LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTRAS

ĮSAKYMAS DĖL KIBERNETINIŲ INCIDENTŲ VALDYMO VIDAUS REIKALŲ MINISTERIJOS VALDOMOSE YPATINGOS SVARBOS INFORMACINĖSE INFRASTRUKTŪROSE PLANO PATVIRTINIMO

2017 m. rugsėjo 20 d. Nr. 1V-651

Vilnius

Vadovaudamasis Lietuvos Respublikos kibernetinio saugumo įstatymo 14 straipsnio 5 dalimi:

T v i r t i n u Kibernetinių incidentų valdymo Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose planą (pridedama).

Vidaus reikalų ministras Eimutis Misiūnas

PATVIRTINTA
Lietuvos Respublikos vidaus reikalų
ministro 2017 m. rugsėjo 20 d.
įsakymu Nr. 1V-651

KIBERNETINIŲ INCIDENTŲ VALDYMO VIDAUS REIKALŲ MINISTERIJOS VALDOMOSE YPATINGOS SVARBOS INFORMACINĖSE INFRASTRUKTŪROSE PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kibernetinių incidentų valdymo Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose plano (toliau – Planas) paskirtis – nustatyti procedūras, Vidaus reikalų ministerijai, kaip ypatingos svarbos informacinių infrastruktūrų valdytojai (toliau – valdytojas), atliekamas siekiant tinkamai valdyti kibernetinius incidentus, nustatytus ypatingos svarbos informacinėse infrastruktūrose.

2. Planas galioja ypatingos svarbos informacinėms infrastruktūroms, nurodytoms Ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąraše, patvirtintame Lietuvos Respublikos Vyriausybės 2017 m. kovo 8 d. nutarimu Nr. 177-2 „Dėl Ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašo patvirtinimo“ ir kurių valdytojas yra Vidaus reikalų ministerija (toliau – Infrastruktūros). Infrastruktūros nurodytos Plano 10 priede. Plano nuostatos taikomos visoms Infrastruktūroms, jei Plane nenurodyta kitaip. Plano nuostatos *mutatis mutandis* taip pat taikomos kibernetinių incidentų valdymui Vidaus reikalų ministerijos valdomuose ir Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – IRD) tvarkomuose valstybės informaciniuose ištekliuose - informacinėse sistemose ir registruose, kurie nėra Infrastruktūros ar jų sudėtinės dalys, tačiau yra susiję ir teikia paslaugas Infrastruktūroms, kiek to nereglamentuoja atitinkamų valstybės informacinių išteklių veiklos tęstinumo valdymo planai, patvirtinti šių valstybės informacinių išteklių valdytojų.

3. Infrastruktūrų architektūrą, konfigūraciją, nustatymus aprašo ir saugo IRD Telekomunikacijų administravimo skyrius ir IRD Sistemų infrastruktūros administravimo skyrius.

4. Infrastruktūrų neveikimo sukeliamas poveikis, žala, didžiausias leistinas Infrastruktūrų neveikimo terminas nurodyti Plano 10 priede.

5. Plane vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Nacionaliniame kibernetinių incidentų valdymo plane, patvirtintame Lietuvos Respublikos Vyriausybės 2016 m. sausio 25 d. nutarimu Nr. 87 „Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos

informacinei infrastruktūrai ir valstybės informaciniams ištekliams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“ ir Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, vartojamas sąvokas.

II SKYRIUS
KIBERNETINIO INCIDENTO VALDYMO ORGANIZAVIMAS

6. Už Infrastruktūrų kibernetinio saugumo organizavimą ir užtikrinimą atsakingas yra IRD. Jei Plane nenurodyta kitaip, už IRD funkcijų pagal Planą vykdymą atsako IRD Informacinių ir telekomunikacinių technologijų pagalbos grupė (toliau – ITT Pagalbos grupė).

7. Asmenų, dalyvaujančių kibernetinio incidento valdymo veikloje, kontaktinė informacija ir funkcijos, išskyrus vietinių tinklų administratorių kontaktinę informaciją, nurodytos Plano 5 priede. Vietinių tinklų administratorių sąrašas ir kontaktinė informacija saugoma ITT Pagalbos grupėje.

8. Kibernetinio incidento valdymo metu informacija keičiamasi tarnybiniu elektroniniu paštu, tarnybiniu fiksuotu telefono ryšiu, tarnybiniu mobiliuoju ryšiu, naudojant Informacinių ir telekomunikacinių technologijų pagalbos posistemę (toliau – ITT pagalbos posistemė), Kibernetinio saugumo informacinį tinklą.

9. Kibernetinių incidentų kategorijos nustatomos pagal kibernetinių incidentų grupes ir kriterijus, pateiktus Plano 1 priede.

10. IRD valdo kibernetinį incidentą, jei Nacionalinis kibernetinio saugumo centras (toliau – Centras) neperima kibernetinio incidento valdymo. Jeigu Centras informuoja, kad perima kibernetinio incidento valdymą, IRD atlieka Plano V ir VI skyriuose nurodytus veiksmus, taip pat vadovaujasi Nacionaliniu kibernetinių incidentų valdymo planu ir vykdo Centro nurodymus dėl kibernetinio incidento valdymo.

11. IRD kreipiasi pagalbos į Centrą, naudodamasis Plano 6 priede pateiktais kontaktiniais duomenimis, jeigu nustatoma, kad negalės savarankiškai suvaldyti kibernetinio incidento per didžiausią leistiną Infrastruktūrų neveikimo terminą, nustatytą Plano 10 priede.

12. Jeigu Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Policija) ir (arba) Valstybinė duomenų apsaugos inspekcija (toliau – Inspekcija) paprašo

patikslinti arba papildyti informaciją apie kibernetinį incidentą, IRD organizuoja papildomos informacijos surinkimą ir pateikimą informacijos prašančiai institucijai jos nustatytu laiku.

13. Kibernetinio incidento valdymo schema pateikta Plano 7 priede.

III SKYRIUS
KIBERNETINIO INCIDENTO NUSTATYMAS

14. Pagrindiniai šaltiniai, kuriais naudojantis gali būti sukeltas kibernetinis incidentas ir sutrikdyta Infrastruktūrų veikla, nurodyti Plano 8 priede.

