

**LIETUVOS RESPUBLIKOS VYRIAUSYBĖS KANCELIARIJA
POLITIKOS ĮGYVENDINIMO GRUPĖ**

PAŽYMA

**DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL LIETUVOS
RESPUBLIKOS VYRIAUSYBĖS 2016 M. SAUSIO 25 D. NUTARIMO NR. 87 „DĖL
NACIONALINIO KIBERNETINIŲ INCIDENTŲ VALDYMO PLANO PATVIRTINIMO“
PAKEITIMO“ PROJEKTO (toliau– Projektas Nr. 1) IR LIETUVOS RESPUBLIKOS
VYRIAUSYBĖS NUTARIMO „DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS 2015 M.
KOVO 18 D. NUTARIMO NR. 281 „DĖL VALSTYBINĖS VARTOTOJŲ TEISIŲ
APSAUGOS 2015–2018 METŲ STRATEGIJOS PATVIRTINIMO“ PAKEITIMO“
PROJEKTO (toliau – Projektas Nr. 2) (toliau kartu – Projektai)
(TAP-18-160; TAIS NR. 18-233(2))**

2018-02-28 Nr. NV-491

Vilnius

Projektų rengėjas: Krašto apsaugos ministerija.

Projektų tikslas: Patikslinti Vyriausybės nutarimus dėl pasikeitusios institucijų atsakomybės kibernetinio saugumo užtikrinimo ir informacijos saugumo incidentų tyrimo srityse.

Dabartinė situacija: Dabar galiojančiuose Vyriausybės nutarimais patvirtintuose Nacionaliniame kibernetinių incidentų valdymo plane ir Valstybinės vartotojų teisių apsaugos 2015-2018 m. strategijoje Ryšių reguliavimo tarnybai numatytos su kibernetinio saugumo užtikrinimu susijusios funkcijos. 2017 m. gruodžio 19 d. Seimas priėmė Kibernetinio saugumo įstatymo ir Elektroninių ryšių įstatymo pakeitimus, kuriais Ryšių reguliavimo tarnybos atliekamas nacionalinių elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo funkcijas 2018 m. sausio 1 d. perdavė Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos. Atitinkamai turi būti patikslinti poįstatyminiai teisės aktai.

Projektų esmė: Teisinis reguliavimas nėra keičiamas iš esmės. Kadangi Ryšių reguliavimo tarnyba jau nebevykdo su kibernetiniu saugumu susijusių funkcijų, siūloma:

- Projektu Nr. 1 patvirtinti naujos redakcijos Nacionalinio kibernetinių incidentų valdymo planą, kuriame patikslintos institucijų atsakomybės, – vietoje Ryšių reguliavimo tarnybos įrašant Nacionalinį kibernetinio saugumo centrą prie Krašto apsaugos ministerijos, taip pat atlikti redakciniai pataisymai;
- Projektu Nr. 2 pakeisti instituciją, atsakingą už Valstybinės vartotojų teisių apsaugos 2015-2018 m. strategijoje nustatytų uždavinių susijusių su kibernetiniu saugumu, įgyvendinimą, – vietoje Ryšių reguliavimo tarnybos įrašant Nacionalinį kibernetinio saugumo centrą prie Krašto apsaugos ministerijos.

Derinimas: Projektai derinti su Teisingumo ministerija. Ryšių reguliavimo tarnyba derinimo išvados neteikė. Neatsižvelgta į Teisingumo ministerijos siūlymą dėl nustatomų terminų Projektą Nr. 1 derinti su kibernetinius incidentus valdančiomis ir (ar) tiriančiomis institucijomis. Krašto apsaugos ministerijos nuomone siūlomas derinimas netikslingas, nes keičiamame Nacionalinio kibernetinių incidentų valdymo plane terminai nėra nustatomi, o tik patikslinami atsižvelgiant į

teisėkūros reikalavimus (vietoje termino „nedelsiant“, nustatomas terminas „nedelsiant, bet ne vėliau kaip per ...“).

Projektai 2018 vasario 27 d. svarstyti Tarpinstituciniame pasitarime, kuriame nutarta pasiūlyti Krašto apsaugos ministerijai Projektus patikslinti pagal suderintas Vyriausybės kanceliarijos Teisės grupės pastabas ir Projektus svarstyti Vyriausybės posėdyje.

