kartą per 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 1 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 Krašto apsaugos ministerijos ir Vyriausybės kanceliarijos paskirtus asmenis, taip pat nedelsdamas informuoja krašto apsaugos ministrą, kuris 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, vykdančias kibernetinio saugumo užtikrinimo funkcijas ir su kuriomis bendradarbiaujama kibernetinio saugumo srityje, ir pateikti informaciją, susijusią su kibernetiniu incidentu.

12

33. Nacionalinis kibernetinio saugumo centras apie Plano 5.25.1–5.45.3 papunkčiuose nustatytus kibernetinius incidentus nedelsdamas, bet ne vėliau kaip per 1 valandą nuo pavojingo kibernetinio incidento identifikavimo ir nuo Plano 5.25.2–5.45.3 papunkčiuose nustatytų kibernetinių incidentų informacijos gavimo, apie kibernetinius incidentus informuoja Valstybės saugumo departamento paskirtą asmenį.

34. Pavojingo kibernetinio incidento nesuvaldžius per maksimalų 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, kuri 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 jų 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 identifikuotas 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 institucijoms pareikalavus, pateikia papildomą informaciją, reikalingą kibernetiniam incidentui tirti;

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

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

37.6. ne vėliau kaip per 8 valandas nuo kibernetinio incidento suvaldymo informuoja RIS teikiamų paslaugų gavėjus (jei tokių yra), jei kibernetinio incidento poveikis padarė arba gali ateityje padaryti žalą 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, tarp KIVT institucijų, elektroniniu būdu per kibernetinio saugumo informacinį tinklą, o jei tokios galimybės nėra – kitomis saugiomis informacijos perdavimo priemonėmis.

39. KIVT institucija, pagal savo 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.

Krašto apsaugos ministerijos
Teisės departamento direktorė
Judita Nagienė

Juozas Olekas
Krašto apsaugos ministras

14

NUMATOMO TEISINIO REGULIAVIMO POVEIKIO VERTINIMO PAŽYMA

Projekto pavadinimai	Lietuvos Respublikos Vyriausybės nutarimo „Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“ projektas (toliau – Nutarimo projektas).
Projekto rengėjas	Lietuvos Respublikos krašto apsaugos ministerija.
Projekto tikslas	Nutarimo projekto tikslas – įgyvendinant Lietuvos Respublikos kibernetinio saugumo įstatymą, nustatyti nacionalinę kibernetinio saugumo incidentų valdymo sistemą, t. y. nustatyti kibernetinio saugumo politiką įgyvendinančių institucijų, kitų viešojo administravimo subjektų, valdančių ir (arba) tvarkančių valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų veikas, atliekamas siekiant suvaldyti kibernetinius incidentus, galinčius sutrikdyti ar sutrikdančius valstybės informacinių išteklių, ypatingos svarbos informacinės infrastruktūros ir (ar) kitų elektroninių ryšių tinklų ir (ar) informacinių sistemų darbą ir taip sukelti grėsmę nacionaliniam saugumui, žmonių sveikatai ar gyvybei, visuomenės gerovei ar valstybės funkcijų vykdymui, taip pat nustatyti tarpinstitucinę kibernetinių incidentų valdymo sąveiką, kibernetinių incidentų klasifikavimo tvarką ir tarpinstitucinį bendradarbiavimą tiriant kibernetinius incidentus.
	Siūlomo projekto poveikio įvertinimas (teigiamos ir (ar) neigiamos pasekmės)
Poveikis atitinkamai sričiai	Priėmus Nutarimo projektą, bus įtvirtinta nacionalinė kibernetinių incidentų valdymo sistema, t. y. nustatyta kibernetinio saugumo politiką įgyvendinančių institucijų, kitų viešojo administravimo subjektų, valdančių ir (arba) tvarkančių valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų veikla, atliekama siekiant suvaldyti kibernetinius incidentus, tarpinstitucinė kibernetinių incidentų valdymo sąveika, kibernetinių incidentų klasifikavimo tvarka ir tarpinstitucinis bendradarbiavimas tiriant kibernetinius incidentus. Tai leis geriau valdyti kibernetinius incidentus, kurie kyla kelių institucijų ar įstaigų informacinėse sistemose ar elektroninių ryšių tinkluose ar gali sutrikdyti kelių institucijų ar įstaigų veiklą, taip pat bus sudarytos sąlygos institucijoms, tiriančioms kibernetinius incidentus, operatyviai gauti informaciją, reikalingą kibernetiniams incidentams tirti. Priėmus Nutarimo projektą, neigiamų pasekmių nenumatoma.
Poveikis valstybės finansams	Priėmus Nutarimo projektą, poveikio valstybės finansams nebus.
Poveikis administracinei naštai	Nutarimo projektas įgyvendina Kibernetinio saugumo įstatymo nuostatas. Poveikis administracinei naštai buvo įvertintas rengiant Kibernetinio saugumo įstatymo projektą. Priėmus Nutarimo projektą, administracinė našta nepadidės.