15. Informacija apie galimą kibernetinį incidentą gaunama iš: IRD darbuotojų, atliekančių Infrastruktūrų bei jų saugą užtikrinančių priemonių stebėseną, Centro ar IRD valdomų automatizuotų kibernetinių incidentų aptikimo priemonių, kompetentingų valstybės institucijų, kitų juridinių arba fizinių asmenų, taip pat kitų valstybių, tarptautinių organizacijų arba institucijų, atliekančių kibernetinio saugumo užtikrinimo funkcijas, ir kitų šaltinių.

16. ITT Pagalbos grupė, gavusi iš 15 punkte nurodytų šaltinių informacijos apie galimą kibernetinį incidentą, per kuo trumpesnį laiką užregistruoja kibernetinį incidentą, užpildydama kibernetinio incidento elektroninę registravimo formą (Plano 9 priedas), nustato šioje informacijoje minimos techninės įrangos fizinę buvimo vietą bei už jos priežiūrą atsakingą vietinio tinklo administratorių ir pateikia šią informaciją IRD Telekomunikacijų administravimo skyriaus arba IRD Sistemų infrastruktūros administravimo skyriaus darbuotojui (toliau – incidento koordinatorius) įvertinti. Jei apie kibernetinį incidentą praneša IRD Telekomunikacijų administravimo skyriaus arba IRD Sistemų infrastruktūros administravimo skyriaus darbuotojas, jis nedelsdamas pradeda vykdyti 17 punkte nurodytus veiksmus.

17. Incidento koordinatorius, įvertinęs jam pateiktą informaciją, pagal kompetenciją patvirtina arba paneigia kibernetinio incidento nustatymo faktą ir informuoja apie tai ITT pagalbos grupę. Siekiant kuo greičiau atlikti šį veiksmą, Incidento koordinatorius bendradarbiauja su informacijos šaltiniu, vietinio tinklo administratoriais, Centru ir kitais subjektais. Vietinių tinklų, kuriuose užfiksuotas kibernetinis incidentas, administratoriai privalo vykdyti IRD incidento koordinatoriaus nurodymus, imtis visų galimų priemonių kibernetiniam incidentui suvaldyti ir per nustatytą terminą užpildyti pranešimų apie kibernetinį incidentą formas bei pateikti jas IRD.

18. Jeigu kibernetinio incidento buvimo faktas paneigiamas, kibernetinio incidento valdymas baigiamas ir apie tai ITT Pagalbos grupė informuoja Centrą (jeigu kibernetinio incidento informacijos šaltinis yra Centras). Jeigu kibernetinio incidento faktas patvirtinamas, ITT Pagalbos grupė:

18.1. apie nustatytą kibernetinį incidentą ir jo koordinatorių per kuo trumpesnį laiką informuoja Plano 5 priede nurodytus asmenis (jeigu jiems tai būtina žinoti pagal atliekamas

funkcijas);

18.2. remdamasi Plano 6 priede pateiktais kontaktiniais duomenimis, apie nustatytą kibernetinį incidentą praneša Centrui (Plano 2 priedas) Organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose nustatyta tvarka;

18.3. jei kibernetinis incidentas galimai turi nusikalstamos veikos požymių, suderinusi su saugos įgaliotiniu, remdamasi Plano 6 priede pateiktais kontaktiniais duomenimis, pagal kompetenciją informuoja apie šį faktą Policiją Informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veikos požymių, užkardyti ir tirti, pateikimo, policijos nurodymų vykdymo bei kibernetinių incidentų tyrimo tvarkos aprašo, patvirtinto Lietuvos policijos generalinio komisaro 2015 m. vasario 2 d. įsakymu Nr. 5-V-101 „Dėl Informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veikos požymių, užkardyti ir tirti, pateikimo, policijos nurodymų vykdymo bei kibernetinių incidentų tyrimo tvarkos aprašo patvirtinimo“ nustatyta tvarka ir sąlygomis;

18.4. jei kibernetinis incidentas yra susijęs su asmens duomenų saugumo pažeidimais, suderinusi su saugos įgaliotiniu, remdamasi Plano 6 priede pateiktais kontaktiniais duomenimis, pagal kompetenciją informuoja apie šį faktą Inspekciją Informacijos apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo, patvirtinto Valstybinės duomenų apsaugos inspekcijos direktoriaus 2015 m. vasario 25 d. įsakymu Nr. 1T-11(1.12.E) „Dėl Informacijos apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo ir rekomenduojamos Informacijos apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones pateikimo Valstybinei duomenų apsaugos inspekcijai formos patvirtinimo“ nustatyta tvarka ir sąlygomis.

IV SKYRIUS
KIBERNETINIO INCIDENTO VERTINIMAS

19. Kibernetinio incidento vertinimo metu Incidento koordinatorius organizuoja informacijos, nustatytos Plano 3 priede apie kibernetinį incidentą, surinkimą. Vietinio tinklo administratoriai pagal kompetenciją teikia informaciją ir vykdo Incidento koordinatoriaus ir Centro nurodymus.

20. IRD Sistemų infrastruktūros administravimo skyrius, IRD Telekomunikacijų administravimo skyrius, IRD Informacinių technologijų paslaugų skyrius, IRD Informacinių sistemų plėtros skyrius ir kiti padaliniai (toliau – IRD padaliniai) pagal kompetenciją kibernetinio incidento vertinimo metu imasi veiksmų kibernetinio incidento įrašų išsaugojimui, jų patikimumui,

vientisumui ir pasiekiamumui užtikrinti.

21. Jeigu kibernetinis incidentas priskirtas vidutinės arba didelės reikšmės kibernetinių incidentų kategorijai, Incidento koordinatorius:

21.1. įvertinęs kibernetinį incidentą ir apibendrinęs visą surinktą informaciją, per kuo trumpesnį laiką pateikia ją Plano 5 priede nurodytiems asmenims (jeigu jiems tai būtina žinoti pagal atliekamas funkcijas);

21.2. pateikia kibernetinio incidento vertinimą (Plano 3 priedas) Centrui:

21.2.1. didelės reikšmės kibernetinio incidento – ne vėliau kaip per 2 valandas nuo jo nustatymo;

21.2.2. vidutinės reikšmės kibernetinio incidento – ne vėliau kaip per 24 valandas nuo jo nustatymo.