Atitiktis Vyriausybės programai: Projektai netiesiogiai susiję su Vyriausybės programos įgyvendinimo plano 5.2.1. darbo „Kibernetinių incidentų prevencija ir valdymo sistemos tobulinimas“ nuostatų įgyvendinimu.

Dalykinio vertinimo išvada: Siūlome Projektus svarstyti Vyriausybės posėdžio B dalyje. Krašto apsaugos ministerija Projektus patikslins pagal Tarpinstituciniame pasitarime suderintas pastabas.

Politikos įgyvendinimo grupės patarėjas
Kiveris

Valdas



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

2018-02-07 Nr. 12-01-191

DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMŲ PROJEKTŲ

Lietuvos Respublikos krašto apsaugos ministerija parengė ir teikia Lietuvos Respublikos Vyriausybės 2016 m. sausio 25 d. nutarimo Nr. 87 „Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“ pakeitimo projektą (toliau – 1 projektas) ir Lietuvos Respublikos Vyriausybės 2015 m. kovo 18 d. nutarimo Nr. 281 „Dėl Valstybinės vartotojų teisių apsaugos 2015–2018 metų strategijos patvirtinimo“ pakeitimo projektą (toliau – 2 projektas) (toliau kartu – Nutarimų projektai).

Nutarimų projektais įgyvendinamos Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 1, 2, 4, 6, 10, 15, 16, 18 straipsnių pakeitimo, 8 straipsnio pripažinimo netekusiu galios ir įstatymo papildymo priedu įstatymo Nr. XIII-920 ir Lietuvos Respublikos elektroninių ryšių įstatymo Nr. IX-2135 3, 8, 9, 42¹ ir 71 straipsnių pakeitimo įstatymo Nr. XIII-921 nuostatos, kuriomis Lietuvos Respublikos ryšių reguliavimo tarnybos atliekamos nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio funkcijos 2018 m. sausio 1 d. perduotos Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos. Atsižvelgiant į tai, kad nuo 2018 m. sausio 1 d. Ryšių reguliavimo tarnyba nebevykdo su kibernetiniu saugumu susijusių funkcijų, 1 projektu tikslinamos Nacionalinio kibernetinių incidentų valdymo plano (toliau – Planas) nuostatos, kuriose buvo nurodyta ši institucija, taip pat atliekami kiti redakciniai pataisymai, o 2 projektu pakeičiama institucija, atsakinga už Valstybinės vartotojų teisių apsaugos 2015–2018 metų strategijos priede nustatytų uždavinių, susijusių su kibernetiniu saugumu, įgyvendinimą, – vietoj Ryšių reguliavimo tarnybos nurodomas Nacionalinis kibernetinio saugumo centras.

Nutarimų projektai skelbiami Lietuvos Respublikos Seimo kanceliarijos teisės aktų informacinėje sistemoje. Pasiūlymų iš visuomenės negauta.

Nutarimų projektai buvo pateikti derinti Lietuvos Respublikos teisingumo ministerijai ir Ryšių reguliavimo tarnybai. Ryšių reguliavimo tarnyba per nustatytus terminus išvados nepateikė. Pagal Teisingumo ministerijos siūlymus 1 projektu keičiamas Planas buvo patikslintas, o į siūlymą dėl nustatomų terminų 1 projektą derinti su kibernetinius incidentus valdančiomis ir (ar)

tiriančiomis institucijomis neatsižvelgta, nes keičiamame Plane šioms institucijoms terminai naujai nėra nustatomi, o tik patikslinami atsižvelgiant į teisėkūros reikalavimus (vietoj termino „nedelsiant“, nustatomas terminas „nedelsiant, bet ne vėliau kaip per ...“).

Vadovaujantis Numatomo teisinio reguliavimo poveikio vertinimo metodikos, patvirtintos Lietuvos Respublikos Vyriausybės 2003 m. vasario 26 d. nutarimu Nr. 276 „Dėl Numatomo teisinio reguliavimo poveikio vertinimo metodikos patvirtinimo“, 4 punktu, Nutarimų projektų numatomo teisinio reguliavimo poveikio vertinimas neatliekamas.

Atsižvelgdami į tai, kad Nutarimų projektais įgyvendinamos 2018 m. sausio 1 d. įsigaliojusių įstatymų nuostatos, prašytume Nutarimų projektus įvertinti skubos tvarka.