Kita svarbi informacija Nėra.

Informacija apie asmenį ir instituciją, atsakingą už poveikio vertinimą

Vardas ir pavardė	Miroslavas Tribockis
Pareigos	Vyriausiasis specialistas

Institucija (padalinys)	Krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų departamento Kibernetinio saugumo ir elektroninės informacijos saugos skyrius
Telefono numeris ir elektroninio pašto adresas	Tel. 8 706 80 807, el. paštas miroslavas.tribockis@kam.lt

Juozas Olekas
Krašto apsaugos ministras

16

LIETUVOS RESPUBLIKOS VYRIAUSYBĖS KANCELIARIJOS VIEŠOJO VALDYMO IR SOCIALINĖS APLINKOS DEPARTAMENTO INFORMACINĖS VISUOMENĖS SKYRIUS

PAŽYMA

DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL NACIONALINIO KIBERNETINIŲ INCIDENTŲ VALDYMO PLANO PATVIRTINIMO“ PROJEKTO (Nr. 15-0635-01-N) (TAIS Nr. 15-6282(3))

2015-11-24 Nr. NV-3771
Vilnius

1. **Projekto rengėja:** Krašto apsaugos ministerija.

2. **Projekto tikslas, esmė.** Nutarimo projekto tikslas – įgyvendinant Kibernetinio saugumo įstatymą, reglamentuoti nacionalinę kibernetinio saugumo incidentų valdymo sistemą, t. y. nustatyti kibernetinio saugumo politiką įgyvendinančių institucijų, kitų viešojo administravimo subjektų, valdančių ir (arba) tvarkančių valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų veikas, atliekamas siekiant suvaldyti kibernetinius incidentus, galinčius sutrikdyti ar sutrikdančius valstybės informacinių išteklių, ypatingos svarbos informacinės infrastruktūros ir (ar) kitų elektroninių ryšių tinklų ir (ar) informacinių sistemų darbą ir taip sukeliančius grėsmę nacionaliniam saugumui, žmonių sveikatai ar gyvybei, visuomenės gerovei ar valstybės funkcijų atlikimui, taip pat nustatyti tarpinstitucinę kibernetinių incidentų valdymo sąveiką, kibernetinių incidentų klasifikavimo tvarką ir tarpinstitucinį bendradarbiavimą tiriant kibernetinius incidentus.

Nustatoma, kad už kibernetinių incidentų valdymą bus atsakingi Nacionalinis kibernetinio saugumo centras ir Ryšių reguliavimo tarnyba. Siūloma įteisinti informavimo apie kibernetinius incidentus tvarką ir patvirtinti, kad įvykus kibernetiniam incidentui informacija apie jį keičiamasi kibernetinio saugumo informaciniame tinkle ir šį incidentą iš pradžių bando valdyti tvarkytojas. Jeigu nepakanka išteklių incidentui suvaldyti, jo valdymą pagal kompetenciją perima Nacionalinis kibernetinio saugumo centras arba Ryšių reguliavimo tarnyba. Jeigu išteklių incidentui suvaldyti vis dar trūktų, informuojamas krašto apsaugos ministras, o, pavojingo kibernetinio incidento nesuvaldžius per maksimalų leistiną terminą, sprendimą dėl tolesnio jo valdymo priima Vyriausybė. Prireikus informuojami Seimas ir Respublikos Prezidento kanceliarija.

3. **Derinimas.** Nutarimo projektas derintas su Energetikos ministerija, Finansų ministerija, Lietuvos banku, Policijos departamentu prie Vidaus reikalų ministerijos, Ryšių reguliavimo tarnyba, Susisiekimo ministerija, Valstybine duomenų apsaugos inspekcija, Vidaus reikalų ministerija, Ūkio ministerija, Teisingumo ministerija ir visuomene.

Nutarimo projektas svarstytas 2015 m. rugsėjo 1 d. ministerijų atstovų pasitarime ir patikslintas pagal pasitarime pateiktas pastabas. Papildomai patikslintas nutarimo projektas derintas su Valstybės saugumo departamentu, Respublikos Prezidento kanceliarija ir Seimo kanceliarija.

Dėl pastabų ir pasiūlymų, į kuriuos neatsižvelgta arba atsižvelgta iš dalies, pridedama nutarimo projekto derinimo pažyma.