V SKYRIUS
KIBERNETINIO INCIDENTO SUVALDYMAS

22. Siekiant suvaldyti kibernetinį incidentą ir atkurti įprastą Infrastruktūrų veiklą, Plano 5 priede nurodyti asmenys, atlikdami savo funkcijas, imasi visų galimų organizacinių, techninių ir teisinių priemonių (toliau – kibernetinio incidento valdymo priemonės). Tuo atveju, kai Infrastruktūra yra valstybės informacinė sistema ar registras, vadovaujamasi šiuo Planu ir patvirtintu Infrastruktūros veiklos tęstinumo valdymo planu.

23. Valdant kibernetinį incidentą, siekiama:

23.1. sustabdyti ar bent apsunkinti kibernetinio incidento poveikio ir (ar) jo keliamos žalos plitimą Infrastruktūrose (stabdymas);

23.2. išsaugoti kuo daugiau Infrastruktūrų techninės ir programinės įrangos įrašų apie kibernetinį incidentą (įrašų išsaugojimas);

23.3. pašalinti Infrastruktūrų techninės ir programinės įrangos pažeidžiamumus, kuriuos išnaudojus kilo kibernetinis incidentas ar bent neleisti šių pažeidžiamumų išnaudoti (pažeidžiamumų šalinimas);

23.4. įsitikinti, kad kibernetinis incidentas tomis pačiomis ar panašiomis aplinkybėmis negalės pasikartoti (uždarymas).

24. Pagrindiniai kriterijai, kuriais vadovaujantis priimami sprendimai dėl kibernetinio incidento valdymo priemonių:

24.1. nurodytų Plano 5 priede asmenų pasiūlymai dėl kibernetinio incidento valdymo;

24.2. numatytas galimas poveikis ir žala, nurodyti Plano 10 punkte;

24.3. kibernetinio incidento įrašų išsaugojimo, jų patikimumo, vientisumo ir pasiekiamumo užtikrinimas;

24.4. didžiausias leistinas Infrastruktūrų neveikimo terminas, nustatytas Plano 10 priede;

24.5. kibernetinio incidento valdymo sprendimams įgyvendinti reikalingas laikas ir ištekliai;

24.6. turimo laiko ir išteklių efektyvus paskirstymas vienu metu valdant daugiau nei vieną kibernetinį incidentą;

24.7. kita galima žala, kurią gali padaryti kibernetinis incidentas, priėmus jo valdymo sprendimus.

25. Jeigu kibernetinis incidentas priskirtas nereikšmingų kibernetinių incidentų kategorijai, Incidento koordinatorius, atsižvelgdamas į kibernetinio incidento tipą ir galimas jo valdymo priemones, parenka ir taiko efektyviausias galimas kibernetinio incidento valdymo priemones.

26. Jeigu kibernetinis incidentas priskirtas vidutinės ir didelės reikšmės kibernetinių incidentų kategorijai:

26.1. Incidento koordinatorius teikia informaciją Plano 5 priede nurodytus asmenims (jeigu jiems tai būtina žinoti pagal atliekamas funkcijas) apie kibernetinio incidento įvertinimą ir galimas kibernetinio incidento valdymo priemones;

26.2. nurodyti Plano 5 priede asmenys, iš Incidento koordinatoriaus gavę išsamią informaciją apie galimas kibernetinio incidento valdymo priemones, per kuo trumpesnį laiką įvertina padėtį ir priima sprendimą dėl efektyviausių ir mažiausiai žalos padarysiančių kibernetinio incidento valdymo priemonių taikymo ir jas taiko;

26.3. suvaldžius kibernetinį incidentą, ITT pagalbos grupė apie kibernetinio incidento suvaldymo rezultatus informuoja Plano 5 priede nurodytus asmenis (jeigu jiems tai būtina žinoti pagal atliekamas funkcijas);

26.4. IRD padaliniai pagal kompetenciją per kuo trumpesnį laiką nuo kibernetinio incidento sustabdymo imasi priemonių pažeidžiamumui, dėl kurio įvyko kibernetinis incidentas, pašalinti;

26.5. apie kibernetinio incidento suvaldymą ITT pagalbos grupė per kuo trumpesnį laiką informuoja Centrą, o 18.3 ir 18.4 punktuose nustatytais atvejais – Policiją ir Inspekciją pagal kompetenciją ir praneša apie taikytas kibernetinio incidento valdymo priemones (Plano 3 priedas); Inspekcija informuojama, jei kibernetinis incidentas yra susijęs su asmens duomenų saugumo pažeidimais, Policija informuojama, jei kibernetinis incidentas galimai turi nusikalstamos veikos požymių, informacija Policijai ir Inspekcijai teikiama suderinus su saugos įgaliotiniu;

26.6. visi šiame punkte nurodyti asmenys ir subjektai bendrauja ir keičiasi informacija, efektyviai panaudodami prieinamas, 8 punkte nurodytas komunikavimo priemones. Esant poreikiui gali būti sušaukiamas pasitarimas.

VI SKYRIUS
INFRASTRUKTŪRŲ VEIKLOS ATKŪRIMAS

27. IRD padaliniai pagal kompetenciją įvertina Infrastruktūrų būklę, nustato pažeistas jų dalis ir per kuo trumpesnį laiką imasi veiksmų pažeistoms dalims atkurti arba pakeisti ir (arba) teikia Plano 5 priede nurodytiems asmenims (jeigu jiems tai būtina žinoti pagal atliekamas funkcijas) siūlymus dėl pažeistų dalių atkūrimo arba pakeitimo, jeigu to negali padaryti savo jėgomis.

28. Prieš atkuriant Infrastruktūrų veiklą, IRD padaliniai pagal kompetenciją patvirtina, kad pašalinti pažeidžiamumai, dėl kurių įvyko kibernetinis incidentas ir (ar) įgyvendintos kitos priemonės, neleidžiančios šių pažeidžiamumų išnaudoti.

29. ITT Pagalbos grupė informuoja Centrą apie atkurtą Infrastruktūrų veiklą ir pašalintus pažeidžiamumus bei įgyvendintas kitas priemones, neleidžiančias šių pažeidžiamumų išnaudoti.

VII SKYRIUS
KIBERNETINIO INCIDENTO TYRIMAS

30. Didelės reikšmės kibernetinių incidentų tyrimą organizuoja Veiklos tęstinumo valdymo grupė, sudaryta IRD direktoriaus įsakymu. Vidutinės reikšmės ir nereikšmingi kibernetiniai incidentai paprastai netiriami, jie gali būti tiriami IRD direktoriaus pavedimu.