Atsižvelgiant į tai, kad ryšių ir informacinių sistemų kibernetinis saugumas yra glaudžiai susijęs su elektroninių ryšių tinklų ir viešųjų elektroninių ryšių paslaugų nepertraukiamu veikimu (vientisumu), už kurio įgyvendinimo priežiūrą yra atsakinga Ryšių reguliavimo tarnyba, jos atstovą nuspręsta palikti Kibernetinio saugumo tarybos sudėtyje ir Lietuvos Respublikos Vyriausybės 2015 m. balandžio 23 d. nutarimo Nr. 422 „Dėl Kibernetinio saugumo tarybos sudarymo ir jos reglamento patvirtinimo“ nekeisti.

Nutarimų projektų rengimą inicijavo Krašto apsaugos ministerija. Nutarimų projektus parengė Krašto apsaugos ministerijos Teisės departamento (direktorė Judita Nagienė, tel. (8 5) 273 5545, el. p. judita.nagiene@kam.lt) Teisėkūros skyriaus (viršininkė Inga Šilinytė, tel. (8 5) 273 5563, el. p. inga.silinyte@kam.lt) vyr. specialistas Tomas Vainius (tel. (8 5) 263 5908, el. p. tomas.vainius@kam.lt) ir Krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų departamento (direktorius Jonas Skardinskas, tel. 8 706 80 800, el. p. jonas.skardinskas@kam.lt) Kibernetinio saugumo ir elektroninės informacijos saugos skyriaus viršininkas Artūras Litvaitis (tel. 8 706 80 806, el. p. arturas.litvaitis@kam.lt).

PRIDEDAMA:

1. 1 projektas, 1 lapas.
2. Planas, 9 lapai.
3. 2 projektas, 1 lapas.
4. 2 projekto lyginamasis variantas, 2 lapai.

Krašto apsaugos ministras



Raimundas Karoblis

T. Vainius, tel. (8 5) 263 5908, el. p. tomas.vainius@kam.lt
A. Litvaitis, tel. 8 706 80 806, el. p. arturas.litvaitis@kam.lt

LIETUVOS RESPUBLIKOS VYRIAUSYBĖ

NUTARIMAS

DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS 2016 M. SAUSIO 25 D. NUTARIMO NR. 87 „DĖL NACIONALINIO KIBERNETINIŲ INCIDENTŲ VALDYMO PLANO PATVIRTINIMO“ PAKEITIMO

Nr.
Vilnius

Lietuvos Respublikos Vyriausybė n u t a r i a:

Pakeisti Lietuvos Respublikos Vyriausybės 2016 m. sausio 25 d. nutarimą Nr. 87 „Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“ ir jį išdėstyti nauja redakcija:

„LIETUVOS RESPUBLIKOS VYRIAUSYBĖ

NUTARIMAS

DĖL NACIONALINIO KIBERNETINIŲ INCIDENTŲ VALDYMO PLANO PATVIRTINIMO

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

Patvirtinti Nacionalinį kibernetinių incidentų valdymo planą (pridedama).“

Ministras Pirmininkas

Krašto apsaugos ministras

Krašto apsaugos ministerijos
Teisės departamento direktorė
Judita Nagienė

KAMAD
Dokumentų administravimo
skyriaus vyr. specialistė
Jurgita Kulikauskaitė

Raimundas Karoblis
Krašto apsaugos ministras

NACIONALINIS KIBERNETINIŲ INCIDENTŲ VALDYMO PLANAS

I SKYRIUS BENDROSIOS NUOSTATOS

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

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

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

II SKYRIUS KIBERNETINIŲ INCIDENTŲ KLASIFIKAVIMO TVARKA

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

5. Kibernetiniai incidentai skirstomi į keturias kategorijas:

- 5.1. pavojingi kibernetiniai incidentai;
- 5.2. didelės reikšmės kibernetiniai incidentai;
- 5.3. vidutinės reikšmės kibernetiniai incidentai;
- 5.4. nereikšmingi kibernetiniai incidentai.