4. **Dalykinio vertinimo išvada.**

Derinimo pažymos pagrindinės pastabos:

4.1. Teisingumo ministerija, atsižvelgdama į tai, kad nereikšmingų incidentų gali būti iki kelių šimtų per dieną, pasiūlė įpareigoti pranešti ne apie kiekvieną iš jų. Krašto

apsaugos ministerija argumentavo, kad tokia nuostata įtvirtinta Kibernetinio saugumo įstatyme.

4.2. Vyriausybės kanceliarijos Teisės departamentas suabejojo, kad nutarimo projektu, be kita ko, siūloma plačiau, negu nustatyta Kibernetinio saugumo įstatyme, reguliuoti kibernetinį saugumą įgyvendinančių institucijų ir kitų subjektų veiksmus. Krašto apsaugos ministerijos nuomone, siūlomas teisinis reglamentavimas yra pagrįstas ir atitinka Kibernetinio saugumo įstatymo tikslus. Be to, šiame įstatyme nustatyta, kad Nacionalinis kibernetinio saugumo centras atlieka ir kitas teisės aktuose nustatytas funkcijas kibernetinio saugumo užtikrinimo srityje.

4.3. Vyriausybės kanceliarijos Teisės departamentas nurodė, kad kai kurios Nacionalinio kibernetinių incidentų valdymo plano (toliau – Planas) projekto nuostatos dubliuoja Kibernetinio saugumo įstatymo nuostatas. Pritariame Krašto apsaugos ministerijos nuomonei, kad, neperkėlus kai kurių šio įstatymo nuostatų, kibernetinio saugumo sistema ir incidentų valdymo mechanizmas nebūtų nuoseklūs ir aiškūs.

4.4. Vyriausybės kanceliarijos Viešojo valdymo ir socialinės aplinkos departamento Informacinės visuomenės skyrius pasiūlė nutarimo projekto nutariamąją dalį papildyti nuostatomis, iki kada turės būti parengti Organizaciniai ir techniniai kibernetinio saugumo reikalavimai, nurodyti Plano projekto 5.1 papunktyje, ir Kibernetinio saugumo informacinio tinklo nuostatai. Krašto apsaugos ministerija nurodė, kad šių dokumentų parengimas turės būti organizuotas nedelsiant po Plano priėmimo. Tačiau lieka neaišku, iki kada jie turi būti parengti.

4.5. Valstybės saugumo departamentas pasiūlė Plano projekto turinyje užsiminti apie metodiką, pagal kurią būtų nustatoma, ar incidentas gali turėti įtakos nacionaliniam saugumui. Krašto apsaugos ministerija nurodė, kad apie tokius incidentus bus informuojamas Valstybės saugumo departamentas, bet iš esmės neatsakė, ar tokia metodika būtų reikalinga. Akivaizdu, kad tam tikrais atvejais gali būti sunku nustatyti, ar reikia kreiptis į Valstybės saugumo departamentą. Todėl siūlome tiksliau reglamentuoti, kaip išskirti tokius atvejus.

Teikiamas projektas iš esmės atitinka Vyriausybės darbo reglamento reikalavimus.

Informacinės visuomenės skyriaus vedėja D. Kirkilaitė-Chetcuti

E. Kazakevičius, tel. 8 706 63 889, edmundas.kazakevicius@lrv.lt

LIETUVOS RESPUBLIKOS VYRIAUSYBĖS KANCELIARIJOS
TEISĖS DEPARTAMENTAS

IŠVADA
DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL NACIONALINIO KIBERNETINIŲ INCIDENTŲ VALDYMO PLANO PATVIRTINIMO“ PROJEKTO

(toliau – Projektas)
(Nr. 15-0635-02-N) (TAIS Nr. 15-6282(5))

2015-11-26 Nr. NV-3781
Vilnius

Įvertinę Projekto atitiktį įstatymams, Vyriausybės nutarimams ir teisės technikos reikalavimams, teikiame šias pastabas:

1. Pažymėtina, kad Projektu siūlomo tvirtinti Nacionalinio kibernetinių incidentų valdymo plano (toliau – Planas) 5 punkte nustatyta, kad išskiriamos keturios kibernetinių incidentų kategorijos (pavojingi, didelės reikšmės, vidutinės reikšmės, nereikšmingi), o pagal Plano 6 punktą kriterijus, kuriais remiantis kibernetinis incidentas priskiriamas atitinkamai kategorijai, nustato Lietuvos Respublikos Vyriausybė ir Lietuvos Respublikos ryšių reguliavimo tarnyba. Be to, Plano 8 punkte nustatyta, kad Nacionalinis kibernetinio saugumo centras ar Ryšių reguliavimo tarnyba pagal kompetenciją kibernetinį incidentą *gali priskirti* pavojingam kibernetiniam incidentui, jei identifikuotas didelės reikšmės kibernetinis incidentas ir (ar) jo poveikis gali sukelti (sukelia) bent vieną iš Plano 8 punkte nurodytų padarinių. Sistemiškai vertinant anksčiau minėtas Plano nuostatas, trūksta aiškumo, ar vis dėlto Lietuvos Respublikos Vyriausybė ir (ar) Lietuvos Respublikos ryšių reguliavimo tarnyba nustatys ir tuos kriterijus, pagal kuriuos incidentai bus priskiriami pavojingiems, ar šiuo atveju incidentų klasifikavimas bus paliekamas spręsti kompetentingoms institucijoms Plano 8 punkte nustatyta tvarka. Siūlome Plano reguliavimą tikslinti šia apimtimi, prireikus atsisakyti nepagrįstos minėtų institucijų diskrecijos („kibernetinį incidentą *gali priskirti* pavojingam kibernetiniam incidentui“).

2. Siekiant teisinio aiškumo, Plano 9 punkte siūlytume patikslinti, kad Nacionalinis kibernetinio saugumo centras arba Ryšių reguliavimo tarnyba turi teisę patikslinti kibernetinio incidento kategoriją (priskirti didesnės ar mažesnės reikšmės kibernetinių incidentų kategorijai) tokiems incidentams, kuriems, atsižvelgdami į nustatytus kriterijus, Plano 5.2-5.4 papunkčiuose numatytoms kibernetinių incidentų kategorijoms 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 identifikuotas kibernetinis incidentas. Kartu pažymėtina, kad, kaip minėta ankstesnėse Lietuvos Respublikos Vyriausybės kanceliarijos Teisės departamento pastabose Projektui, pagal siūlomą Plano 9 punkto redakciją neaišku, kokiais kriterijais vadovaujantis Nacionalinis kibernetinio saugumo centras arba Ryšių reguliavimo tarnyba turės teisę patikslinti kibernetinio incidento kategoriją, kokia tvarka ir kada tai bus atliekama ir pan. Be kita ko, neaiškus Plano 9 punkto nuostatos santykis su Plano 8 punkte aptariamais minėtų institucijų įgaliojimais priskirti didelės reikšmės incidentą pavojingam, t.y. suteikti jam didesnę kategoriją.

3. Pakartotinai norėtume pastebėti, kad mūsų nuomone, Plano 10 punkto turinys yra perteklinis, atsižvelgiant į tai, kad Lietuvos Respublikos kibernetinio saugumo įstatymo III skyriuje reguliuojamos ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų, elektroninės informacijos prieglobos paslaugų teikėjų, taip pat viešojo administravimo subjektų pareigos, įgyvendinant kibernetinio saugumo užtikrinimo priemones, tame tarpe ir kibernetinių incidentų prevenciją. Kartu pažymime, kad Projekto rengėjų derinimo pažymoje pateikti argumentai dėl Plano 10 punkto tikslingumo yra daugiau praktinio, nei teisinio pobūdžio. Be to, Plano 10 punkto pirmo sakinio formuluotė yra netiksli „kibernetinių incidentų prevenciją *Ryšių ir informacinių sistemų* vykdo jų tvarkytojai“.

15

4. Plano 12 punkte siūlome vartoti Plano 11 punkte nurodytą formuluotę „*galimą* kibernetinį incidentą“ (vietoj „*galimas dalykas, vykstantį* kibernetinį incidentą“).

5. Plano III skyriaus pirmasis skirsnis pavadintas „Kibernetinių incidentų prevencija, identifikavimas ir *vertinimas*“, tačiau minėto skirsnio turinyje apie incidentų vertinimą nėra užsimenama, Plano 15 punkte tik nurodoma, kad KIVT institucija, pagal kompetenciją *įvertinusi gautą informaciją apie kibernetinį incidentą*, apie kibernetinio incidento identifikavimo faktą nedelsdama informuoja kitas KIVT institucijas. Atsižvelgiant į tai, siūlytume apsvarstyti, ar kibernetinių incidentų *vertinimas* išskiriamas pagrįstai.

6. Projekto rengėjai derinimo pažymoje dėl anksčiau teiktų Lietuvos Respublikos Vyriausybės kanceliarijos Teisės departamento pastabų pažymi, kad Lietuvos Respublikos kibernetinio saugumo įstatymas nenustato, kaip tvarkytojai ar valdytojai turi reaguoti į kibernetinius incidentus, tuo tarpu Plano 16 punkte siūloma įtvirtinti, kad tvarkytojai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai ir elektroninės informacijos priegłobos paslaugų teikėjai į kibernetinius incidentus *reaguoja vadovaudamiesi valdytojo kibernetinio saugumo teisės aktais*. Mūsų nuomone, svarstytina, ar pagrįstai įstatymo įgyvendinamajame teisės akte išplečiamas įstatyminis reguliavimas šiuo aspektu. Atsižvelgiant į tai, siūlytume atsisakyti Plano 16 punkto, be kita ko, Plano 17 punktas vertintinas kaip nesukuriantis pridėtinės vertės, įvertinant tai, kad Lietuvos Respublikos kibernetinio saugumo įstatymo 13, 14, 15, 16 straipsnių nuostatose įvardintos valdytojų ir tvarkytojų pareigos kibernetinio saugumo srityje.