31. Kibernetinio incidento tyrimo metu įvertinami kibernetinio incidento (ar panašių ar susijusių kibernetinių incidentų grupės) nustatymo, vertinimo, valdymo, Infrastruktūrų veiklos atkūrimo veiksmai, atlikti dėl įvykusio kibernetinio incidento, siekiant sumažinti kibernetinių incidentų kilimo galimybę, efektyviau valdyti kibernetinius incidentus, efektyviau panaudoti turimus žmogiškuosius, techninius, programinius ir kitus išteklius, greičiau atkurti Infrastruktūrų veiklą.

32. Kibernetinio incidento tyrime dalyvauja Incidento koordinatorius ir kiti kibernetinio incidento suvaldyme dalyvavę asmenys.

33. Kibernetinio incidento tyrimo ataskaitą parengia Veiklos tęstinumo valdymo grupė, ataskaitoje pateikiami pasiūlymai valdytojo vadovui dėl Plano ir Infrastruktūrų kibernetinį saugumą reglamentuojančių teisės aktų ar kitų valdytojo vadovo patvirtintų dokumentų pakeitimo, kibernetinio saugumo būklės gerinimo ir papildomų kibernetinio saugumo priemonių įsigijimo ir (ar) kitų išteklių poreikio užtikrinimo.

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

34. Plano veiksmingumo išbandymas atliekamas periodiškai, bet ne rečiau, kaip kartą per metus. Plano veiksmingumo išbandymas gali būti neatliekamas IRD direktoriaus sprendimu, jei per praėjusius metus nuo paskutinio plano išbandymo buvo sėkmingai suvaldytas bent vienas didelės svarbos kibernetinis incidentas ir buvo atliktas jo tyrimas.

35. Plano veiksmingumo išbandymą organizuoja Veiklos tęstinumo valdymo grupė, sudaryta IRD direktoriaus įsakymu. Bandymo eigoje imituojamas kibernetinis incidentas ir kibernetinio incidento valdymo veikloje dalyvaujantys asmenys atlieka Plane numatytus veiksmus. IRD Informacijos saugos skyrius parengia bandymo ataskaitą (Plano 11 priedas) ir perduoda ją Centrui.

36. Atsižvelgdami į gautus Plano veiksmingumo išbandymo rezultatus, Plano veiksmingumo išbandymo veikloje dalyvavę asmenys, taip pat kibernetinio incidento valdymo veikloje dalyvavę asmenys, įvertinę kibernetinio incidento valdymo metu įgytą patirtį ir nustatę galimus teisinio reguliavimo trūkumus, pateikia valdytojo vadovui pasiūlymus dėl Plano ir Infrastruktūrų kibernetinį saugumą reglamentuojančių teisės aktų ar kitų valdytojo vadovo patvirtintų dokumentų pakeitimo, kibernetinio saugumo būklės gerinimo, papildomų kibernetinio saugumo priemonių įsigijimo. Plano atnaujinimą organizuoja IRD Informacijos saugos skyrius.

_____

Kibernetinių incidentų valdymo Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose plano
1 priedas

KIBERNETINIŲ INCIDENTŲ KATEGORIJŲ SĄRAŠAS

Kibernetinis incidentas		
Grupė	**Apibūdinimas**	**Kategorija**
Kenkimo programinė įranga (angl. *Malicious Software*)	Kenkimo programinė įranga, kai darbo ar tarnybinės stotys aktyviai kontroliuojamos įsibrovėlių (pavyzdžiui, užpakalinės durys (angl. *back door*) Modernios kenkimo programinės įrangos (angl. *advanced persistent threat, APT*) aptikimas RIS. Kenkimo programinė įranga, trikdanti RIS kibernetinio saugumo priemonių darbą	D[1]
	Kenkimo programinė įranga, kurios neaptinka RIS darbo stotyje veikianti antivirusinė programinė įranga. RIS veikianti kenkimo programinė įranga, kurią aptinka antivirusinė programinė įranga per reguliarų patikrinimą	V[2]
	RIS laikmenose ar darbo ir tarnybinėse stotyse veikianti kenkimo programinė įranga, kurią iš karto aptinka antivirusinė programinė įranga. Socialinės inžinerijos metodų naudojimas (manipuliavimas RIS naudotojų emocijomis ir psichologija, pastabumo stoka, technologijų neišmanymu), kai bandoma įtikinti RIS naudotoją atlikti grėsmę RIS keliančius veiksmus, tačiau RIS naudotojas atpažįsta grėsmę ir neatlieka kenkimo programinę įrangą aktyvinančių veiksmų	N[3]
Įsilaužimas	Vykdoma vidinė RIS žvalgyba ar kita įtartina veikla (prievadų skenavimas, slaptažodžių parinkimas, kita), aptikta RIS (neskaitant kenkimo programinės įrangos), sukėlusi RIS veiklos sutrikimus. Piktybiniai veiksmai prieš RIS kibernetinio saugumo priemones	D
	Vykdoma vidinė RIS žvalgyba ar kita įtartina veikla (prievadų skenavimas, slaptažodžių parinkimas, kita), aptikta RIS infrastruktūroje	V
Tinklo perimetro žvalgyba	Vykdoma aktyvi (slaptažodžių parinkimas, bandymai išnaudoti pažeidžiamumus, kita) RIS perimetro žvalgyba ar įtartina veikla (neskaitant kenksmingos programinės įrangos), mėginama paveikti RIS kibernetinio saugumo priemones	V
	Vykdoma RIS perimetro priemonių žvalgyba (nebandant įsilaužti)	N
Tinklo trikdymas	Veiksmas, ilgiau nei 4 valandoms sutrikdęs RIS veiklą	D
	Veiksmas, kuriuo trikdoma (angl. *Denial of Service, DoS*) RIS veikla	V
Neteisėta veika	Vagystė, apgavystė ir panašūs kriminalinio pobūdžio kibernetiniai incidentai	V
Vientisumo pažeidimas	RIS ar jo dalies pažeidimas, sutrikdantis RIS teikiamų paslaugų nepertraukiamą teikimą, galintis turėti įtakos tvarkomų duomenų ir teikiamų paslaugų patikimumui, iškreipti turinį ir mažinti RIS naudotojų pasitikėjimą jais	V

[1] Didelės reikšmės kibernetinis incidentas.
[2] Vidutinės reikšmės kibernetinis incidentas.
[3] Nereikšmingas kibernetinis incidentas.