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

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

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

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

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

7.2. gali visiškai sutrikdyti (arba visiškai sutrikdo) ryšių ir informacinių sistemų veiklą ir taip gali sutrikdyti (sutrikdo) ryšių ir informacinių sistemų teikiamų paslaugų teikimą ilgiau nei valdytojo patvirtintuose ryšių ir informacinių sistemų kibernetinio saugumo politiką ir jos įgyvendinimą reglamentuojančiuose teisės aktuose (toliau – valdytojo kibernetinio saugumo teisės aktai) nurodytą didžiausią leistiną neveikimo terminą (toliau – leistinas neveikimo terminas). Leistinas neveikimo terminas turi būti suderintas su Nacionaliniu kibernetinio saugumo centru;

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

7.4. gali sukelti ekstremalųjį įvykį.

8. Atsižvelgdamas į kibernetinio incidento paplitimo mastą, nustatytus kriterijus, kuriais vadovaujantis kibernetinis incidentas priskiriamas Plano 5.2–5.4 papunkčiuose nurodytoms kategorijoms, ar kibernetinio incidento poveikį ryšių ir informacinei sistemai, Nacionalinis kibernetinio saugumo centras, gavęs iš tvarkytojo, ypatingos svarbos informacinės infrastruktūros valdytojo, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių

paslaugų teikėjo ar elektroninės informacijos prieglobos paslaugų teikėjo informaciją apie nustatytą kibernetinį incidentą, turi teisę patikslinti tvarkytojo, ypatingos svarbos informacinės infrastruktūros valdytojo, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjo ar elektroninės informacijos prieglobos paslaugų teikėjo priskirtą kibernetinio incidento kategoriją (priskirti didesnės ar mažesnės reikšmės kibernetinių incidentų kategorijai).

III SKYRIUS KIBERNETINIŲ INCIDENTŲ VALDYMAS

PIRMASIS SKIRSNIS KIBERNETINIŲ INCIDENTŲ PREVENCIJA, NUSTATYMAS IR VERTINIMAS

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

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

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

12. Tvarkytojai, ypatingos svarbos informacinės infrastruktūros valdytojai apie nustatytą kibernetinį incidentą pagal Plano 16 punkte nurodytą kompetenciją informuoja:

12.1. Nacionalinį kibernetinio saugumo centrą, vadovaudamiesi Vyriausybės patvirtintuose organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose valstybės informaciniais ištekliais ir ypatingos svarbos informacinei infrastruktūrai nustatyta tvarka;

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

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

13. Viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai ir elektroninės informacijos prieglobos paslaugų teikėjai (elektroninės informacijos prieglobos paslaugų teikėjams Plano 13.3 papunktis netaikomas) apie nustatytą kibernetinį incidentą pagal Plano 16 punkte nurodytą kompetenciją informuoja:

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

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

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

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

15. Nacionalinis kibernetinio saugumo centras, įvertinęs gautą informaciją apie kibernetinį incidentą, patvirtina arba, atsižvelgdamas į Plano 8 punktą, patikslina kibernetinio incidento kategoriją ir apie tai nedelsdamas 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. Kibernetinius incidentus valdanti ir (ar) tirianti institucija nedelsdama, bet ne vėliau kaip per 30 minučių nuo informacijos apie kibernetinį incidentą gavimo apie tai informuoja kitas kibernetinius incidentus valdančias ir (ar) tiriančias institucijas:

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

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

16.3. 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 ryšių ir informacinių sistemų veiklai atkurti.

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

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

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

21.1. renka, apdoroja informaciją, susijusią su kibernetiniu incidentu, ir ją pagal Plano 16.1–16.3 papunkčiuose nurodytą kompetenciją teikia kibernetinius incidentus valdančioms ir (ar) tiriančioms institucijoms;

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

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

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

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

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 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 kibernetinius incidentus valdančių ir (ar) tiriančių institucijų atstovai, tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų paskirti kompetentingi asmenys, atsakingi už kibernetinio saugumo organizavimą ir užtikrinimą, ir kiti tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų atstovai, kurių dalyvavimas reikalingas, siekiant suvaldyti kibernetinį incidentą;

22.5. turi teisę į Plano 22.4 papunktyje nurodytą pasitarimą pakviesti kitų kompetentingų ekspertų.