7. Sistemiškai vertinant Lietuvos Respublikos kibernetinio saugumo įstatymo nuostatas, vis dėlto lieka neaišku (Projekto rengėjai derinimo pažymoje taip pat neaptaria argumentų dėl anksčiau teiktos tapačios pastabos), kuo remiantis Plano 19 punkte pavedama nustatyti KIVT institucijų (Ryšių reguliavimo tarnybos, Valstybinės duomenų apsaugos inspekcijos ir policijos) *reagavimo* į kibernetinius incidentus tvarką, kadangi minėto įstatymo 10 straipsnio 2 dalies 10 punkte minima tik kaip Nacionalinis kibernetinio saugumo centras, t.y. laikydamasis krašto apsaugos ministro nustatytos tvarkos, reaguoja į kibernetinius incidentus valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėse infrastruktūrose.

8. Plano 22 punkte yra nurodyta, kad Nacionalinis kibernetinio saugumo centras arba Ryšių reguliavimo tarnyba pagal kompetenciją perėmę valdyti kibernetinį incidentą turi tam tikrus įgaliojimus, pvz., priimti sprendimus, duoti nurodymus ir pan., tuo tarpu pagal Plano 29 punktą minėtos institucijos, be kita ko, turi teisę surengti koordinacinį pasitarimą dėl kibernetinio incidento valdymo. Siekiant sistemiškumo, manytina, kad Nacionalinio kibernetinio saugumo centro, Ryšių reguliavimo tarnybos įgaliojimai turėtų būti dėstomi nuosekliai, pvz., Plano 22 punkte. Kartu pažymėtina, kad Plano 29, 30 punktų reguliavimas yra pernelyg detalus, pvz., tokios nuostatos, kaip „kartu pateikiama informacija apie numatomą pasitarimo datą, laiką ir vietą, jei pasitarimas rengiamas ne elektroninio ryšio priemonėmis“, „Nacionalinis kibernetinio saugumo centras arba Ryšių reguliavimo tarnyba pagal kompetenciją į koordinacinį pasitarimą turi teisę pakviesti kitus kompetentingus ekspertus“, mūsų manymu, galėtų būti, pvz., KIVT institucijų teisės aktų reguliavimo dalyku.

9. Pastebėtina, kad Plano 39 punkto nuostatos, kad KIVT institucijos privalo paskirti kontaktinius asmenis, iš esmės dubliuoja Projekto 2.2 papunkčio reguliavimą. Be to, pastebėtina, kad neaišku, kokia įstatyminio reguliavimo nuostata remdamasi Lietuvos Respublikos Vyriausybė Projekto 2.2 papunktyje įpareigoja jai nepavaldžius subjektus, pvz., Ryšių reguliavimo tarnybą, kai tuo tarpu Projekto 3 punkte nepavaldiems subjektams yra teikiama rekomendacija.

Teisės departamento direktoriaus pavaduotojas Aleksandr Radčenko

Eglė Gasiūnaitė, 8 706 63 766, el. p. e.gasiunaite@lrv.lt

1.
29

LIETUVOS RESPUBLIKOS VYRIAUSYBĖS KANCELIARIJA
TEISĖS DEPARTAMENTAS

IŠVADA
DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL NACIONALINIO KIBERNETINIŲ INCIDENTŲ VALDYMO PLANO PATVIRTINIMO“ PROJEKTO

(toliau – Projektas)
(TAIS Nr. 15-6282(6))

2016 01 19 Nr. NV-186

Vilnius

Įvertinę po Ministerijų atstovų (viceministrų, ministerijų kanclerių) 2015 m. gruodžio 1 d. pasitarimo patikslinto Projekto atitiktį įstatymams, Vyriausybės nutarimams bei teisės technikos reikalavimams, pažymime, kad papildomų pastebėjimų, nei nurodyti Lietuvos Respublikos Vyriausybės kanceliarijos Teisės departamento 2015 m. lapkričio 26 d. išvadoje Nr. NV-3781, neturime.