_____

Kibernetinių incidentų valdymo Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose plano
2 priedas

INFORMATIKOS IR RYŠIŲ DEPARTAMENTAS
PRIE LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS

Šventaragio g. 2, LT- 01510 Vilnius,
tel. (8 5) 271 7177, faks. (8 5) 271 8921, el. p. ird@vrm.lt

Kibernetinio saugumo ir telekomunikacijų
tarnybai prie Krašto apsaugos ministerijos
Šilo g. 5A, 10322 Vilnius
cert@nksc.lt

PRANEŠIMAS
APIE KIBERNETINĮ INCIDENTĄ

_____ Nr._____
(data)

Kontaktinė informacija	Atsakingo už kibernetinio incidento vertinimą asmens vardas, pavardė:
	Pareigos:
	Adresas:
	Telefonas, el. pašto adresas:
Kibernetinio incidento apibūdinimas	**Kibernetinio incidento grupė:** ☐ kenkimo programinė įranga (angl. *Malicious Software*) ☐ įsilaužimas ☐ RIS[1] perimetro žvalgyba ☐ RIS trikdymas ☐ neteisėta veika ☐ vientisumo pažeidimas
	Trumpas kibernetinio incidento apibūdinimas (nurodyti kiek įmanoma detalesnę informaciją):
	Tiksli data, laikas ir fizinė vieta, kada ir kur kibernetinis incidentas įvyko ir nustatytas: 2017- ____ - ____ , _____ val. _____ min.,
	Kibernetinio incidento kategorija: ☐ didelės reikšmės kibernetinis incidentas ☐ vidutinės reikšmės kibernetinis incidentas ☐ nereikšmingas kibernetinis incidentas
	Kibernetinio incidento poveikis[2]:

	☐ gali paveikti viešuosius ryšių tinklus, viešąsias elektroninių ryšių ir elektroninės informacijos prieglobos paslaugas ☐ gali turėti nusikalstamos veikos požymių ☐ gali būti susijęs su asmens duomenų saugumo pažeidimais
Kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo pateikimo dienos, skaičius[3]	
Kibernetinio incidento šalinimo tvarka (turi būti nurodyta, ar tai prioritetas, ar ne)	
Kita svarbi informacija	

[1] Ypatingos svarbos informacinė infrastruktūra ir valstybės informaciniai ištekliai.
[2] Jei nėra žinoma, nurodyti nereikia.
[3] Informacija pateikiama tik pranešime apie nereikšmingą incidentą.

_____

Kibernetinių incidentų valdymo Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose plano
3 priedas

INFORMATIKOS IR RYŠIŲ DEPARTAMENTAS
PRIE LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS

Šventaragio g. 2, LT- 01510 Vilnius,
tel. (8 5) 271 7177, faks. (8 5) 271 8921, el. p. ird@vrm.lt

DIDELĖS IR VIDUTINĖS REIKŠMĖS KIBERNETINIO INCIDENTO VERTINIMO ATASKAITA

_____ Nr._____
(data)

Kontaktinė informacija	Atsakingo už kibernetinio incidento vertinimą asmens vardas, pavardė:
	Pareigos:
	Adresas:
	Telefonas, el. pašto adresas:
Kibernetinio incidento vertinimas	**RIS[1], kurioje nustatytas kibernetinis incidentas, tipas:** ☐ informacinė sistema ☐ registras ☐ elektroninių ryšių tinklas ☐ tarnybinė stotis ☐ kitas
	Kibernetinio incidento veikimo trukmė: *Nurodomas laikotarpis, kurio metu incidentas nebuvo suvaldytas, pvz. nuo NKSC pranešimo iki kompiuterio atjungimo.*
	Kibernetinio incidento šaltinis: *Nurodoma analizės metu nustatytos aplinkybės, naudotojo veiksmai, kurie galimai tapo incidento priežastimi: pvz. prijungta USB laikmena, naudotojo gautas ir atidarytas el. laiškas su žalingą kodą turinčiu priedu ar pan.*
	Kibernetinio incidento požymiai: *Jei naudotos priemonės atpažino ir automatiškai sunaikino kenkimo kodą ar blokavo kenksmingus sujungimus, pakanka nurodyti atpažinto kodo pavadinimą ir prie pranešimo prisegti naudota priemone sugeneruotą patikrinimo ataskaitą.* *Kitais atvejais nurodomi požymiai, kurie leidžia identifikuoti analogiškus atvejus: pvz. kompiuteryje tam tikrame kataloge rasti failai (pavadinimai, HASH sumos), startup kataloge susikūrę automatinio paleidimo įrašai, procesų monitoriuje matomi pašaliniai procesai, fiksuojamos TCP\IP sesijos su domenais a,b,c ar IP adresais 1,2,3.* *Kai nepavyksta nustatyti incidento požymių, rekomenduojame:* - *Microsoft programą „Autoruns“: https://technet.microsoft.com/en-us/sysinternals/bb963902 Įvykdyti komandą* ***autorunsc.exe -a* -c > komp_name.csv Prie pranešimo NKSC pridėti zip formatu archyvuotą***

	sugeneruotos csv. ataskaitos failą. - ***Įdiegti pagal NKSC portale pateikiamas instrukcijas FireEye HX agentą.***
	Kibernetinio incidento veikimo metodas: *Jeigu pavyko nustatyti kenkimo procesą, prisegama Jūsų turimo Sandbox sprendimo sugeneruota analizė.*
	Galimos kibernetinio incidento pasekmės: *Jeigu pavyko nustatyti, nurodoma padaryta žala*
	Kibernetinio incidento poveikio pasireiškimo (galimo išplitimo) mastas: *Nurodoma paveiktų kompiuterių, tinklų kiekis, kokiose zonose (serveriai, technologinis tinklas, administracijos darbo stotys ir pn.)*
	Kibernetinio incidento būsena: ☐ aktyvus (jeigu nepavyksta pašalinti incidento) ☐ pasyvus
	Priemonės, kuriomis kibernetinis incidentas: *Nurodomi tyrimui naudotų priemonių pavadinimai*
	Galimos kibernetinio incidento valdymo priemonės: *Nurodomi veiksmai, kurių imtasi incidentui suvaldyti.*
Kita svarbi informacija	*Nurodoma valdytojo nustatyta kibernetinio incidento kategorija, nuoroda į pranešimą apie šį incidentą.* *Nurodoma, ar incidentas turi galimai nusikalstamos veikos požymių, taip pat ar incidentas susijęs su asmens duomenų saugumo pažeidimu.* *Nurodomos institucijos, kurios buvo informuotos apie šį incidentą, kita svarbi informacija.*

[1] Ypatingos svarbos informacinė infrastruktūra ir valstybės informaciniai ištekliai.