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

24. Nacionalinis kibernetinio saugumo centras apie pavojingo kibernetinio incidento nustatymą ir pavojingo kibernetinio incidento valdymo veiksmų eigą nedelsdamas, bet ne vėliau kaip per vieną valandą nuo pavojingo kibernetinio incidento nustatymo informuoja Lietuvos Respublikos krašto apsaugos ministeriją, Lietuvos Respublikos Vyriausybės kanceliariją, Lietuvos Respublikos Seimo kanceliariją ir Lietuvos Respublikos Prezidento kanceliariją ir kartu pateikia apibendrintą informaciją apie kibernetinį incidentą ir galimą jo poveikį.

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

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

27. Vyriausybės kanceliarija, Seimo kanceliarija ir Prezidento kanceliarija nedelsdamos, bet ne vėliau kaip per 8 valandas nuo informacijos apie pavojingą kibernetinį incidentą gavimo informuoja atitinkamai Ministrą Pirmininką, Seimo Pirmininką ir Prezidentą.

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

informuoja naudodamasis kibernetinio saugumo informaciniu tinklu ar kitomis saugiomis informacijos perdavimo priemonėmis.

29. Nacionalinis kibernetinio saugumo centras, nustatęs, kad nepakanka turimų kibernetinius incidentus valdančių ir (ar) tiriančių institucijų, tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų išteklių pavojingam kibernetiniam incidentui suvaldyti, nedelsdamas informuoja Krašto apsaugos ministeriją ir Vyriausybės kanceliariją. Krašto apsaugos ministras ne vėliau kaip per 4 valandas nuo anksčiau nurodytos informacijos gavimo priima sprendimą dėl pavojingo kibernetinio incidento valdymo priemonių.

30. 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.

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

32. Nesuvaldžius pavojingo kibernetinio incidento per leistiną neveikimo terminą, Nacionalinis kibernetinio saugumo centras nedelsdamas, bet ne vėliau kaip per vieną valandą nuo leistino neveikimo termino pabaigos informuoja apie tai Vyriausybės kanceliariją, taip pat informaciją apie kibernetinį incidentą ir tolesnius kibernetinio incidento valdymo veiksmus ir priemones (kartu su Vyriausybės pasitarimo protokolo projektu) pateikia Vyriausybei, kuri priima sprendimą dėl kibernetinio incidento valdymo veiksmų ir priemonių.

TREČIASIS SKIRSNIS

KIBERNETINIO INCIDENTO ANALIZĖ IR TARPINSTITUCINIS BENDRADARBIAVIMAS TIRIANT KIBERNETINIUS INCIDENTUS

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

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

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

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

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

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

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

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

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

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

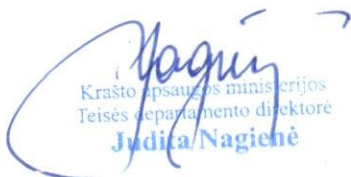
35.5. kibernetinio saugumo informaciniame tinkle paskelbia susistemintą ir aktualią informaciją apie kibernetinio incidento nustatymą ir suvaldymą;

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

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

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

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


Krašto apsaugos ministerijos
Teisės departamento direktorė
Jurgita Nagienė

KAMAD
Dokumentų administravimo
skyriaus vyr. specialistė
Jurgita Keli




Raimundas Karoblis
Krašto apsaugos ministras

LIETUVOS RESPUBLIKOS VYRIAUSYBĖ

NUTARIMAS

DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS 2015 M. KOVO 18 D. NUTARIMO NR. 281 „DĖL VALSTYBINĖS VARTOTOJŲ TEISIŲ APSAUGOS 2015–2018 METŲ STRATEGIJOS PATVIRTINIMO“ PAKAITIMO

Nr.
Vilnius

Lietuvos Respublikos Vyriausybė n u t a r i a:

Pakeisti Valstybinę vartotojų teisių apsaugos 2015–2018 metų strategiją, patvirtintą Lietuvos Respublikos Vyriausybės 2015 m. kovo 18 d. nutarimu Nr. 281 „Dėl Valstybinės vartotojų teisių apsaugos 2015–2018 metų strategijos patvirtinimo“:

1. Pakeisti priedo trisdešimt ketvirtąją pastraipą ir ją išdėstyti taip:

„	P-3-2-5; vartotojams ir verslo subjektams suteiktų rekomendacijų, konsultacijų ir (ar) metodinės pagalbos paslaugų kibernetinio saugumo klausimais (skleidžiant informaciją per žiniasklaidos priemones ir interneto svetaines www.nksc.lt , www.cert.lt) skaičius, vienetais	100	100	100	100	Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos“
---	--	-----	-----	-----	-----	--