Teisės departamento direktoriaus pavaduotojas Aleksandr Radčenko

Eglė Gasiūnaitė, tel. 8 706 63 766, el. p. egle.gasiunaite@lrv.lt

LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL NACIONALINIO KIBERNETINIŲ INCIDENTŲ VALDYMO PLANO PATVIRTINIMO“ DERINIMO PAŽYMA

Institucijos pavadinimas, rašto data, numeris	**Pasiūlymai ir pastabos**	**Žyma apie pritarimą pastaboms ir pasiūlymams**
Lietuvos Respublikos Vyriausybės kanceliarijos Teisės departamentas, 2015-11-26, Nr. NV-3781	1. Pažymėtina, kad Projektu siūlomo tvirtinti Nacionalinio kibernetinių incidentų valdymo plano (toliau – Planas) 5 punkte nustatyta, kad išskiriamos keturios kibernetinių incidentų kategorijos (pavojingi, didelės reikšmės, vidutinės reikšmės, nereikšmingi), o pagal Plano 6 punktą kriterijus, kuriais remiantis kibernetinis incidentas priskiriamas atitinkamai kategorijai, nustato Lietuvos Respublikos Vyriausybė ir Lietuvos Respublikos ryšių reguliavimo tarnyba. Be to, Plano 8 punkte nustatyta, kad Nacionalinis kibernetinio saugumo centras ar Ryšių reguliavimo tarnyba pagal kompetenciją kibernetinį incidentą *gali priskirti* pavojingam kibernetiniam incidentui, jei identifikuotas didelės reikšmės kibernetinis incidentas ir (ar) jo poveikis gali sukelti (sukelia) bent vieną iš Plano 8 punkte nurodytų padarinių. Sistemiškai vertinant anksčiau minėtas Plano nuostatas, trūksta aiškumo, ar vis dėlto Lietuvos Respublikos Vyriausybė ir (ar) Lietuvos Respublikos ryšių reguliavimo tarnyba nustatys ir tuos kriterijus, pagal kuriuos incidentai bus priskiriami pavojingiems, ar šiuo atveju incidentų klasifikavimas bus paliekamas spręsti kompetentingoms institucijoms Plano 8 punkte nustatyta tvarka. Siūlome Plano reguliavimą tikslinti šia apimtimi, prireikus atsisakyti nepagrįstos minėtų institucijų diskrecijos („kibernetinį incidentą *gali priskirti* pavojingam kibernetiniam incidentui“).	**Atsižvelgta iš dalies**. Patikslintas Plano 6 punktas ir išdėstytas taip: „6. Kriterijus, kuriais vadovaujantis kibernetinis incidentas priskiriamas **Plano 5.2–5.4 papunkčiuose nustatytoms** ~~atitinkamai~~ kategorija~~i~~**oms**, nustato:“ Manome, kad, patikslinus Plano 8 punktą, kiekvienas kibernetinis incidentas, atitinkantis Plano 8.1–8.4 papunkčiuose pateiktus požymius, būtų prisikirtas pavojingiems kibernetiniams incidentams, ir kartu būtų pasunkintas kibernetinio incidento valdymas. Pavyzdžiui, jei kibernetinis incidentas atitinka bent vieną iš Plano 8.1–8.4 papunkčių, bet gali būti suvaldytas per 10 minučių, nepatyrus žalos, tokio kibernetinio incidento priskyrimas pavojingam kibernetiniam incidentui sutrukdytų operatyviai incidentą suvaldyti, nes pavojingo kibernetinio incidento metu įsijungtų kitas kibernetinio incidento valdymo procesas ir būtų atliekamos papildomos Ryšių reguliavimo tarnybos ar Nacionalinio kibernetinio saugumo centro funkcijos.
	3. Pakartotinai norėtume pastebėti, kad mūsų nuomone,	**Atsižvelgta iš dalies.**