_____

Kibernetinių incidentų valdymo Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose plano
4 priedas

INFORMATIKOS IR RYŠIŲ DEPARTAMENTAS
PRIE LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS

Šventaragio g. 2, LT- 01510 Vilnius,
tel. (8 5) 271 7177, faks. (8 5) 271 8921, el. p. ird@vrm.lt

PRANEŠIMAS
APIE DIDELĖS IR VIDUTINĖS REIKŠMĖS KIBERNETINIO INCIDENTO SUSTABDYMĄ IR PAŠALINIMĄ

_____ Nr._____
(data)

Kontaktinė informacija	Atsakingo už kibernetinio incidento vertinimą asmens vardas, pavardė:
	Pareigos:
	Adresas:
	Telefonas, el. pašto adresas:
Kibernetinio incidento apibūdinimas	Tiksli data ir laikas, kada kibernetinis incidentas sustabdytas ir pašalintas: 2017- ____ - ____ , _____ val. _____ min.
	Kibernetinio incidento atsiradimo priežastys (nurodyti kiek įmanoma detalesnę informaciją):
	Kibernetinio incidento šaltinis:
	Kibernetinio incidento pasekmės: ☐ informacijos/duomenų nutekėjimas ☐ informacijos/duomenų praradimas ☐ informacijos/duomenų iškraipymas ☐ veiklos sutrikimai ☐ operacijų ir/ar el. paslaugų sutrikimai ☐ patirta žala[1] ☐ padaryta žala reputacijai ☐ neautorizuoti pokyčiai sistemose ☐ įrangos sugadinimas ☐ įdiegtų saugumo priemonių panaikinimas, sugadinimas ☐ kitos (nurodyti kiek įmanoma detalesnę informaciją)
Taikytos kibernetinio incidento valdymo priemonės	Veiksmai, kurių imtasi sustabdant ir pašalinant kibernetinį incidentą, ir (arba) kibernetinio incidento pasekmes:
Kita svarbi informacija	

[1] Jeigu žinoma, nurodomi patirti nuostoliai (piniginė žalos išraiška).

_____

Kibernetinių incidentų valdymo Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose plano
5 priedas

ASMENŲ, DALYVAUJANČIŲ KIBERNETINIO INCIDENTO VALDYMO VEIKLOJE, KONTAKTINĖ INFORMACIJA IR FUNKCIJOS

Eil.Nr.	Vardas, pavardė	Kontaktinė informacija (telefono numeris, el. pašto adresas ir kt.) [1]	Funkcijos [2]
1.	Evaldas Serbenta	(8 5) 271 7240 evaldas.serbenta@vrm.lt	Tvirtina sprendimus dėl didelės reikšmės kibernetinių incidentų
2.	Artūras Kavolis	(8 5) 271 7176 arturas.kavolis@vrm.lt	Vadovauja Veiklos atkūrimo valdymo grupei, priima sprendimus, koordinuoja incidentų valdymą, koordinuoja IRD padalinių veiksmus
3.	ITT pagalbos grupė	(8 5) 271 7777 ittpagalba@vrm.lt http://ittpagalba.vrm.lt/	Registruoja kibernetinius incidentus ir nukreipia juos vykdyti, teikia pranešimus ir ataskaitas Centrui, vykdo IRD kontaktinio asmens funkcijas, tvarko ITT pagalbos posistemę
4.	Romualdas Šaulys	(8 5) 271 8477 romualdas.saulys@vrm.lt	Vadovauja ITT pagalbos grupei, konsultuoja incidento vertinimo, veiklos atkūrimo klausimais (4), ITT pagalbos posistemės funkcionavimo klausimais, koordinuoja ITPS darbuotojų veiksmus
5.	IRD Telekomunikacijų administravimo skyriaus budėtojas	+370 618 66590 vrtt@vrm.lt	Vykdo IRD kontaktinio asmens funkcijas
6.	Algimantas Saugėnas	(8 5) 271 7271 algimantas.saugenas@vrm.lt	Koordinuoja TAS darbuotojų veiksmus
7.	Jonas Vaitkevičius	(8 5) 271 7272 jonas.vaitkevicius@vrm.lt	Pagal kompetenciją vykdo stebėseną, patvirtina, vertina, stabdo, šalina incidentą, atkuria Infrastruktūrų veiklą; vykdo IRD kontaktinio asmens funkcijas
8.	Ramūnas Rulevičius	(8 5) 219 8634 ramunas.rulevicius@vrm.lt	Pagal kompetenciją vykdo stebėseną, patvirtina, vertina, stabdo, šalina incidentą, atkuria Infrastruktūrų veiklą
9.	Almantas Venckus	(8 5) 271 72 38 almantas.venckus@vrm.lt	Pagal kompetenciją vykdo stebėseną, patvirtina, vertina,