2. Pakeisti priedo trisdešimt penktąją pastraipą ir ją išdėstyti taip:

„	P-3-2-6; interneto svetainėse www.nksc.lt ir www.cert.lt pateiktų rekomendacijų ir elektroninių priemonių, padėjusių Lietuvos interneto vartotojams, efektyvumas, procentais	70	75	80	85	Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos“
---	--	----	----	----	----	--

Ministras Pirmininkas

Teisingumo ministras

Krašto apsaugos ministerijos
Teisės departamento direktorė
Judita Vagienė

KAMAD
Dokumentų administravimas
skyriaus vyriausioji
Jurgita K.

R. Karolis
Raimundas Karolis
Krašto apsaugos ministras

LIETUVOS RESPUBLIKOS VYRIAUSYBĖ

NUTARIMAS

DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS 2015 M. KOVO 18 D. NUTARIMO NR. 281 „DĖL VALSTYBINĖS VARTOTOJŲ TEISIŲ APSAUGOS 2015–2018 METŲ STRATEGIJOS PATVIRTINIMO“ PAKEITIMO

Nr.
Vilnius

Lietuvos Respublikos Vyriausybė n u t a r i a:

Pakeisti Valstybinę vartotojų teisių apsaugos 2015–2018 metų strategiją, patvirtintą Lietuvos Respublikos Vyriausybės 2015 m. kovo 18 d. nutarimu Nr. 281 „Dėl Valstybinės vartotojų teisių apsaugos 2015–2018 metų strategijos patvirtinimo“:

1. Pakeisti priedo trisdešimt ketvirtąją pastraipą ir ją išdėstyti taip:

„		P-3-2-5; vartotojams ir verslo subjektams suteiktų rekomendacijų, konsultacijų ir (ar) metodinės pagalbos paslaugų kibernetinio saugumo klausimais (skleidžiant informaciją per žiniasklaidos priemones ir interneto svetaines www.nksc.lt , www.cert.lt , www.esaugumas.lt) skaičius, vienetais	100	100	100	100	Lietuvos Respublikos ryšių reguliavimo tarnyba Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos“
---	--	--	-----	-----	-----	-----	---

2. Pakeisti priedo trisdešimt penktąją pastraipą ir ją išdėstyti taip:

„		P-3-2-6; interneto svetainėje svetainėse www.nksc.lt ir www.cert.lt pateiktų rekomendacijų ir elektroninių priemonių, padėjusių Lietuvos interneto vartotojams, efektyvumas, procentais	70	75	80	85	Lietuvos Respublikos ryšių reguliavimo tarnyba Nacionalinis kibernetinio saugumo centras prie Krašto
---	--	--	----	----	----	----	--

							apsaugos ministerijos“
--	--	--	--	--	--	--	-----------------------------------

Ministras Pirmininkas

Teisingumo ministras



Raimundas Karoblis
Krašto apsaugos ministras



LIETUVOS RESPUBLIKOS TEISINGUMO MINISTERIJA

Biudžetinė įstaiga, Gedimino pr. 30, LT-01104 Vilnius,
tel. (8 5) 266 2984, faks. (8 5) 262 5940, el. p. rastine@tm.lt,
atsisk. sąskaita LT267044060000269484 AB SEB bankas, banko kodas 70440.
Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 188604955

Lietuvos Respublikos krašto apsaugos ministerijai

2018-01- Nr.

Į 2018-01-12 Nr. 12-01-44

DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMŲ PROJEKTŲ DERINIMO

Lietuvos Respublikos teisingumo ministerija, pagal kompetenciją išnagrinėjusi Lietuvos Respublikos Vyriausybės nutarimo „Dėl Lietuvos Respublikos Vyriausybės 2016 m. sausio 25 d. nutarimo Nr. 87 „Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“ (toliau – Planas) pakeitimo“ projektą (toliau – Nutarimo projektas) ir Lietuvos Respublikos Vyriausybės nutarimo „Dėl Lietuvos Respublikos Vyriausybės 2015 m. kovo 18 d. nutarimo Nr. 281 „Dėl Valstybinės vartotojų teisių apsaugos 2015–2018 metų strategijos patvirtinimo“ pakeitimo“ projektą, esminių pastabų ir pasiūlymų neturi.