	Plano 10 punkto turinys yra perteklinis, atsižvelgiant į tai, kad Lietuvos Respublikos kibernetinio saugumo įstatymo III skyriuje reguliuojamos ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų, elektroninės informacijos prieglobos paslaugų teikėjų, taip pat viešojo administravimo subjektų pareigos, įgyvendinant kibernetinio saugumo užtikrinimo priemones, tame tarpe ir kibernetinių incidentų prevenciją. Kartu pažymime, kad Projekto rengėjų derinimo pažymoje pateikti argumentai dėl Plano 10 punkto tikslingumo yra daugiau praktinio, nei teisinio pobūdžio. Be to, Plano 10 punkto pirmo sakinio formuluotė yra netiksli „kibernetinių incidentų prevenciją *Ryšių ir informacinių sistemų* vykdo jų tvarkytojai“.	Patikslinta Plano 10 punkto pirmo sakinio formuluotė. Sutinkame su Teisės departamento nuomone, kad Plano 10 punkto tikslingumas yra daugiau praktinio nei teisinio pobūdžio. Tačiau kartu norime atkreipti dėmesį, kad Planas bus įgyvendinamas praktiškai ir jame, mūsų nuomone, turi atsispindėti visas kibernetinio incidento valdymo ciklas.
	5. Plano III skyriaus pirmasis skirsnis pavadintas „Kibernetinių incidentų prevencija, identifikavimas ir *vertinimas*“, tačiau minėto skirsnio turinyje apie incidentų vertinimą nėra užsimenama, Plano 15 punkte tik nurodoma, kad KIVT institucija, pagal kompetenciją *įvertinusi gautą informaciją apie kibernetinį incidentą*, apie kibernetinio incidento identifikavimo faktą nedelsdama informuoja kitas KIVT institucijas. Atsižvelgiant į tai, siūlytume apsvarstyti, ar kibernetinių incidentų *vertinimas* išskiriamas pagrįstai.	**Atsižvelgta iš dalies.** Plano 14 punkte nustatyta, kad tvarkytojai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai ir elektroninės informacijos prieglobos paslaugų teikėjai, identifikavę 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, reikalingas kibernetiniam incidentui suvaldyti. Informacijos surinkimas buvo prilygintas kibernetinio incidento vertinimui. Atsižvelgdami į pateiktą pastabą, patikslinome ir aiškiau išdėstėme Plano 14 punktą.
	6. Projekto rengėjai derinimo pažymoje dėl anksčiau teiktų Lietuvos Respublikos Vyriausybės kanceliarijos Teisės departamento pastabų pažymi, kad Lietuvos Respublikos kibernetinio saugumo įstatymas nenustato, kaip tvarkytojai ar valdytojai turi reaguoti į kibernetinius incidentus, tuo tarpu Plano 16 punkte siūloma įtvirtinti, kad tvarkytojai,	**Neatsižvelgta.** Viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų saugumo ir vientisumo užtikrinimo taisyklių, patvirtintų Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2011 m. spalio 21 d. įsakymu Nr. 1V-1013 „Dėl Viešųjų ryšių tinklų,

23

	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*. Mūsų nuomone, svarstytina, ar pagrįstai įstatymo įgyvendinamajame teisės akte išplečiamas įstatyminis reguliavimas šiuo aspektu. Atsižvelgiant į tai, siūlytume atsisakyti Plano 16 punkto, be kita ko, Plano 17 punktas vertintinas kaip nesukuriantis pridėtinės vertės, įvertinant tai, kad Lietuvos Respublikos kibernetinio saugumo įstatymo 13, 14, 15, 16 straipsnių nuostatose įvardintos valdytojų ir tvarkytojų pareigos kibernetinio saugumo srityje.	viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų saugumo ir vientisumo užtikrinimo taisyklių patvirtinimo“ (Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2015 m. birželio 23 d. įsakymo Nr. 1V-776 redakcija), 3.1 papunktyje nustatyta, kad viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai privalo įgyvendinti tinkamas technines ir organizacines priemones savo teikiamų viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų saugumui užtikrinti; šios priemonės turi užtikrinti saugumo lygį, atitinkantį iškilusią grėsmę, ir užkirsti kelią incidentams arba sumažinti jų poveikį viešiesiems ryšių tinklams ir (arba) viešųjų elektroninių ryšių paslaugų gavėjams, o pagal 5.1 papunktį elektroninės informacijos prieglobos paslaugų teikėjai privalo įgyvendinti tinkamas kibernetinio saugumo užtikrinimo technines ir organizacines priemones savo teikiamų elektroninės informacijos prieglobos paslaugų saugumui užtikrinti; šios priemonės turi užtikrinti saugumo lygį, atitinkantį iškilusią grėsmę, ir užkirsti kelią incidentams arba sumažinti jų poveikį. Atitinkamai pagal Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašą, tvirtinamą Lietuvos Respublikos Vyriausybės nutarimo „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“ projektu, ypatingos svarbos informacinės infrastruktūros ir valstybės informacinių išteklių valdytojai teisės aktuose, reglamentuojančiuose RIS kibernetinį saugumą, turės nustatyti kibernetinio incidento valdymo organizavimo principus. Atsižvelgdami į tai, kad aukščiau nurodyti teisės aktai yra