			stabdo, šalina incidentą, atkuria Infrastruktūrų veiklą
10.	Ramūnas Bakšys	(8 5) 271 7129 ramunas.baksys@vrm.lt	Atkuria veiklą (5)
11.	Jonas Ignatavičius	(8 5) 271 7383 jonas.ignatavicius@vrm.lt	Koordinuoja SIAS darbuotojų veiksmus
12.	Justinas Mačionis	(8 5) 271 8586 justinas.macionis@vrm.lt	Pagal kompetenciją vykdo stebėseną, patvirtina, vertina, stabdo, šalina incidentą, atkuria Infrastruktūrų veiklą
13.	Dmitrij Miasnikov	(8 5) 219 8637 dmitrij.miasnikov@vrm.lt	Pagal kompetenciją vykdo stebėseną, patvirtina, vertina, stabdo, šalina incidentą, atkuria Infrastruktūrų veiklą
14.	Renata Mačiulevičienė	(8 5) 271 8819 renata.maciuleviciene@vrm.lt	Organizuoja Plano tikslinimą ir atnaujinimą, konsultuoja teisiniais incidento vertinimo ir incidento tyrimo klausimais, įskaitant incidentus, kurie galimai turi nusikalstamos veikos požymių
15.	Bronius Dručiūnas	(8 5) 271 7195 bronius.druciunas@vrm.lt	Dalyvauja incidento tyrime, Plano veiksmingumo išbandyme, rengia tyrimo, Plano veiksmingumo išbandymo ataskaitą
16.	Valentinas Kraujalis	(8 5) 271 7376 valentinas.kraujalis@vrm.lt	Dalyvauja incidento tyrime, Plano veiksmingumo išbandyme, bendradarbiauja su EU LISA (2, 6)
17.	Romualda Jakelienė	(8 5) 271 8385 romualda.jakeliene@vrm.lt	Konsultuoja incidento vertinimo, veiklos atkūrimo klausimais (4)
18.	Augustinas Zeirys	(8 5) 271 7298 augustinas.zeirys@vrm.lt	Konsultuoja incidento vertinimo, veiklos atkūrimo klausimais (2, 6)
19.	Neringa Rukšėnienė	(8 5) 219 8649 neringa.rukseniene@vrm.lt	Konsultuoja incidento vertinimo, veiklos atkūrimo klausimais (7, 8, 9, 10)
20.	Vietinių tinklų administratoriai	Sąrašas saugomas ITT pagalbos grupėje, pateikiamas ITT pagalbos posistemėje	Vykdo kompiuterinių darbo vietų patikrą, atjungimą, įkalčių išsaugojimą, pildo pranešimų apie incidentus, įvykusius vietiniame tinkle, formas, vykdo IRD incidento koordinatoriaus nurodymus

[1] Mobiliųjų telefonų numerių sąrašas saugomas ITT pagalbos grupėje.

[2] Skliaustuose nurodytos Infrastruktūros, priklausančios funkcijos vykdytojo kompetencijai (Plano 10 priedo eilės numeriai).

Kibernetinių incidentų valdymo Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose plano
6 priedas

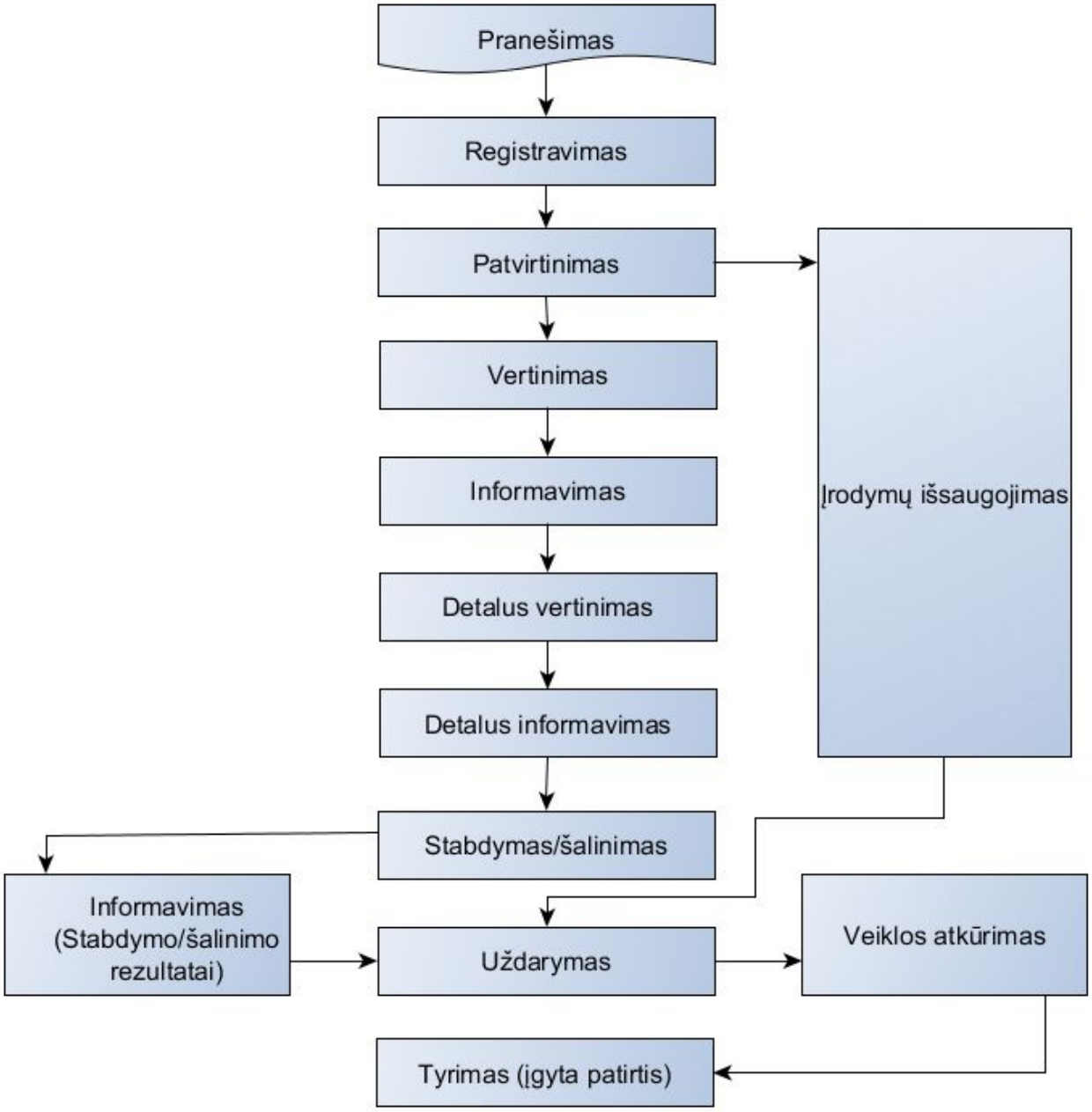
INSTITUCIJŲ, DALYVAUJANČIŲ KIBERNETINIO INCIDENTO VALDYMO VEIKLOJE, KONTAKTINĖ INFORMACIJA