Kartu atkreipiame dėmesį į tai, kad Nutarimo projektu tvirtinamo Plano 4 punkte įvedamas trumpinys „ryšių ir informacinės sistemos“. Atsižvelgiant į tai, siūlytina šį trumpinį vartoti ir Plano 16.1 papunktyje. Manytina, kad būtų tikslinga Nutarimo projektą derinti ir su Plano 16 punkte nurodytomis kibernetinius incidentus valdančiomis ir (ar) tiriančiomis institucijomis, atsižvelgiant į tai, kad Plano 16 punkte naujai nustatomas 30 minučių terminas, per kurį kibernetinius incidentus valdančios ir (ar) tiriančios institucijos turi informuoti kitas kibernetinius incidentus valdančias ir (ar) tiriančias institucijas. Ši pastaba taikoma ir kitų Plano punktų ir papunkčių, kuriais nustatomi nauji terminai, atžvilgiu.

Teisingumo viceministras

Giedrius Ruseckas

Jurgita Urbaitė, (8 5) 266 2924, el. p. jurgita.urbaite@tm.lt



**LIETUVOS RESPUBLIKOS VYRIAUSYBĖS KANCELIARIJA
TEISĖS GRUPĖ**

IŠVADA

**DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL LIETUVOS
RESPUBLIKOS VYRIAUSYBĖS 2016 M. SAUSIO 25 D. NUTARIMO NR. 87 „DĖL
NACIONALINIO KIBERNETINIŲ INCIDENTŲ VALDYMO PLANO PATVIRTINIMO“
PAKEITIMO“ PROJEKTO (toliau– Projektas) IR LIETUVOS RESPUBLIKOS
VYRIAUSYBĖS NUTARIMO „DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS 2015 M.
KOVO 18 D. NUTARIMO NR. 281 „DĖL VALSTYBINĖS VARTOTOJŲ TEISIŲ
APSAUGOS 2015–2018 METŲ STRATEGIJOS PATVIRTINIMO“ PAKEITIMO“
PROJEKTO (TAP-18-160; TAIS NR. 18-233(2))**

2018-02-19 Nr. NV-435

Vilnius

Įvertinę teikiamų projektų atitiktį įstatymams, Vyriausybės nutarimams ir teisės technikos reikalavimams, teikiame šias pastabas ir pasiūlymus:

1. Teisės aktų projektų, kuriuos Vyriausybė siūlo įtraukti į Seimo IV (pavasario) sesijos darbų programą, sąraše numatyta teikti Seimui svarstyti (gegužės mėn.) Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymo projektą, todėl šiame kontekste atkreiptinas dėmesys, kad poreikis keisti Projektą, įsigaliojus naujam įstatyminiam reguliavimui, bus sąlygotas dar kartą, o tai nesudaro galimybių teisėkūros ekonomiškumui. Šiame kontekste siūlytume įvertinti, ar šiuo metu vis tik tikslinga Planą dėstyti nauja redakcija, be kita ko, įvertinus tam tikrų atliekamų pakeitimų redakcinį pobūdį, taip pat tam tikras Plano nuostatas, kurios yra daugiau deklaratyvaus pobūdžio (atkartoja Kibernetinio saugumo įstatymo nuostatas) (pvz., Plano 10 punktas), arba stokoja įstatyminio pagrįstumo, pvz., Plano 17 punktas dėl reagavimo į kibernetinius incidentus vadovaujantis valdytojo kibernetinio saugumo teisės aktais ir pan.

Kartu pažymime, kad į minėto Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymo projektą turėtų būti įtrauktos nuostatos, aiškiai apibrėžiančios Projektu keičiamo Nacionalinio kibernetinių incidentų valdymo plano (toliau – Planas) turinį (reguliuojamų santykių apimtį), kadangi pagal šiuo metu galiojančio Kibernetinio saugumo įstatymo 18 straipsnio 3 dalį Nacionaliniame kibernetinių incidentų valdymo plane nustatoma tarpinstitucinio bendradarbiavimo tiriant kibernetinius incidentus tvarka ir kibernetinių incidentų klasifikavimo tvarka, tuo tarpu Plano turinys apima ne tik tuos aspektus, bet ir institucijų 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, taip pat tarpinstitucinę kibernetinių incidentų valdymo sąveiką.