24

		Kibernetinio saugumo įstatymo įgyvendinamieji teisės aktai, manome, kad Plane nėra išplečiamas įstatymų galios reguliavimas, o kaip tik nustatomi subjektų veiksmai, susiję su kibernetinio incidento valdymu, pagal kituose Kibernetinio saugumo įstatymo įgyvendinamuosiuose teisės aktuose patvirtintus reikalavimus. Kodėl neatsižvelgta į siūlymą atsisakyti Plano 17 punkto (Projekto 18 punktas), žr. 3 pastabos argumentus.
Lietuvos Respublikos Vyriausybės kanceliarijos Viešojo valdymo ir socialinės aplinkos departamento Informacinės visuomenės skyrius, 2015-11-24, Nr. NV-3771	4.1. Teisingumo ministerija, atsižvelgdama į tai, kad nereikšmingų incidentų gali būti iki kelių šimtų per dieną, pasiūlė įpareigoti pranešti ne apie kiekvieną iš jų. Krašto apsaugos ministerija argumentavo, kad tokia nuostata įtvirtinta Kibernetinio saugumo įstatyme.	**Neatsižvelgta.** Reikalavimai dėl informacijos apie kibernetinius incidentus pateikimo yra ne šio teisės akto reguliavimo dalykas ir nustatomi kitame Kibernetinio saugumo įstatymo įgyvendinamajame teisės akte – Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, apraše. Projektas šiuo metu yra parengtas ir derinamas su Teisingumo ministerija.
	4.2. Vyriausybės kanceliarijos Teisės departamentas suabejojo, kad nutarimo projektu, be kita ko, siūloma plačiau, negu nustatyta Kibernetinio saugumo įstatyme, reguliuoti kibernetinį saugumą įgyvendinančių institucijų ir kitų subjektų veiksmus. Krašto apsaugos ministerijos nuomone, siūlomas teisinis reglamentavimas yra pagrįstas ir atitinka Kibernetinio saugumo įstatymo tikslus. Be to, šiame įstatyme nustatyta, kad Nacionalinis kibernetinio saugumo centras atlieka ir kitas teisės aktuose nustatytas funkcijas kibernetinio saugumo užtikrinimo srityje.	**Neatsižvelgta.** Žr. argumentus dėl Teisės departamento 6 pastabos.
	4.4. Vyriausybės kanceliarijos Viešojo valdymo ir socialinės aplinkos departamento Informacinės visuomenės skyrius pasiūlė nutarimo projekto nutariamąją dalį papildyti nuostatomis, iki kada turės būti parengti Organizaciniai ir techniniai kibernetinio saugumo reikalavimai, nurodyti Plano projekto 5.1 papunktyje, ir Kibernetinio saugumo informacinio tinklo nuostatai.	**Neatsižvelgta** Kibernetinio saugumo įstatymo 20 straipsnio 2 dalis nustato, kad „Vyriausybė, krašto apsaugos ministras, vidaus reikalų ministras, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija, Policijos departamentas iki 2014 m. gruodžio 31 d. priima šio įstatymo įgyvendinamuosius teisės aktus“, todėl manome, kad Vyriausybės nutarimu nustačius

25

	Krašto apsaugos ministerija nurodė, kad dokumentų parengimas turės būti organizuotas nedelsiant po Plano priėmimo. Tačiau išlieka neaišku, iki kada jie turi būti parengti.	naujas teisės aktų rengimo datas Vyriausybė viršytų įgaliojimus.

Juozas Olekas
Krašto apsaugos ministras

21

2015 m. prioritetas

Siūlau įtraukti į Vyriausybės posėdžio (pasitarimo) darbotvarkės projektą

2016-01-21

Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo (Nr.15-0635-01-N(2) (15-6282(5))

Pranešėjas: krašto apsaugos ministras J.Olekas

Dalyvauja: KAM Kibernetinio saugumo ir informacinių technologijų departamento Kibernetinio saugumo ir elektroninės informacijos saugos skyriaus patarėjas T.Stamulis

Klausimo kuratorius: N.Makštelienė

2015 08 25

Apsvarstyta ministerijų atstovų pasitarime	Ministerijų atstovų pasitarimo protokolo išrašas
2015-09-01/2015-12-01 (data)	1. Pasiūlyti KAM: 1.1. atsižvelgti į TM ir TD pastabas; 1.2. įtraukti Vyriausybės kancelijos Viešojo valdymo ir socialinės aplinkos departamento Informacinės visuomenės skyriaus pastabas. 2. Patikslintą projektą svarstyti VAP. (2015-09-01) 1. Pasiūlyti Krašto apsaugos ministerijai atsižvelgti į Vyriausybės kanceliarijos Teisės departamento ir Viešojo valdymo ir socialinės aplinkos departamento Informacinės visuomenės skyriaus pastabas. 2. Patikslintą projektą svarstyti Vyriausybės posėdžio B dalyje. (2015-12-01)
Informacija apie projekto svarstymą Vyriausybės pasitarime ar/ir Vyriausybės posėdyje	Papildoma informacija