Eil.Nr.	Institucija	Kontaktinė informacija (telefono numeris, el. pašto adresas)	Pastabos
1.	Kibernetinio saugumo ir telekomunikacijų tarnyba prie Lietuvos Respublikos krašto apsaugos ministerijos (Centras)	Tel. (8 5) 210 3849 cert@nksc.lt	
2.	Lietuvos kriminalinės policijos biuro Sunkaus ir organizuoto nusikalstamumo tyrimo 5-oji valdyba (Policija)	Tel. (8 5) 271 7933 donatas.mazeika@policija.lt	
3.	Valstybinė duomenų apsaugos inspekcija (Inspekcija)	www.ada.lt ada@ada.lt tel. (8 5) 271 8204 faks. (8 5) 261 9494	Pranešimai teikiami per interneto svetainę www.ada.lt naudojantis el. paslaugų sistema; nesant tokios galimybės, pranešimai teikiami el. paštu ada@ada.lt; nesant tokių galimybių, informuojama telefonu (8 5) 271 2804 arba faksu (8 5) 261 9494

_____

Kibernetinių incidentų valdymo Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose plano
7 priedas

KIBERNETINIO INCIDENTO VALDYMO SCHEMA



Kibernetinių incidentų valdymo Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose plano
8 priedas

PAGRINDINIAI ŠALTINIAI, KURIAIS NAUDOJANTIS GALI BŪTI SUKELTAS KIBERNETINIS INCIDENTAS, IR JŲ APRAŠYMAS

Eil.Nr.	Kibernetinio incidento šaltinis	Aprašymas
1.	Išorinės kompiuterinės laikmenos	Prijungiama apkrėsta laikmena (USB atmintinė, išorinis kietasis diskas, atminties kortelė, optinė laikmena ir pan.), gaunama neteisėta prieiga
2.	Internetas	Atsiunčiama apkrėsta programinė įranga arba nukreipiama į apkrėstą svetainę, gaunama neteisėta prieiga
3.	Interneto svetainių pagrindu veikianti programinė įranga	Išnaudojamas svetainės ar programinės įrangos pažeidžiamumas (žinomas arba ne), gaunama neteisėta prieiga arba sutrikdomas prieinamumas
4.	Elektroninis paštas	Atidarius apkrėstą el. laiško priedą ar pasinaudojus el. laiške esančia nuoroda į apkrėstą svetainę, gaunama neteisėta prieiga
5.	Prarasta įranga	Panaudojant prarastą (pamestą, pasisavintą ar pan.) įrangą ir (ar) joje esančią informaciją gaunama neteisėta prieiga
6.	Socialinė inžinerija	Apgaulės būdu žodžiu, telefonu, el. paštu, internetu ar kitu būdu atskleidžiama informacija, suteikianti galimybę gauti neteisėtą prieigą
7.	Paskirstyta paslaugos trikdymo ataka (angl. *Distributed denial of service, DDoS*)	Didelio kiekio fiktyvių užklausų teikimas išsemia infrastruktūros veikimui būtinus išteklius ir sutrikdomas jos prieinamumas
8.	Kiti kibernetinių incidentų šaltiniai	Kiti būdai (šantažas, spaudimas, papirkimas, fizinis įsilaužimas ir kt.) siekiant gauti neteisėtą prieigą, sutrikdyti prieinamumą

_____

Kibernetinių incidentų valdymo Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose plano
9 priedas

KIBERNETINIO INCIDENTO ELEKTRONINĖ REGISTRAVIMO FORMA

Informacija apie kibernetinį incidentą	
Registruojama minimali žinoma informacija apie kibernetinį incidentą, surenkama vertinant kibernetinį incidentą pagal Organizacinius ir techninius kibernetinio saugumo reikalavimus	

Kibernetinių incidentų valdymo Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose plano 10 priedas

VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ YPATINGOS SVARBOS INFORMACINIŲ INFRASTRUKTŪRŲ SĄRAŠAS

Eil. Nr.	Ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašo punkto numeris	Neveikimo sukeliamas poveikis, žala	Ilgiausias leistinas neveikimo laikas
1.	5	Neveikia šio priedo 2-4 ir 6-10 p. nurodytos Infrastruktūros	8 val.
2.	18	Sutrinka teisėsaugos institucijų darbas: valstybės sienos kirtimas, dokumentų išdavimas užsieniečiams, asmenų duomenų patikra (išduodant asmens dokumentus, sulaikius asmenį ir kt. atvejais)	8 val.
3.	19	Visiškai ar iš dalies neveikia šio priedo 2, 4, 6-10 p. nurodytos Infrastruktūros	8 val.
4.	20	Neveikia šio priedo 2, 6-10 p. nurodytos Infrastruktūros	8 val.
5.	21	Esminė neigiama įtaka teisėsaugos institucijų veiklai ir viešajam saugumui	8 val.
6.	33	Neigiama įtaka valstybės veikloms, susijusioms su užsieniečiais, valstybės sienos kirtimu, neigiamas poveikis valstybės įvaizdžiui	8 val.
7.	43	Sutrinka ikiteisminio tyrimo įstaigų, prokuratūros ir teismų veikla	8 val.
8.	45	Neigiama įtaka valstybės veikloms, susijusioms su užsieniečiais	8 val.
9.	49	Neigiama įtaka valstybės veikloms, susijusioms su administracine teisena, kyla neigiamas poveikis viešojo saugumo įvaizdžiui	8 val.
10.	89	Neigiama įtaka šio priedo 2 p. nurodytos Infrastruktūros veiklai, ikiteisminiams tyrimams, viešajam saugumui	8 val.

_____

Kibernetinių incidentų valdymo Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose plano
11 priedas

KIBERNETINIŲ INCIDENTŲ VALDYMO YPATINGOS SVARBOS INFORMACINĖSE INFRASTRUKTŪROSE PLANO IŠBANDYMO ATASKAITOS FORMA

(Veiklos tęstinumo valdymo grupės susitikimo data ir dokumento numeris)

Plano bandyme dalyvavo Veiklos tęstinumo valdymo grupės nariai, kiti asmenys:
1. _____
2. _____
3. _____
... _____

Kibernetinio incidento apibūdinimas:

_____
_____
_____

Ypatingos svarbos informacinės infrastruktūros, valstybės informacinės sistemos, registrai ar kitos informacinės sistemos, kurias paveikė kibernetinis incidentas:

_____
_____
_____

Kibernetinio incidento valdymo eiga:

_____
_____
_____

Rasti Plano trūkumai, kiti trūkumai:

_____
_____
_____

Pasiūlymai dėl trūkumų šalinimo:

_____
_____
_____

Veiklos tęstinumo valdymo grupės vadovo ir ataskaitą parengusio asmens parašai:

_____ _____
(vardas, pavardė) (parašas)

_____ _____
(vardas, pavardė) (parašas)

_____