2. Išlieka aktualus poreikis tikslinti reguliavimą Plano 8 punkte, kadangi nėra apibrėžta, kokiais kriterijais vadovaujantis Nacionalinis kibernetinio saugumo centras turės teisę patikslinti kibernetinio incidento kategoriją, kokia tvarka ir kada tai bus atliekama ir pan.

3. Plano 24 ir 27 punktų kontekste turėtų būti sistemiškai peržiūrėta, kodėl pagal analogiją apie kibernetinį incidentą neinformuojamas krašto apsaugos ministras (tik ministerija), kai tuo tarpu pagal Plano 29 punktą ministras įsijungia tik tuomet, kad incidento nepavyksta suvaldyti. Kartu Plano 27, 29 punktuose aptariamą institucinį bendradarbiavimą siūlome įvertinti sistemiškai,

pvz., priskiriant tiesioginius informavimo įgaliojimus krašto apsaugos ministrui, įvertinus siekį konsoliduoti informacinių išteklių saugumo sritį.

4. Plano 32 punkto nuoroda, kad Vyriausybė *priima sprendimą* dėl kibernetinio incidento valdymo veiksmų ir priemonių, suponuoja, kad tai atliekama Vyriausybės posėdyje priimant Vyriausybės nutarimą, tačiau tai nekoreliuoja su prieš tai šiame punkte nurodyta išlyga „kartu su Vyriausybės pasitarimo protokolo projektu“. Aptariama nuostata, mūsų nuomone, turėtų būti dėstoma taip, kad pakaktų Vyriausybės pasitarimo lygmens. Kartu siūlome Plano 29, 32 punktuose suvienodinti nuorodas kibernetinio incidento valdymo *priemonės, veiksmai*.

5. Mūsų nuomone, Plano 7.2 papunkčio paskutinis sakinyss „Leistinas neveikimo terminas turi būti suderintas su Nacionaliniu kibernetinio saugumo centru“ yra ne šio teisės akto reguliavimo dalykas, o, pvz., valdytojo kibernetinio saugumo teisės aktų rengimo (derinimo) proceso dalis.

6. Siūlome įvertinti, akcentuojant tai, kad poįstatyminiuose teisės aktuose vengiama perrašyti įstatymo nuostatų, ar Plano 12 ir 13 punktuose tikslinga pakartotinai išskirti Kibernetinio saugumo įstatymo 13-16 straipsniuose nurodytų subjektų pareigas teikti tam tikrą informaciją.

7. Siūlome tikslinti redakciniu aspektu Plano 16 punktą („informuoja *kitas* <...> institucijas“). Kartu atkreipiame dėmesį į neapibrėžtą nuorodą „*kitomis* informacijos perdavimo priemonėmis“ (Plano 33 punktas).

8. Pastebime, kad Plane vartojamas terminas „nedelsiant“ tam tikrais atvejais sukonkretinamas nurodant maksimalų laiko tarpą veiksams atlikti, tačiau tam tikrais atvejais – ne. Siūlome reguliavimą tikslinti sistemiškai (pvz., žr. Plano 15, 29 punktus).

Plane išskiriami terminai (pvz., per 30 min, per vieną valandą, per 8 valandas) taip pat turėtų būti įvertinti ir jų užtikrinimo aspektu, nes tam tikri laikotarpiai gali būti nerealizuojami, pvz., ne darbo ar švenčių dienomis.

9. Plano turinys turi būti peržiūrėtas sistemiškai atsisakant vertinamojo pobūdžio nuorodų, pvz., „visiškai“, „visų įmanomų“, „didžiausi“ ir pan.

10. Atkreipiame dėmesį, kad pagal Teisės aktų projektų rengimo rekomendacijas, kurias tvirtina teisingumo ministras, teisės aktuose vengtina nuorodų į žemesnės galios teisės aktus, be to, pateikiamos nuorodos turi atitikti anksčiau minėtų rekomendacijų reikalavimus (pvz., Plano 6, 13 punktai).

Teisės grupės vyresnioji patarėja

Eglė Gasiūnaitė